



# Promoting information security as a cultural and behavioural change

---

**2010**

***Europe Direct is a service to help you find answers  
to your questions about the European Union.***

**Freephone number (\*):  
00 800 6 7 8 9 10 11**

(\*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

More information on the European Union is available on the Internet  
(<http://europa.eu>).

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2010

ISBN 978-92-9204-048-2

doi:10.2824/19099

© European Union, 2010

Reproduction is authorised provided the source is acknowledged.

*Printed in Italy*

PRINTED ON WHITE CHLORINE-FREE PAPER





## Introductory Note

This volume presents selected results achieved by the European Network and Information Security Agency (ENISA) in the field of information security awareness for the year 2010. The white papers included have been produced as part of the Work Programme 2010 of the Agency.

This edition consists of one book containing the following publications: *Online as soon as it happens, E-mail security, Malicious software, Online security at home, Preventing identity theft, Security when working remotely, Security while travelling.*

The information has been compiled based on studies, analysis, research and interviews conducted by ENISA.

The collection is published in English and it has been prepared for documentation purposes.







# General Table of Contents

<b><i>ONLINE AS SOON AS IT HAPPENS (I)</i></b> .....	<b>7</b>
<b><i>E-MAIL SECURITY (II)</i></b> .....	<b>71</b>
<b><i>MALICIOUS SOFTWARE (III)</i></b> .....	<b>107</b>
<b><i>ONLINE SECURITY AT HOME (IV)</i></b> .....	<b>155</b>
<b><i>PREVENTING IDENTITY THEFT (V)</i></b> .....	<b>197</b>
<b><i>SECURITY WHEN WORKING REMOTELY (VI)</i></b> .....	<b>241</b>
<b><i>SECURITY WHILE TRAVELLING (VII)</i></b> .....	<b>275</b>



## About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the Agency facilitates contacts between the European institutions, the Member States and the private business and industry actors.

### **Contact details:**

For general enquiries on information security awareness matters, please use the following details:

e-mail: Isabella Santa, Senior Expert Awareness Raising - [awareness@enisa.europa.eu](mailto:awareness@enisa.europa.eu)

Internet: <http://www.enisa.europa.eu/>

### **Legal Notice**

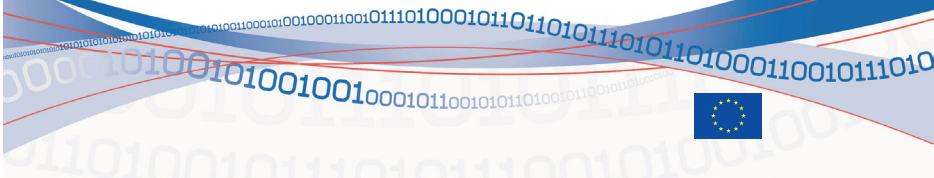
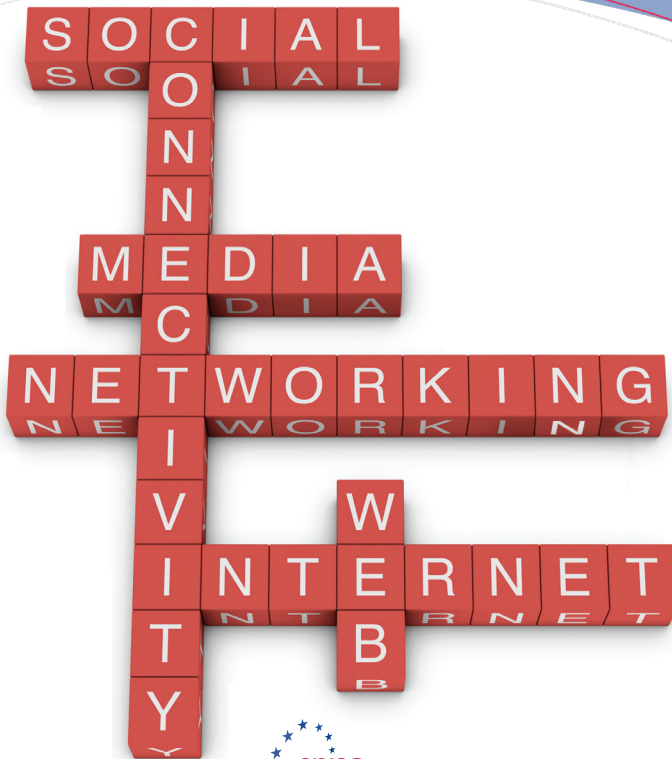
Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless it is stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

Third party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external web sites referenced in this publication.

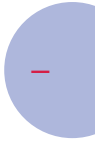
This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic mechanical, photocopying, recording, or otherwise without the prior written permission of ENISA, or as expressly permitted by Law or under terms agreed with the appropriate rights organisations. Source must be acknowledged at all times. Enquiries for reproduction can be sent to the contact address quoted in this publication.

© European Network and Information Security Agency (ENISA), 2010







**Online as soon as it happens**

*February 2010*

## Acknowledgments

Several parties supported and contributed directly or indirectly to this work in a number of ways.

ENISA wishes to acknowledge the efforts of the members of the AR Community and their organisations, Ms. Sonia Valerio of AR Enterprise S.r.l., Mr. Diego Fernández of ISDEFE, Ms. Zeina Zakhour of Atos Origin, Mr. Arjen de Landgraaf of E-Secure-IT, INTECO, Ms. Sissel Thomassen of InfoSecure, Mr. Mathieu Gorge of VigiTrust, Mr. Nicola Fabiano of Studio Legale Fabiano, Mr. Hans Pongratz of Technical University of Munich, Mr. Brian Honan of BH Consulting, Mr. Johannes Wiele of Defense AG, Mr. Corradino Corradi of Vodafone, Ms. Meltini Christodoulaki of Forth-ICS, Ms. Tara Taubman and Mr. Raoul Chiesa of @ Mediaservice.net S.r.l. who provided valuable inputs, material and prompt support for the compilation of the paper.

Finally we would also like to acknowledge and to thank Mr. Edward Kershaw of The Nielsen Company and Ms. Roberta Ruzzi of Vodafone, who contributed to this document with informal reviews, valuable insights, observations, suggestions. The content would be incomplete and incorrect without their help.





# Contents

- ACKNOWLEDGMENTS ..... 10
- EXECUTIVE SUMMARY ..... 13**
- PART 1 – SOCIAL NETWORKING GOES MOBILE ..... 15**
- INTRODUCTION ..... 16**
- SOCIAL NETWORK: A DEFINITION ..... 18**
- MOBILE SOCIAL NETWORK: A DEFINITION ..... 20**
- A EUROPEAN OVERVIEW ..... 21**
  - SOCIAL NETWORKING REACH IN EUROPEAN COUNTRIES ..... 21
  - MOBILE SOCIAL NETWORKING REACH IN EUROPEAN COUNTRIES ..... 21
- A MARKETING CHANNEL ..... 24**
- PART 2 – THE SOCIAL MOBILE EXPERIENCE ..... 27**
- MAIN FEATURES ..... 28**
- WHY SOCIAL MOBILE? ..... 29**
- PART 3 – PRIVACY AND SECURITY ISSUES ..... 31**
- PRIVACY ISSUES ..... 32**
  - THIRD PARTIES ..... 32
  - OTHER USERS ..... 33
  - PLATFORM PROVIDERS ..... 33
- MAJOR RISKS AND THREATS RELATED TO MSNs ..... 34**
  - IDENTITY THEFT ..... 34
  - MALWARE ..... 35
  - CORPORATE DATA LEAKAGE AND REPUTATION RISK ..... 36
  - STOLEN OR LOST MOBILE PHONE ..... 38
  - USER’S POSITION TRACKING ..... 38
  - DATA MISUSE ..... 39



<b>PART 4 – EUROPEAN DIRECTIVE ON DATA PROTECTION ..</b>	<b>41</b>
<b>WHAT IS THE RIGHT TO PRIVACY AND HOW IS IT PROTECTED BY EUROPEAN LEGISLATION? .....</b>	<b>42</b>
<b>DIRECTIVE 95/46/EC ON DATA PROTECTION .....</b>	<b>44</b>
A GENERAL OVERVIEW .....	44
THE HOUSEHOLD EXEMPTION .....	45
WHAT CAN THE DATA SUBJECT DO IN CASE OF VIOLATION OF HIS RIGHTS?	46
DATA PROTECTION WORKING PARTY .....	47
<b>DATA PROTECTION WORKING PARTY OPINION 5/2009 ..</b>	<b>48</b>
SOCIAL NETWORK PROVIDERS UNDER THE LENS OF THE DIRECTIVE .....	48
<i>SNS providers as data controllers</i> .....	48
<i>SNS users as data subjects</i> .....	49
APPLICABILITY OF THE DIRECTIVE TO NON-EU BASED SOCIAL NETWORKS	50
<b>IS THE SNS USER RESPONSIBLE FOR COMPLIANCE WITH THE DIRECTIVE? .....</b>	<b>51</b>
SNS USERS AS DATA CONTROLLERS .....	52
CONSEQUENCES DERIVING FROM THE QUALIFICATION OF SNS USERS AS DATA CONTROLLERS .....	54
<b>PART 5 – GOLDEN RULES .....</b>	<b>55</b>
<b>GOLDEN RULES .....</b>	<b>56</b>
<b>CONCLUSIONS .....</b>	<b>60</b>
<b>ACRONYMS .....</b>	<b>61</b>
<b>REFERENCES AND SOURCES FOR FURTHER READING .....</b>	<b>62</b>



## Executive summary

Experiencing online social networking sites (SNSs) has become one of the most popular activities carried out on the Internet. The modern way of staying in touch with business and personal contacts is to be present on social networking sites and to communicate using e-mail and other digital tools. The social networking phenomenon has registered an exceptional growth trend and there has been a widening in terms of users' profiles involved in such activity <sup>(1)</sup>, affecting and changing consequently the way people get in contact, meet, communicate and share opinion, information and ideas. This phenomenon is rapidly evolving not only in relation to the audience, changing its demographics, but also in relation to the way the audience itself can experience social networks. Besides traditional computer-based access, users are now able to access social networks through their mobile phones.

Mobile social network (MSN or social mobile) is a means of communication using a combination of voice and data devices over networks including cellular technology and private and public IP infrastructure <sup>(2)</sup>. Subscribers access social networks on their mobile phone by browsing over the mobile internet, through downloaded applications and by text – messaging <sup>(3)</sup>. In this paper we will refer and take into particular consideration the 'on deck' services <sup>(4)</sup>, coming pre-packaged with the purchase

---

<sup>(1)</sup> This shift has primarily been driven by Facebook, which started as a service for university students; now almost one third of its global audience is aged 35–49 years and almost one quarter is over 50 years old. Source: The Nielsen Company, *Global faces and networked places*, March 2009, available at <http://blog.nielsen.com/nielsenwire/nielsen-news/social-networking-new-global-footprint/> (last visited on 5 October 2009).

<sup>(2)</sup> Nick Lane, Nicky Walton-Flynn, Freda Benlamlih (Informa Telecoms & Media), *Mobile social networking* – the paper was sponsored by Buongiorno and the research has been carried out by Informa Telecoms & Media, July–September 2008 – available at [http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno\\_final-fmt\\_nl-3110-f.pdf](http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt_nl-3110-f.pdf) (last visited on 18 November 2009).

<sup>(3)</sup> Users can register a phone that allows them to send text message post directly to their user profile.

<sup>(4)</sup> 'On deck' refers to applications that operate through a partnership between social network companies and wireless phone carriers whereby programs and application are distributed via the wireless carrier.



of a mobile phone. Nevertheless the overall data and figures provided in this document include all modes of access to social networking.

Nowadays many mobile users use their phone as a backup device for business and personal data, contacts and pictures also keeping a record of their personal details and access codes. As a consequence, a lost or stolen mobile phone can cause serious damage considering that all information and data, about the user and his contacts, entrusted on SNSs and linked to the mobile phone could be used in an illegitimate way. Case studies from different European countries show that a considerable number of users are unaware of their exposure to security risks and privacy issues. While many of the privacy issues originating from the web-based access to SNSs also apply to MSNs, there are also a number of unique risks and threats against MSNs.

ENISA believes that users' awareness is the first line of defence regarding their privacy and security of their data. This white paper aims to provide a set of recommendations for raising the awareness of SNSs users and in particular of social mobile users of the risks and the possible consequences related to their improper use.

This document does not cover the access of SNSs through mobile phone by minors <sup>(5)</sup> and consequently any matters related to this aspect. Finally, it should not be seen as either a comprehensive source of all risks associated to the usage of social networks or as a technical guideline or specification to secure standards or solutions.

---

<sup>(5)</sup> Nevertheless the data provided for the description of the social networking scenario in Europe include the access of social networks also by users aged 15 and older.

# PART 1 – SOCIAL NETWORKING GOES MOBILE



## Introduction

According to recent statistics there are more than 65 million active users currently accessing Facebook through their mobile devices and the ones that do so are almost 50% more active than non-mobile users <sup>(6)</sup>.

Today mobile devices are not only used for voice communication or simple peer-to-peer connections between people who know each other, but also for data connection to the Internet. Moreover, with their sophisticated and user friendly features, mobile devices are not only consuming content but are also capable of producing and storing content. The rapid development of information and communication technologies, especially the Internet and the mobile phone, has transformed the way people interact with each other and connect with the environment around them. Over the last few years, a plethora of new applications have sprung up, enabling a whole new dimension of social interaction. Portability, high capacity memories and 'always on' technology are pushing the use of mobile devices for an increasing number of services in the everyday life and are bringing the networking environment definitely closer to users. The MSN services that come pre-packaged with the purchase of a mobile phone, to which we refer in this paper, support social networks through their ubiquitous usability and easy sharing of location, information and experiences and allow access to SNSs anytime and anywhere with just a click <sup>(7)</sup>.

Users need guidance and education on how simple lack of attention or voluntary misconduct when accessing and using social networks through a mobile phone can have unexpected consequences which can be avoided by following some good practices that each user should be aware of. Several stories highlight that many users are unaware of the risks and

---

<sup>(6)</sup> Facebook press room, statistics available at <http://www.facebook.com/press/info.php?statistics> (last visited on 5 October 2009).

<sup>(7)</sup> This paper does not include the description of the 'off deck' services referring to those applications that do not come pre-packaged with the purchase of a mobile phone but have to be downloaded from the Internet or from a wireless provider after the time of purchase.



threats related to the misuse of the information they entrust to an SNS and of the proper way to protect their privacy<sup>(8)</sup>. Severe reputational and personal damage can be caused not only by the users themselves but also by other users and third parties, using the social networking tools in an improper way. For example, in the UK, a teacher has been suspended for complaining on Facebook about her class<sup>(9)</sup> and in Italy, the forgery of a Professor's identity has been discovered on Facebook, while friends and colleagues of the victim were chatting and sharing information with someone that was not who he claimed to be<sup>(10)</sup>.

ENISA believes that increasing awareness of the risks and the possible consequences related to social networks' improper use is the first line of defence. This paper is designed to provide comprehensive information about the MSN services and the risks and threats connected to their use. It will also analyse the social networking world under the lens of the European directive on data protection.

---

<sup>(8)</sup> According to a recent survey conducted by AVG and CMO Council 'less than one third of social networkers are taking actions to protect themselves online', *Bringing social security to the online community*, 26 August 2009, available at [www.avg.com.au/files/media/avg\\_socialsecurity\\_2009-08-26\\_au.pdf](http://www.avg.com.au/files/media/avg_socialsecurity_2009-08-26_au.pdf) (last visited on 19 November 2009).

<sup>(9)</sup> MailOnline, *Teacher is suspended for jibe on Facebook about her class*, 1 August 2009, available at <http://www.dailymail.co.uk/news/article-1202210/Teacher-suspended-jibe-Facebook-class.html> (last visited on 26 November 2009).

<sup>(10)</sup> LaStampa.it, *Facebook, rubata l'identita' a un Professore di Trento*, 5 January 2009, available at [http://www.lastampa.it/\\_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID\\_blog=30&ID\\_articolo=5580&ID\\_sezione=38&sezione=News](http://www.lastampa.it/_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=5580&ID_sezione=38&sezione=News) (last visited on 26 November 2009).



## Social network: a definition

A social network is an online community that allows people, through a built-up profile, to meet, communicate, keep in touch, share pictures and videos with other community members with whom a connection is shared.

The social network's structure includes having a profile (which contains personal information about the user), friends (trusted community members that can post comments on the user's profile and send private messages) and groups (people with the same interests meet online and discuss a variety of topics). Some social networks also allow users to personalise their profile using widgets or to create their own blog entries.

From a functional point of view <sup>(1)</sup>, social networks can be classified in two main categories: 'general purpose' and 'niche' social networks.

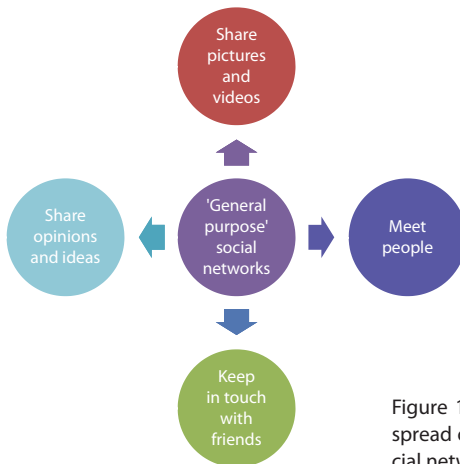


Figure 1: Different types of interests spread out from 'general purpose' social networks.

<sup>(1)</sup> For a deeper analysis see Alexander Richter, Michael Koch, *Functions of social networking services*, in: Proceedings of the 8th International Conference on the Design of Cooperative Systems, Carry-le-rouet, France, Institut d'Etudes Politiques d'Aix-en-Provence, 2008, available at <http://www.kooperationssysteme.de/docs/pubs/RichterKoch2008-coop-sns.pdf> (last visited on 5 November 2009).



‘General purpose’ social networks have as a primary scope communication and interaction among users and anybody is free to join the online community since they do not cater to any specific theme or interest but they gather a variety of interests. Among others, Facebook, Myspace, Badoo and Netlog belong to this category. On the other side, ‘niche’ social networks allow users to perform a specific activity<sup>(12)</sup>. Business-oriented social networks such as LinkedIn or reunion sites such as Classmates.com are in fact sites focused on a specific interest such as professional contacts or the search for old school friends.

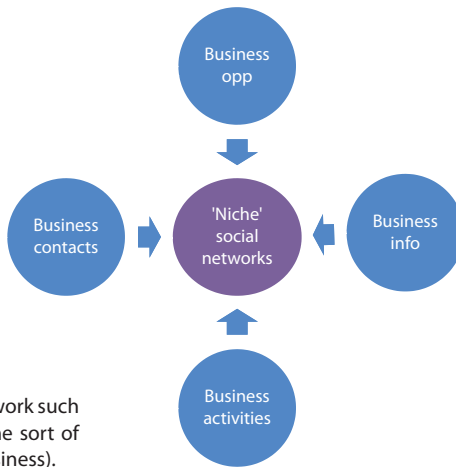


Figure 2: A ‘niche’ social network such as LinkedIn attracts the same sort of interest (i.e. professional/business).

<sup>(12)</sup> Joseph Bonneau, Sören Preibusch, *The privacy jungle: On the market for data protection in social networks*, Eighth Workshop on the Economics of Information Security (WEIS 2009), 24–25 June 2009, available at <http://weis09.infosecon.net/files/156/index.html> (last visited on 5 November 2009).

## Mobile social network: a definition

A first generation of social networking on mobile networks began in 1999/2000 as chat services launched in some European and non European countries<sup>(13)</sup>. The phenomenon spread rapidly and evolved through the years to the current environment and services offered. According to Facebook<sup>(14)</sup>, there are more than 180 mobile operators in 60 countries working to deploy and promote Facebook mobile products.

Mobile social networking is a means of communication using a combination of voice and data devices over networks including cellular technology and private and public IP infrastructure<sup>(15)</sup>. Generally speaking MSNs can be divided into two categories: 'on deck' and 'off deck'. 'On deck' refers to services that operate through a partnership between social network companies and wireless phone carriers. This category of services programs and applications which enable the social networking experience are distributed via the wireless carrier and are pre-packaged with the purchase of a mobile phone. 'Off deck' refers instead to services whose applications do not come pre-packaged and the user has to download the application from the Internet or from a wireless provider after the time of purchase.

Many SNSs, like MySpace and Facebook, offer phone versions of their services, allowing users to interact with their friends. This enables the users to experience the social networks on their handset and to gain advantages from getting immediate alerts and notification of changes in

---

<sup>(13)</sup> For a complete description of the history of mobile social networking see Nick Lane, Nicky Walton-Flynn, Freda Benlamlih (Infoma Telecoms & Media), *Mobile social networking* – the paper was sponsored by Buongiorno and the research has been carried out by Infoma Telecoms & Media, July-September 2008 – available at [http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno\\_final-fmt\\_nl-3110-f.pdf](http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt_nl-3110-f.pdf) (last visited on 18 November 2009).

<sup>(14)</sup> Facebook press room, statistics available at <http://www.facebook.com/press/info.php?statistics> (last visited on 5 October 2009).

<sup>(15)</sup> Nick Lane, Nicky Walton-Flynn, Freda Benlamlih (Infoma Telecoms & Media), *Mobile social networking* – the paper was sponsored by Buongiorno and the research has been carried out by Infoma Telecoms & Media, July-September 2008 – available at [http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno\\_final-fmt\\_nl-3110-f.pdf](http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt_nl-3110-f.pdf) (last visited on 18 November 2009).



their communities (immediacy), to personalize and reflect personal preferences and conditions (intimacy) and to spot the presence of others in the local area (discovery of others in proximity) <sup>(16)</sup>.

## A European overview

### Social networking reach in European countries

Of the around 283 million European users, 211 million of them, aged 15 and older who accessed Internet via a home or work computer, visited a social networking site. The largest public is represented by the UK with 29 million visitors, reaching 80% of the country's total Internet audience <sup>(17)</sup>. Among all social networking sites, Facebook has gained a top position throughout the majority of European countries. A research conducted by comScore <sup>(18)</sup> stated that, of the 17 European countries included in the study, Facebook played a leading role in the social networking category in 11 of them in terms of unique visitors. The site's largest audience is in the UK with about 23 million visitors followed by France with about 14 million visitors. The only countries in which Facebook does not hold the No 1 or No 2 position are Germany (No 4), Portugal (No 3) and Russia (No 7).

### Mobile social networking reach in European countries

The growing popularity of social networks has determined an increasing demand to access them via mobile phone. The mobile social networking

<sup>(16)</sup> Nick Lane, Nicky Walton-Flynn, Freda Benlamlah (Informa Telecoms & Media), *Mobile social networking* – the paper was sponsored by Buongiorno and the research has been carried out by Informa Telecoms & Media, July-September 2008 – available at [http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno\\_final-fmt\\_nl-3110-f.pdf](http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt_nl-3110-f.pdf) (last visited on 18 November 2009).

<sup>(17)</sup> comScore press release, 17 February 2009, available at [http://www.mediametrix.com/Press\\_Events/Press\\_Releases/2009/2/Social\\_Networking\\_France](http://www.mediametrix.com/Press_Events/Press_Releases/2009/2/Social_Networking_France) (last visited on 5 November 2009).

<sup>(18)</sup> comScore press release, 15 April 2009, available at [http://www.comscore.com/layout/set/popup/Press\\_Events/Press\\_Releases/2009/4/Facebook\\_Top\\_Social\\_Network\\_in\\_Spain](http://www.comscore.com/layout/set/popup/Press_Events/Press_Releases/2009/4/Facebook_Top_Social_Network_in_Spain) (last visited on 5 November 2009).



scenario described by the data and figures below include all kind of access to social networking (such as mobile internet, apps). Social networking attracts three quarters of European Internet users and, in the UK, it is one of the few mobile Internet activities more popular with females than males (Figure 3) in respect of general mobile internet browsing (Figure 4).

### Mobile social networking

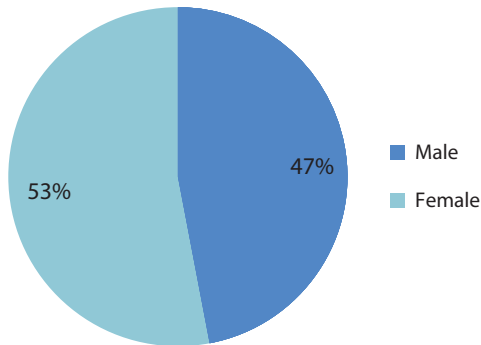


Figure 3: UK, Q4 2009,  
Source: The Nielsen Company.

### General mobile Internet browsing

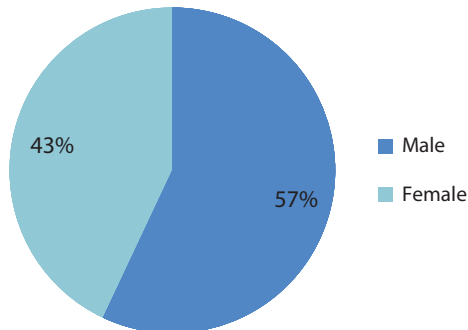


Figure 4: UK, Q4 2009,  
Source: The Nielsen Company.

In the UK, in the fourth quarter of 2008, 2 million people visited a social network through their handset, corresponding to an increase in 2008 of 249% <sup>(19)</sup>. The number of social mobile users grew rapidly. In the fourth quarter of 2009 figures for the UK show that 3.9 million people accessed a social network through their handset with an increase of almost 200% on Q4, 2008 <sup>(20)</sup>.

The most popular social networking sites accessed via personal computer are also the leading ones being used over mobile phones. Facebook represents the vast majority of social networking's active reach on mobile phones and it has been the most visited site in at least four European countries: the UK, Italy, Spain and France <sup>(21)</sup>.

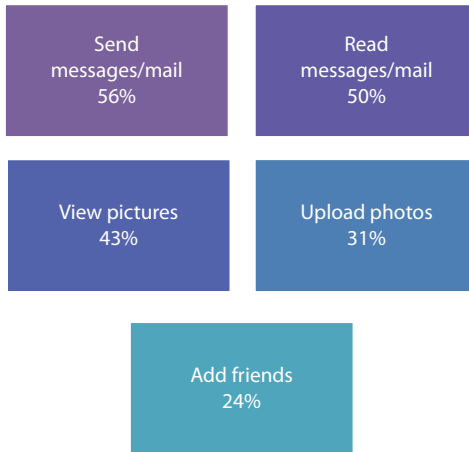


Figure 5: Top five mobile social networking activities  
 Source: The Nielsen Company.

<sup>(19)</sup> The Nielsen Company, *Global faces and networked places*, March 2009, available at <http://blog.nielsen.com/nielsenwire/nielsen-news/social-networking-new-global-footprint/> (last visited on 5 November 2009).

<sup>(20)</sup> ENISA has been provided with this data by The Nielsen Company.

<sup>(21)</sup> ENISA has been provided with this data by The Nielsen Company. It refers to Q2, 2009 and to Q1, 2009 (France).

Figure 5 shows the top five social networking activities conducted on a mobile phone at a pan-European level <sup>(22)</sup>. Other activities are also carried out on a mobile phone, such as: receive text alert (23%), view profiles (15%), create or update profile (13%), upload videos (10%), participate in chat rooms (8%) and post blogs (7%).

## A marketing channel

Social networks are communication channels with features largely comparable to newspaper, radio and television. Companies with a product or service should consider it as another vehicle to target the audience and to communicate with consumers <sup>(23)</sup>.

Social networks provide significant competition for publishers in terms of consumer attention but also give them the opportunity to create a tailored content, reflecting the public's desires and tastes and to optimize campaign reach. The time spent on social networks, by chatting with friends, posting content and so on, increase the size and value of the network, making the social network more attractive as an engaging advertising medium <sup>(24)</sup>. Mobile advertising provides the opportunity for op-



<sup>(22)</sup> The Nielsen Company, *Mobile media nei mercati emergenti e in Italia*, IAB Seminar, 16 July 2008, available at <http://www.iabseminar.it/video.aspx?IDSessione=12> (last visited on 5 November 2009).

<sup>(23)</sup> The Nielsen Company, *Global faces and networked places*, March 2009, available at <http://blog.nielsen.com/nielsenwire/nielsen-news/social-networking-new-global-footprint/> (last visited on 5 November 2009).

<sup>(24)</sup> Mashable, *The social media guide, Exploring best practices for building and monetizing mobile social networks*, 3 October 2008, available at <http://mashable.com/2008/10/03/mobile-social-networking/> (last visited on 30 November 2009).



erators to earn revenues from greater data usage as users click through to, and browse, advertiser sites, or else respond to advertisement by SMS <sup>(25)</sup>. In this regard, mobile social networks will play a leading role in term of revenues <sup>(26)</sup>.

The exploitation and monetization of social networks include the following economical variables:

- ✓ Advertising (based on users' preferences and main source of income).
- ✓ Premium (in order to obtain a more advanced profile or use more applications users need to subscribe to options, subject to charges).
- ✓ Donations (users make donations for the maintenance of the platform).
- ✓ Payment for use (users need to pay for the access and usage of certain tools) <sup>(27)</sup>.

---

<sup>(25)</sup> Juniper Research, *Mobile advertising, because I'm worth it*, extract from *Mobile advertising delivery channels, strategies & forecasts 2008-2013*, 2008, available at [http://www.c2mweb.eu/files/Whitepaper\\_Mobile\\_Advertising.pdf](http://www.c2mweb.eu/files/Whitepaper_Mobile_Advertising.pdf) (last visited on 30 November 2009).

<sup>(26)</sup> *Advertising to Fuel Mobile Social Networking Growth as User Generated Content Revenues Reach \$7.3bn by 2013*, available at <http://arabcrunch.com/2008/09/advertising-to-fuel-mobile-social-networking-growth-as-user-generated-content-revenues-reach-73bn-by-2013.html> (last visited on 25 January 2010).

<sup>(27)</sup> INTECO, *Study on the privacy of personal data and on the security of information in social networks*, February 2009, available at [http://www.inteco.es/Security/Observatory/Publications/Studies\\_and\\_Reports/estudio\\_redes\\_sociales\\_en](http://www.inteco.es/Security/Observatory/Publications/Studies_and_Reports/estudio_redes_sociales_en) (last visited on 24 November 2009).







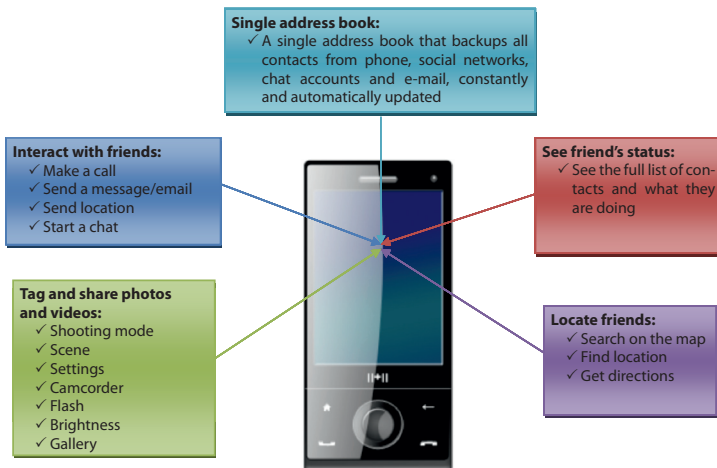
## PART 2 – THE SOCIAL MOBILE EXPERIENCE



## Main features

The world of social networking and the new ways of communicating are no longer confined to the user's desk. The online social network experience has been extended into everyday life without the need for a PC screen thanks to the integration between mobile phones and social networks. The launch of this technology has brought the networking environment closer to the user, empowering and enhancing opportunities for interaction and communication. MSNs offer almost the same services of web-based social networks but with a much greater interaction with everyday life. 'Online as soon as it happens' better summarizes and describes the social mobile experience, allowing users to test a new kind of interaction and communication where every moment and thought can appear online as soon as soon it is experienced.

In particular, the MSN's services coming pre-packaged with the purchase of a mobile phone offer the chance to combine web-based and phone-based information in order to gather in one place all user contacts, communities, entertainment and personal favourites.





One of the results of this interaction is the 'social phonebook' which provides one place to store contacts available on a SNS and the ones already stored in a mobile phone, keeping them constantly synchronized. The user can rotate through all of the contacts displayed in the mobile's screen, pick up a friend and choose how to communicate, either by message, chat or e-mail. After synchronizing the social networks contacts and the chat accounts, users can see what their friends are doing in that very specific moment and where they are thanks to the map function that can locate them in real time. The quick and easy way to communicate can be found in another new feature provided by MSNs which is the possibility to take a picture and/or a video, to save it and tag it on the mobile phone and share it online, as soon as it happens, with friends and peers.

## Why social mobile?

It has been estimated that in 2011 the number of mobile social network users worldwide will be 554 million, corresponding to 13.3% of mobile phone subscribers, with a growing trend for 2012: 803 million users, corresponding to 18.8% of mobile phone subscribers<sup>(28)</sup>. In Europe, in 2012, the number of users will be 134 million meaning that one out of five mobile phone subscribers will use the mobile device to access a social network<sup>(29)</sup>.

The increasing demand to access social networks on the move is a natural consequence for social networks, as consumers are used to communi-

<sup>(28)</sup> eMarketer, April 2008, available at [http://www.emarketer.com/Report.aspx?code=emarketer\\_2000489](http://www.emarketer.com/Report.aspx?code=emarketer_2000489) (last visited on 2 November 2009).

<sup>(29)</sup> Nick Lane, Nicky Walton-Flynn, Freda Benlamlah (Informa Telecoms & Media), *Mobile social networking* – the paper was sponsored by Buongiorno and the research has been carried out by Informa Telecoms & Media, July-September 2008 – available at [http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno\\_final-fmt\\_nl-3110-f.pdf](http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt_nl-3110-f.pdf) (last visited on 2 November 2009), The daily bit, *Un fenomeno chiamato mobile social networking*, September 2008, available at <http://www.thedailybit.net/index.php?method=section&action=zoom&id=2489> (last visited on 18 November 2009) and Lastampa.it, *In Europa il social network piace sul cellulare*, August 2008, available at [http://www.lastampa.it/\\_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID\\_blog=30&ID\\_articolo=5054&ID\\_sezione=38&sezione=News](http://www.lastampa.it/_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=5054&ID_sezione=38&sezione=News) (last visited on 18 November 2009).



cating with friends via mobile calls and text. Using a mobile phone to access social networks does not require much of a change in consumer habits<sup>(30)</sup>. On the contrary, it lets the user explore new ways of communicating. Since a mobile phone is always with the user, it is possible to be constantly in touch with friends and peers and communicate what they are up to and where they are, anytime and anywhere, without the limitation of traditional web-based



access. It is no longer, in fact, only a question of what the user is doing but also where he is located, since the new map function provided by mobile phones allows users to find and locate their friends and also to get directions. The quick and easy access to social networks can also be considered as a pre-eminent reason for this phenomenon. It is now possible to enter the user's personal profile with just a click and to upload a picture as soon as it has been taken with a mobile phone.

In this regard, it should be noted that the information posted and published, such as pictures, videos and comments, via the mobile phone services are the user's responsibility. This means that the user needs to take care of all the content he publishes about himself or his friends in order to protect his own and other people's privacy, personal and professional life.

---

<sup>(30)</sup> The Nielsen Company, *Global faces and networked places*, March 2009, available at <http://blog.nielsen.com/nielsenwire/nielsen-news/social-networking-new-global-footprint/> (last visited on 5 October 2009).

**PART 3 – PRIVACY AND SECURITY ISSUES**



## Privacy issues

Every SNS user should be aware of the risks and threats related to the use of social networks. Besides the services and opportunities offered, social networks are not exempt from risks affecting users' privacy, personal and professional life. In this regard, it should be noted that general social networks are exposed to a higher level of risk than, for example, professional social networks since users, in general social networks, not only publish information related to their work experience or their studies but also information and data related to their tastes, ideology or experiences, thus making available much more information about themselves than in professional social networks <sup>(31)</sup>. Privacy issues can arise from three different types of attackers <sup>(32)</sup>:

- ✓ third parties.
- ✓ other users.
- ✓ platform providers.

### Third parties

Third parties may gain fraudulent access to personal data published on a user profile or by stealing or finding a lost mobile. Information and data collected in such a manner can cause severe privacy issues. Access by a third party can also occur without violating any technical rules and is due basically to the privacy profile level which is not set properly by the user (who hasn't paid enough attention to the privacy settings). On some

---

<sup>(31)</sup> INTECO, *Study on the privacy of personal data and on the security of information in social networks*, February 2009, available at [http://www.inteco.es/Security/Observatory/Publications/Studies\\_and\\_Reports/estudio\\_redes\\_sociales\\_en](http://www.inteco.es/Security/Observatory/Publications/Studies_and_Reports/estudio_redes_sociales_en) (last visited on 24 November 2009).

<sup>(32)</sup> Martin Pekárek, Stefanie Pöttsch, *A comparison of privacy issues in collaborative workspaces and social networks*, published online 28 July 2009, available at <http://www.springerlink.com/content/g54qk93430581554/?p=dae26d8123004ccf88e5004aa1aba269&pi=0> (last visited on 5 November 2009); Martin Pekárek, Ronald Leenes, *Privacy and Social Network Sites: Follow the Money!* January 15-16, 2009, available at [www.w3.org/2008/09/msnws/papers/tilt.pdf](http://www.w3.org/2008/09/msnws/papers/tilt.pdf) (last visited on 24 November 2009).



sites, users that change their default settings from private to public receive a security message about the risks they could face by making their profile public <sup>(33)</sup>.

## Other users

Other users also have the same potential as third parties to cause privacy issues. It is possible in fact to leave comments on the personal profile of other community members or to tag a picture portraying the user without his consent in an awkward situation. Many privacy issues can be traced back to the out-of-context use of personal data, with a greater impact when this involves trusted contacts who normally have legitimate access to a high level of information <sup>(34)</sup>. This is why it is also important to agree with friends and peers on the rules to be followed when using and accessing social networks in order to ensure secure personal data processing.

## Platform providers

The user can regulate, through the privacy settings, who has access to the information that decides to provide. Nevertheless, in some cases, the platform provider has full access to user data, collecting for example the user's IP address and browser type and the information provided is available in search results across the network and to third-party search engines.

---

<sup>(33)</sup> *Privacy setting for social networks*, available at <http://blog.safetyclicks.com/2008/09/03/social-networks-and-privacy-settings/> (last visited on 5 November 2009).

<sup>(34)</sup> Martin Pekárek, Stepanie Pötzsch, *A comparison of privacy issues in collaborative workspaces and social networks*, published online 28 July 2009, available at <http://www.springerlink.com/content/g54qk93430581554/?p=dae26d8123004ccf88e5004aa1aba269&pi=0> (last visited on 5 November 2009).





## Major risks and threats related to MSNs

Social networks have drastically modified the traditional use of the Internet, turning it into an increasingly communicative medium and attracting millions of users that access SNSs through a PC screen or a mobile phone. The growing popularity of the social mobile phenomenon creates significant opportunities for business and personal purposes but also exposes its users to security risks and threats.

### Identity theft

Identity theft in mobile social networks is one of the most important threats as its consequences may affect the reputation and privacy of the user. Identity theft can be easily carried out by a malicious attacker in a mobile environment because it can be performed by stealing, permanently or temporarily, security credentials (i.e. 'Man in the Middle' attack), or by stealing the device <sup>(35)</sup>. Once the attacker takes control of the phone or has intercepted user credentials, he will be able to take full control of the user's account by publishing comments in the name of the legitimate user, by changing the current password and e-mail address to perma-

#### Italy – Professor's fake profile on Facebook

*A fake profile of a University professor in Turin was created on Facebook. The professor wanted to create his own Facebook page but he found out that someone else had already registered him, creating a profile with very offensive features, affecting his reputation. The episode was immediately reported to the public prosecutor in Turin for the necessary investigation and measures to be taken.*

<sup>(35)</sup> ENISA, *Security issues in the context of authentication using mobile devices (Mobile eID)*, 2008, available at [http://www.enisa.europa.eu/act/it/eid/mobile-eid/?searchterm=security issues mobile devices](http://www.enisa.europa.eu/act/it/eid/mobile-eid/?searchterm=security%20issues%20mobile%20devices).





nently take control of the account or by using the compromised account to spread malicious software — or ‘malware’ — through social engineering. The ‘forgery’ of a user’s identity can have a very serious impact on his personal life and reputation at work.

### Spain – Multiple identity theft aimed at celebrities

*During 2009 there have been multiple identity theft cases in Spain, aimed at celebrities and well-known people. A Spanish writer and a politician found out that fake profiles of them were circulating on a social network, with comments and opinions published in their names, affecting their reputation and privacy.*

## Malware

As social networking sites allow their users to interconnect, they constitute an ideal platform for the distribution of malware. Although there is not yet any known mobile malware propagation through mobile social networks, this kind of social network can send especially crafted malware directly to mobile phones, using also Bluetooth and Wifi features in mobile phones to propagate. Malware could steal information stored in the mobile social network, or infect the mobile phone itself in order to access the information stored; it could even use the device as a proxy to propagate the malware infection through SMS to the phone’s contacts and through the Internet connection to the contacts in the mobile social network. Twitter, Facebook, Myspace and other social networking platforms have been used to distribute malware. The widespread takes place when a link to a website, rigged with malicious software, is posted by an infected computer on a social networking site. Users click on the link, trusting the friends who posted the links, not knowing that their friends have been hacked <sup>(36)</sup>. One

<sup>(36)</sup> InfoWorld, *Hackers put social networks such as Twitter in crosshairs*, 17 August 2009, available at [http://www.infoworld.com/d/security-central/hackers-put-social-networks-such-twitter-in-cross-hairs-832?source=IFWNLE\\_nlt\\_sec\\_2009-08-17](http://www.infoworld.com/d/security-central/hackers-put-social-networks-such-twitter-in-cross-hairs-832?source=IFWNLE_nlt_sec_2009-08-17) (last visited on 19 November 2009).



of the methods encouraging social networking users to click on infected links is the technique of sending out spoofed e-mail. Hackers create an e-mail message, appearing to be sent from a social networking site inducing the user to update the personal account or open an attachment containing the new password <sup>(37)</sup>.

### Corporate data leakage and reputation risk

Users discuss and share their experiences, including work ones, on social networking sites. In addition, users have been linking their numerous accounts available on different social networking sites, thus syndicating and federating the posts among the linked profiles. This interconnection especially between professional and personal social networking sites distributes data cross-boundaries and makes it extremely difficult to contain and remove indiscretions.

#### **UK- Data leakage for airlines companies**

*In 2008, Virgin Atlantic airlines investigated allegations that its staff posted rude comments on Facebook criticised the cleanliness of the company's fleet and of its passengers. The 13 members of the Virgin Atlantic staff have been dismissed for their behaviour. Later, a similar episode involved the British airlines check-in staff based in Gatwick who posted on Facebook messaging saying that travellers are 'smelly' and that operation's at Heathrow's Terminal 5 are 'shambolic'. An investigation was launched after the episode.*

---

<sup>(37)</sup> Due to the newer techniques used by hackers, identifying malicious links has become harder. One of newer methods consists of hijacking Twitter's trending topics by creating Twitter new accounts and posting messages related to the most trending topic discussed on Twitter at that time. This would allow the post to be aggregated in Twitter search results where unsuspecting users would click on the included link. The text accompanying the link would be intriguing to those interested in the subject, tempting them to click through.



Consequently, users posting professional information on their business profile could have these posts distributed to their Facebook or Twitter accounts leading to the accidental disclosure of corporate sensitive data.

### **Italy – Critics of her company on Facebook: fired**

*An Italian woman working for a company based in Milan was fired because of comments posted on her Facebook profile about the company. The employee created a group online, aiming to gather all her colleagues in other cities working for the same company, in order to complain about being an employee at the company.*

### **France – Video spreading on Facebook: breach of investigation secrecy**

*The leak of a night bus video surveillance tape, revealing the violent assault of a passenger, provoked outrage in France in mid-April 2009. The footage was posted by a French policeman on his Facebook profile and showed a violent attack inside a Parisian night bus where a passenger was robbed and brutally assaulted by a gang. It would have been just another urban violent robbery had the policeman not posted the footage on his Facebook profile. In fact, once the video was available online, it spread all over the Internet on various social networking sites and raised uproar in the country. The posting of the video was considered a direct violation of the victims' rights as they were clearly identifiable in the footage. The repercussions of this leak led the main victim to file a lawsuit denouncing a breach of investigation secrecy. Ironically the policeman was bewildered by the video spreading like wildfire as he believed it was only destined for his friends to see. He immediately deleted the video and his Facebook account hoping to contain the incident but it had already circulated on all possible networks.*



Mobile social network services can contribute, intentionally or unintentionally, to the information leakage. The real-time spread through social mobile of corporate data can cause serious damage to organisations. Users can also be affected by this threat as a result of unauthorised posts or photographs in real time which can affect their privacy and reputation at work.

### Stolen or lost mobile phone

A lost or stolen mobile phone can cause serious damage. Nowadays the mobile phone has become a database, with all kind of information kept in it, and used as a backup device for important data, access codes, contacts, pictures and with the record of users' personal and corporate details. Many mobile users use their mobile phone for corporate e-mail with copies of them held on the phone. If the mobile phone gets lost or stolen, it is necessary to change the passwords of the SNSs, e-mail and any other sites that have been linked to the mobile in order to protect the user's personal information and the privacy of friends, company and clients whose contacts on the SNS have been synchronized with the mobile phone.

### User's position tracking

Mobile service providers and some mobile phones are equipped with the necessary technology to track the devices, which implies that the users themselves are being tracked. Companies are launching new applications and widgets which implement this capability into mobile social networks. The map function gives users the chance to see, in real time, where their friends are located and to choose who can see where they are. The related threat is the possibility of knowing the geographical position of the user and to perform an attack directly aimed at his account or through the accounts of his contacts. Once this information is available, malicious activities such as blackmail, hijacking, stalking, physical attack etc. could be carried out, affecting the user's personal security.



## Data misuse

The access to personal information gained either through a lost, stolen or hacked mobile phone, or just because too many details have been provided on a SNS's profile can head to the possible misuse of such personal data, jeopardizing personal and professional life. The spreading of incorrect and private information becomes a relevant issue especially when it affects not only private life but also the working environment.

### **Greece- Fake profile with nude pictures posted by the ex-boyfriend on Facebook**

*In October of 2009, the Greek Hotline which receives reports for illegal Internet content (SafeLine) received a report from a woman who claimed that after she broke up with her boyfriend, he created a fake profile of her on Facebook, posting pictures of her naked. The woman immediately realised that the only person who could have access to those pictures was her ex-boyfriend and so she reported him. Following the report, the specific account has been removed.*

### **UK – Payout for data misuse on Facebook**

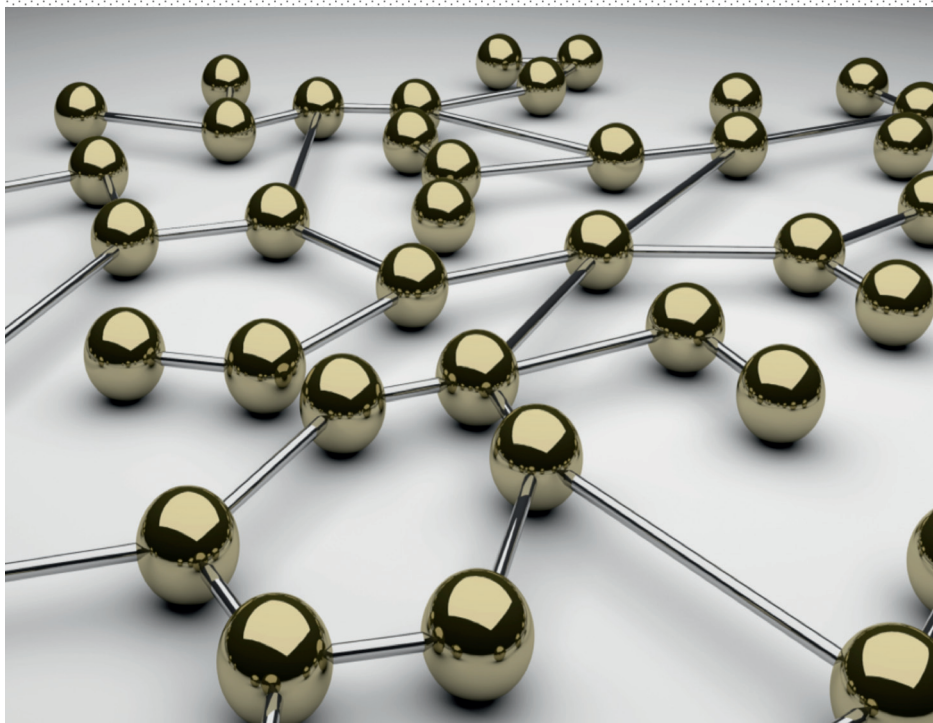
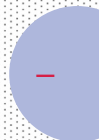
*In the UK a businessman sued an old school friend for creating a fake Facebook profile of him. The plaintiff claimed that the set up profile contained personal information 'for all to see' including false information about his sexual orientation and political views. The victim sought damages for libel and misuse of private information and won the case at the High Court which condemned the defendant to pay the damages.*







## PART 4 – EUROPEAN DIRECTIVE ON DATA PROTECTION



## What is the right to privacy and how is it protected by European legislation?

The right to privacy is a negative right of not interfering in someone's private and family life<sup>(38)</sup>. On the other hand, data protection is a positive concept that implies that everyone has the right to the protection of personal data concerning themselves and that such data must be processed fairly, with a purpose limitation and with the consent of the person concerned or on a lawful basis<sup>(39)</sup>. The existing data protection framework is constituted by:

- ✓ Directive 95/46/EC on data protection<sup>(40)</sup> ('DPD' or 'directive').
- ✓ Directive 2002/58/EC on e-privacy<sup>(41)</sup>.
- ✓ RFID recommendation<sup>(42)</sup>.

The scope of the DPD is to apply to the processing, wholly or partly, by automated and non-automated means, of personal data which form part of a filing system or are addressed to be part of it<sup>(43)</sup>. Member States, in line with the DPD, shall consequently protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy in relation to the processing of personal data<sup>(44)</sup>.

<sup>(38)</sup> See Article 7, Charter of Fundamental Rights of the European Union, OJ C 364/1, 18.12.2000.

<sup>(39)</sup> See Article 8, Charter of Fundamental Rights of the European Union, OJ C 364/1, 18.12.2000.

<sup>(40)</sup> Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.

<sup>(41)</sup> Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002. The Council of the European Union adopted, on 26 October 2009, a directive amending, amongst others, the e-privacy directive. The amendments include an obligation for Internet service providers to notify data breaches to the competent national regulator. The directive needs to be signed by the presidents of the Council and the European Parliament and will enter into force the day following publication in the Official Journal of the European Union (OJ).

<sup>(42)</sup> Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, OJ L 122, 16.5.2009.

<sup>(43)</sup> See Article 3, DPD.

<sup>(44)</sup> See Article 1, DPD. The status of implementation of the DPD in each Member State is available at [http://ec.europa.eu/justice\\_home/fsj/privacy/law/implementation\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm) (last visited on 20 October 2009).





### Italy – Social network: watch out for side effects

*In May 2009, a nurse, working at a hospital in Udine, published on her Facebook profile almost 50 pictures taken inside the intensive care unit. In some of the photos, patients receiving medical treatment were visible. The Italian Data Protection Authority (DPA) decided to open a preliminary investigation in order to ascertain a possible breach of the right to privacy. Earlier the same year, another case took place at a hospital in Turin, where a nurse published on her Facebook profile a picture of an unconscious, drunk patient after adding some offensive comments. The nurse was suspended for ten days. Since these two alarming cases, highlighting the lack of users' awareness when accessing SNSs, the Italian DPA has released a short guide to 'help those planning to sign up to a social network and those who have already joined a social network to use this new tool knowledgeably.'*

The e-privacy directive specifies and complements the DPD <sup>(45)</sup> in order to ensure a harmonisation of the Member States' provisions thereby ascertaining an equal level of protection of fundamental rights and freedoms.

The RFID recommendation provides guidance on measures to be adopted for the deployment of RFID <sup>(46)</sup> applications to ensure the respect of national legislation implementing the DPD and the directive on e-privacy <sup>(47)</sup>. The DPD and e-privacy directive are wholly applicable to the RFID applications that process personal data <sup>(48)</sup>.

<sup>(45)</sup> See Article 1, 2 para., e-privacy directive.

<sup>(46)</sup> Radio-frequency identification (RFID) is a technology enabling the processing of personal data, including personal data. In particular RFID applications allow the processing of personal data stored on the tag (see Recital 4, RFID recommendation).

<sup>(47)</sup> See Article 2, RFID recommendation.

<sup>(48)</sup> See Recital 10, RFID recommendation.



## Directive 95/46/EC on data protection

### A general overview

The DPD provides a definition of personal data as any information related to a data subject (as an identified or identifiable natural person) and referring to physical, economic, cultural or mental factors. Any operation performed upon personal data, such as collection, storage or disclosure is a processing of personal data, the purpose and means of which are determined by the data controller that according to the law can be any natural or legal person, public authority, agency or any other body <sup>(49)</sup>.

Member States shall provide that personal data must be:

- ✓ Processed fairly and lawfully.
- ✓ Collected for specified, explicit and legitimate purposes and used accordingly.
- ✓ Appropriate and relevant in relation to the purpose for which they are processed.
- ✓ Accurate and kept up to date.
- ✓ Kept no longer than the time necessary for the purpose for which they are processed <sup>(50)</sup>.



Personal data can be processed if:

- ✓ The data subject has been adequately informed and has given unambiguously his consent for the collection and further use of his data.
- ✓ Processing is necessary to perform a contract having as a party the data subject or to enter into a contract requested by the data subject.
- ✓ A legal obligation requires the processing of personal data.

---

<sup>(49)</sup> See Article 2(a), (b) and (d) of the DPD. In practical terms a data controller can be, for example, a medical practitioner that would usually be the controller of the data processed on his clients or a company would be the controller of the data processed on its clients and employees.

<sup>(50)</sup> See Article 6, DPD.



- ✓ Processing data is necessary in order to ensure the essential interests of the data subject.
- ✓ Processing is necessary to perform tasks of public interests or carried out by an official authority.
- ✓ The data controller has a legitimate interest in processing the personal data of the data subject; this interest, however, has to be necessary balanced with the right to privacy of the data subject <sup>(51)</sup>.

The data subject has the right to <sup>(52)</sup>:

- ✓ Be informed of any processing of his data.
- ✓ Access data concerning him.
- ✓ Object to the processing on compelling and legitimate grounds.

### The household exemption

As provided in Article 3(2) of the directive, the obligations related to the processing of personal data do not apply in two specific circumstances:

- ✓ In any case of processing activities that fall inside the public security, defence or criminal law enforcement's areas that are not part of the competence of the EC and remain a national prerogative.
- ✓ In the course of a *purely* personal or household activity (i.e. the household exemption) <sup>(53)</sup>.

The scope of this last provision is further clarified by Recital 12 of the DPD which states that the processing of data carried out by a natural person in the exercise of activities which are *exclusively* personal or domestic, such as correspondence and the holding of records of addresses <sup>(54)</sup>, should be excluded from the protection principles of the directive.

---

<sup>(51)</sup> See Article 7, DPD.

<sup>(52)</sup> See Article 10 et seq., DPD.

<sup>(53)</sup> See Article 3, para. 2, DPD.

<sup>(54)</sup> See Recital 12, DPD.



The Court of Justice of the European Communities (CJ) expressed its position on the application of the household exemption in the *Lindqvist* case<sup>(55)</sup>. Mrs Lindqvist, a worker for a local Swedish parish, published on a web page, for religious purpose, information (such as name, last name, telephone number) of her parishioners without their consent. She was prosecuted for violation of the national law on personal data. The CJ found that the exemption provided by Article 3(2) of the directive could not be applicable since it is related 'only to activities which are carried out in the course of private and family life of individuals, which is not clearly the case with the processing of personal data consisting in publication on the Internet so that those data are made accessible to an indefinite number of people'<sup>(56)</sup>.

The case mentioned above has added another element in order to determine whether the household exemption should be applicable but at the same time it is not clear when the number of people, to which data are available, should be considered indefinite.

The issue is still open<sup>(57)</sup>.

### What can the data subject do in case of violation of his rights?

In each Member State one or more public authority should be responsible for ensuring the proper application of the DPD<sup>(58)</sup>.

<sup>(55)</sup> Court of Justice, Case C-101/01, Criminal proceedings against Bodil Lindqvist, OJ C 7, 10.1.2004.

<sup>(56)</sup> Court of Justice, Case C-101/01, Criminal proceedings against Bodil Lindqvist, OJ C 7, 10.1.2004, para. 47.

<sup>(57)</sup> Brendan Van Alsenoy, Joris Ballet et al., *Social networks and web 2.0: Are users also bound by data protection regulations?*, published online on 1 October 2009, available at <http://www.springerlink.com/content/u11161037506t68n/?p=3605a236b4e54d6f87bdcf40d6199825&pi=4> (last visited on 20 October 2009); Rebecca Wong, Joseph Savirimuthu, 'All or nothing: this is the question?: The application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet', John Marshall Journal of Computer & Information Law, Vol. 25, No 2, 2008, available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1003025#](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1003025#) (last visited on 20 October 2009).

<sup>(58)</sup> An overview of national data protection authorities is available at [http://ec.europa.eu/justice\\_home/fsj/privacy/nationalcomm/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm) (last visited on 21 October 2009).



The supervisory authority has investigative and effective power of intervention and, when the national provisions adopted in accordance with the directive have been violated, it has the power to engage in legal proceedings or to bring these violations to the attention of the judicial authority.

The data subject can submit his complaint to the supervisory authority, which must examine the claim and may temporarily prohibit the data processing. If the DPD has been violated then the supervisory authority can intervene by ordering to erase, destroy or ban in a definitive way the data processing. If the claim to the supervisory authority did not lead to a satisfactory result, the data subject, with the support of a legal adviser, can submit his case to the judgment of a court <sup>(59)</sup>.

### Data Protection Working Party

The Working Party is an independent European advisory body, set up under Article 29 of the directive, composed of data protection commissioners of each Member State, of a representative of the Commission and of a representative of the authority or authorities established for the Community institutions and bodies <sup>(60)</sup>.

The tasks of the Working Party are:

- ✓ Supporting the uniform application of the national measures adopted under the directive.
- ✓ Providing the European Commission with an opinion on the level of protection in the Community and third countries.



<sup>(59)</sup> 'Data protection in the European Union', online guide available at [http://ec.europa.eu/justice\\_home/fsj/privacy/guide/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/guide/index_en.htm) (last visited on 20 October 2009).

<sup>(60)</sup> The list of members of the Working Party is available at [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/members\\_en.htm#chairman](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/members_en.htm#chairman) (last visited on 21 October 2009).



- ✓ Advising the European Commission on any proposed amendment of the DPD, on any additional and specific measures to protect the rights and freedoms of natural persons regarding the processing of personal data.
- ✓ Giving an opinion on codes of conduct drawn up at Community level.

Moreover, the Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community <sup>(61)</sup>.

## Data Protection Working Party Opinion 5/2009

### Social network providers under the lens of the directive

In June 2009, the Working Party issued an opinion on online social networking <sup>(62)</sup> (the 'Opinion'), aiming to provide SNS providers with guidance on the technical and organisational measures to adopt in order to comply with the European data protection legislation. According to the Opinion, the provisions of the directive apply to SNS providers in most cases, even if their headquarters are located outside of the European Economic Area.

#### SNS providers as data controllers

SNS providers are data controllers under the directive since they determine the purposes and means of personal data by providing the tools and services related to user management. According to Article 10 of the

---

<sup>(61)</sup> See Article 30(1) and (3) of the DPD.

<sup>(62)</sup> Article 29 — Data Protection Working Party — Opinion 5/2009 on online social networking, 12.6.2009, available at [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2009\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm) (last visited on 21 October 2009).



directive, SNS providers should make users aware of their identity and of the different purposes for which they process personal data. In particular the Working Party recommends SNS providers to:

- ✓ Make aware SNS users about the privacy risks to themselves and to others when they upload information on the SNS.
- ✓ Remind SNS users that uploading information about other individuals may violate their privacy.
- ✓ Advise SNS users on the fact that uploading pictures or information about other individuals should be done with the individual's consent.
- ✓ Offer privacy-friendly default settings, which allow users to specifically and freely consent to any access to their profile's content that is beyond their self-selected contacts in order to reduce the risk of unlawful processing by third parties.
- ✓ Provide the SNS's homepage with a link to a complaint facility, for any data protection issues.
- ✓ Delete personal data provided by a user when he registers on an SNS as soon as either the user or the SNS provider decides to delete the account; moreover, when a user decides not to use the service for a defined period of time, the profile should be set to inactive.

### SNS users as data subjects

Users, in most cases, are considered data subjects, as far as their activities on an SNS are carried out in the course of a purely personal or household activity. In fact, generally speaking, their activities are covered by the household exemption that allows them not to comply with the obligations provided for a data controller. As a consequence users have the right to be informed of any processing of their data, to access them or to object to a specific data processing. The Opinion also stresses the importance of allowing users to use a pseudonym instead of their real identity. SNSs may need, to register a user, some personal data but still do not need to publish the real names of members on the Internet since security measures to protect personal data, such as authentication mechanisms, can still be implemented with the usage of a pseudonym.



## Applicability of the directive to non-EU based social networks

The connecting criteria for the application of the national legislation adopted according to the directive are set out in Article 4 of the DPD which provides that the data protection laws of the Member States shall apply when:

- ✓ The data controller is established in the territory of a Member State.
- ✓ The data controller is not established in the territory of a Member State but in a place where its national law applies, according to international public law.
- ✓ The data controller is located outside the European Community but makes use of equipment located in the territory of a Member States for processing personal data.



The use of equipment for processing personal data is considered a decisive element for the application of the directive. The degree of disposal given to the data controller over the equipment that triggers the application of the DPD is the one that allows him to determine the purpose and the procedure of data processing <sup>(63)</sup>. The use of cookies <sup>(64)</sup> and similar software devices by an online social service provider can also be seen as the use of equipment in the Member State's territory, thus invoking that Member State's data protection law <sup>(65)</sup>. In Europe, many of the best-

<sup>(63)</sup> Article 29 — Data Protection Working Party — Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites, 30.5.2002, available at [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2002\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2002_en.htm) (last visited on 22 October 2009).

<sup>(64)</sup> Cookies are pieces of data created by a web server that can be stored in text files that may be put on the Internet user's hard disk, while a copy may be kept by the website.

<sup>(65)</sup> Article 29 — Data Protection Working Party — Opinion 1/2008 on data protection issues related to search engines, of 4.4.2008, available at [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2008\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm) (last visited on 22 October 2009).





known US-based social networks, such as Myspace<sup>(66)</sup>, Facebook<sup>(67)</sup>, LinkedIn<sup>(68)</sup> and Twitter<sup>(69)</sup>, use cookies. The Working Party states<sup>(70)</sup> therefore that the national law of Member States, where the user's personal computer is located, applies to the question under what conditions his personal data may be collected by placing cookies on his hard disk<sup>(71)</sup>. Based on this consideration the Working Party has concluded that the directive should be applicable to non-EU based social networks.

## Is the SNS user responsible for compliance with the directive?

The responsibility for the unlawful processing of third-party data may lie with the user himself according to Member States' criminal and civil law provisions (i.e. defamation, penal liability, right of personal portrayal, etc.). However, at this point, some considerations and evaluations have been made by researchers and scholars in order to understand if and to what extent the data-processing operations carried out by an SNS user could be considered subject to the directive.

<sup>(66)</sup> Myspace privacy policy available at <http://www.myspace.com/index.cfm?fuseaction=misc.privacy> (last visited on 22 October 2009).

<sup>(67)</sup> Facebook privacy policy available at <http://www.facebook.com/policy.php> (last visited on 22 October 2009).

<sup>(68)</sup> LinkedIn privacy policy available at [http://www.linkedin.com/static?key=privacy\\_policy#priority](http://www.linkedin.com/static?key=privacy_policy#priority) (last visited on 22 October 2009).

<sup>(69)</sup> Twitter privacy policy available at <https://twitter.com/privacy> (last visited on 22 October 2009).

<sup>(70)</sup> Article 29 — Data Protection Working Party — Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites, 30.5.2002, available at [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2002\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2002_en.htm) (last visited on 22 October 2009).

<sup>(71)</sup> For a deeper analysis see Aleksandra Kuczerawy, *Facebook and its EU Users — Applicability of the EU Data Protection Law to US Based SNS*, in Bezzi M., Duquenoy P., Fischer-Hübner S., Hansen M. (eds.), *Post-Summer School Proceedings of the IFIP/PrimiLife Summer School on 'Privacy and Identity Management for Life'*, Nice, France, 7-11 September, Springer-Verlag (2010, forthcoming).



## SNS users as data controllers

Based on the definition provided by Article 2(d) of the directive a data controller is:

‘the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the *purpose* and *means* <sup>(72)</sup> of processing of personal data [...]’.

In order to qualify a user as a data controller it is necessary to analyse what the purpose and means of data processing available to an SNS user are and what decision-making power he has with regards to both <sup>(73)</sup>. As in most cases the purpose of SNS providers is economic, since they generate much of their revenue through advertising and marketing <sup>(74)</sup>. For the SNS user, the main aim is entertainment, such as interacting with friends or meeting new people. In some cases, for example when a business-oriented social network is chosen, such as LinkedIn, the purpose can be related to business and career opportunities. In any case the scope of data-processing operations is chosen freely by the user when he decides to access a specific social network.

The major features and settings of an SNS are provided and set up unilaterally by the SNS provider, which decides how to carry out the data processing. In this context, as it has been observed <sup>(75)</sup>, a small margin of decision-making power still remains with the user regarding the means by which the data are processed. The user in fact can still decide, when

<sup>(72)</sup> Emphasis added.

<sup>(73)</sup> Brendan Van Alsenoy, Joris Ballet et al., *Social networks and web 2.0: are users also bound by data protection regulations?*, published online on 1 October 2009, available at <http://www.springerlink.com/content/u11161037506t68n/?p=3605a236b4e54d6f87bdcf40d6199825&pi=4> (last visited on 20 October 2009).

<sup>(74)</sup> Article 29 — Data Protection Working Party — Opinion 5/2009 on online social networking, 12.6.2009, available at [http://ec.europa.eu/justice/fsj/privacy/workinggroup/wpdocs/2009\\_en.htm](http://ec.europa.eu/justice/fsj/privacy/workinggroup/wpdocs/2009_en.htm) (last visited on 21 October 2009).

<sup>(75)</sup> Brendan Van Alsenoy, Joris Ballet et al., *Social networks and web 2.0: are users also bound by data protection regulations?*, published online on 1 October 2009, available at <http://www.springerlink.com/content/u11161037506t68n/?p=3605a236b4e54d6f87bdcf40d6199825&pi=4> (last visited on 20 October 2009).



accessing an SNS, what information to upload and by which means among the ones available and, as a consequence, it could be stated that he only acts as a controller 'with regards to the content he chooses to provide and the processing operations he initiates' <sup>(76)</sup>.

This statement does not exclude the margin for the application of the household exemption, which still remains the most questionable point. As described above, the exemption provided by Article 3(2) of the DPD should not be applicable any time the data entrusted to the Internet are made available to an indefinite number of people. Considering nevertheless that no further elements are provided by the law or jurisprudence, regarding the applicability of Article 3(2) of the DPD, it could be argued that at least those SNS users who choose a public setting for their account fall within the scope of the directive. In fact, in general, private profiles are only accessible to those with whom a connection is shared but even in this case 'a large private public' could access the data uploaded <sup>(77)</sup>.

---

<sup>(76)</sup> Brendan Van Alsenoy, Joris Ballet et al., *Social networks and web 2.0: are users also bound by data protection regulations?*, published online on 1 October 2009, available at <http://www.springerlink.com/content/u11161037506t68n/?p=3605a236b4e54d6f87bdcf40d6199825&pi=4> (last visited on 20 October 2009).

<sup>(77)</sup> Brendan Van Alsenoy, Joris Ballet et al., *Social networks and web 2.0: are users also bound by data protection regulations?*, published online on 1 October 2009, available at <http://www.springerlink.com/content/u11161037506t68n/?p=3605a236b4e54d6f87bdcf40d6199825&pi=4> (last visited on 20 October 2009).



## Consequences deriving from the qualification of SNS users as data controllers

The implication deriving from the qualification of an SNS user as a data controller is to ensure that his processing activities are carried out in accordance with the main provisions of the directive <sup>(78)</sup>, such as:

- ✓ The criteria set forth in Article 7 for making the data processing legitimate (such as obtaining the unambiguous consent of the individual to whom the data are related, necessary processing, etc.).
- ✓ The rights of the data subject to obtain information (Article 10), to access data (Article 12), to object (Article 14).
- ✓ The confidentiality and security of processing as set forth in Articles 16 and 17.

This framework basically defines what the liability of the SNS user as a data controller should be towards data subjects in case of breaching data protection principles.

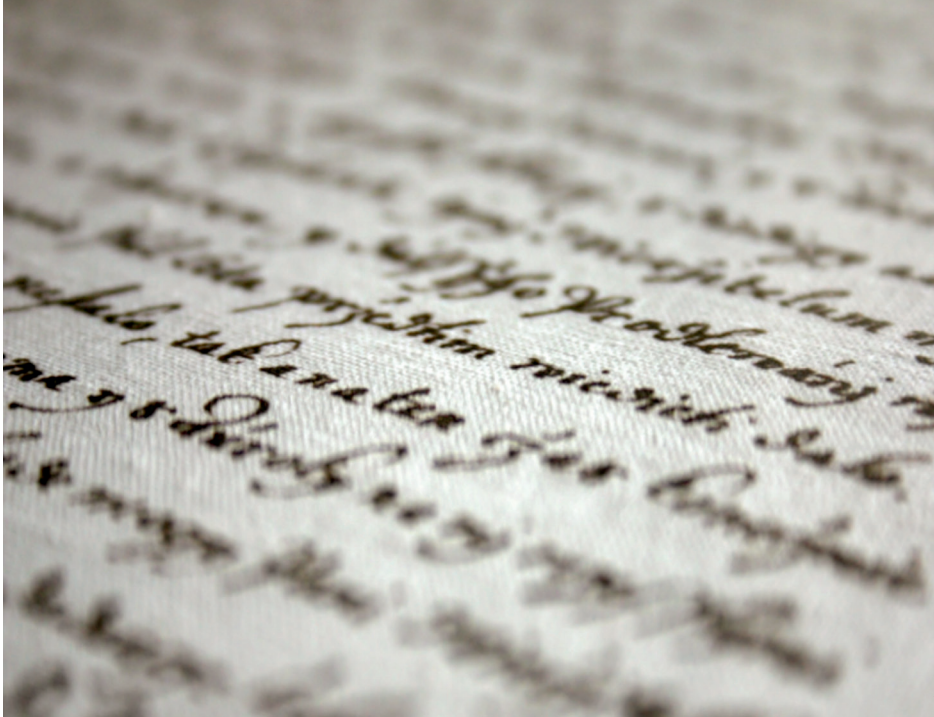
Considering the extraordinary development of social networks and the increasing number of users involved in social networking activities, it is evident that the evaluations and considerations above underline the necessity for a legislative review and interpretation to clarify this grey-area such as the responsibility of data controllers who are not legal persons. The SNS users' activities should be clearly regulated for example by setting a limit on the collection of personal data over which natural persons become subject to the provision of data protection legislation <sup>(79)</sup>.

---

<sup>(78)</sup> Rebecca Wong, *Social networking: Anybody is a data controller*, posted online on 23 September 2008, last revised on October 3, 2008 available at [http://papers.ssrn.com/sol3/cf\\_dev/AbsByAuth.cfm?per\\_id=653673](http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=653673) (last visited on 23 October 2009).

<sup>(79)</sup> ENISA, *Presentation to the LIBE Committee of the European Parliament. How to strengthen the EU legislation, improve international cooperation and secure the growing market of internet service*, 2008, available at <http://www.enisa.europa.eu/act/it/library/pp/eu-leg>

# PART 5 – GOLDEN RULES



## Golden rules

These safety tips draw on analysis of data and available research. This section is intended to provide, in one convenient place, recommendations to raise awareness about the risks and threats related to the misuse of social networks, in particular when accessed through mobile phone, with advice on how to avoid unwanted consequences.

Category	No	Recommendations	Description
Pay attention to what you post and upload	1	Consider carefully which images, videos and information you choose to publish	Remember that a social network is a public space; only post information or upload images you are comfortable with, keeping in mind that at a later stage you might be confronted with the content you uploaded, e.g. in a job interview. Information and pictures you post online should be considered permanent. They can be copied and stored by other individuals and can resurface years later in search engines.
	2	Never post sensitive information	Do not make information such as address, date of birth or financial data available in your profile. A criminal might access your profile and steal your identity.
	3	Use a pseudonym	You do not need to use your real name in an online profile. Using a nickname can help you protect your identity and privacy; only close contacts will know who is behind the nickname.

>>>

Category	No	Recommendations	Description
Choose your friends with care	4	Do not accept friend requests from people you do not know	Be selective about who you accept as a friend on a social network. You do not have to feel obliged to add someone to your friends' list. Politely refuse or simply ignore the request.
	5	Verify all your contacts	Ensure that the people you are in contact with or who sent a friend request are really who they say they are. Do not trust them immediately.
Protect your work environment and avoid reputation risk	6	When joining a social networking site use your personal e-mail address	Do not use your company e-mail address but your private one and do not post confidential or competitive information about your organization. Be careful about the information you reveal about your workplace, for example do not post pictures shot in front of your office with the company's address or logo on the background that may lead to your job or workplace address.
	7	Be careful how you portray your company or organisation online	Consider what your employer would think before posting any comments or material online about your company or organisation.
	8	Do not mix your business contacts with your friend contacts	You have no control over what your friends may post online or how they may portray you and consequently what your employer, colleagues and clients may be exposed to.

>>>

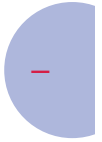
Category	No	Recommendations	Description
Protect your mobile phone and the information saved on it from any physical intrusion	9	Do not let anyone see your profile or personal information without your consent	Before accessing your profile through your mobile phone pay attention to the environment and people that are surrounding you. If someone is trying to see what you are doing access your profile in a safer place.
	10	Do not leave your mobile phone unattended	Someone with malicious intent could update your profile and status with false details. Remember to log out from the social network once your navigation is over and not to allow the social network to remember your password (this function is called 'Auto-complete').
	11	Do not save your password on your mobile phone	Mobile phones can be easily lost or stolen and if you save your password on your mobile device anyone who may have possession of it can access your profile, see your pictures and friends. Try to commit your password to memory and if you write it down be careful where you store it.
	12	Use the security features available on your mobile phone	Remember to lock the keypad when not in use and to protect the device with a PIN or a password. Backup your details to another device such a PC in case your mobile phone is lost or stolen. Configure connections (such as Bluetooth and Wi-fi), especially in airports and public spaces, to be secure and if your mobile device has a built in firewall remember to enable it.

>>>





Category	No	Recommendations	Description
Respect other people's privacy	13	Be careful what you publish about someone else	Do not upload pictures or personal information regarding other people without their consent. You might commit a criminal offence.
Inform yourself	14	Read carefully and in full the privacy policy and the conditions and terms of use of the social network you choose	Always be informed about who provides the service and how your personal information will be used and who has the right to access the information you post.
Protect your privacy with the privacy settings	15	Use privacy-oriented settings	Set the profile privacy level properly. Check the privacy settings of your profile — who can see your pictures, who can contact you and who can add comments in order to avoid making your profile available to everyone.
Report immediately lost or stolen mobile	16	Be careful when using your mobile phone and pay attention to where you put it	Report immediately stolen or lost mobile phone with contacts and pictures saved in its memory and personal information regarding you and your friends (e.g. those friends whose contacts on the SNS have been synchronized with the mobile phone) and change the passwords on the social networks you are a member of.
Pay attention to the location based services and information of your mobile phone	17	Deactivate location based services when not using them.	Remember to deactivate location based features of your mobile phone if you don't need them.



## Conclusions

The huge potential of mobile social networks in the immediate future let us imagine the enormous benefits that everyone could get from the integration of mobility, always-on connectivity, and social networking services. Such a reality could be a great advantage for lifelong learning, community living, and knowledge-sharing but, as boundaries between public and private spaces will blur, also new risk scenarios will emerge. Companies should assure that their staff members understand and explicitly accept the security and privacy requirements of the organization they work for. Employees should be educated to understand that the information placed in web profiles or in twitter streams may be misused by others looking for important facts and figures and may cause damage to the company's reputation and to their carrier. Every user should be aware of the fact that the information they entrust to an SNS are linked to their real identity, thus exposing them and eventually their friends to the risk and threat scenarios described in this paper.

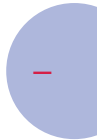
The conducted analysis showed that many of the privacy issues originating from the web-based access to SNSs also apply to MSNs but there are also a number of unique risks and threats against MSNs. The real-time spread of information and data through social mobile can cause serious damage that can affect private and working environment, a lost or stolen mobile phone can cause the loss of important data, contacts, pictures, personal details and access codes, threatening the user's privacy and the one of his friends whose contacts on the SNS have been synchronized with the mobile phone.

Awareness raising and information security empowerment is the first line of defence and the first security measure related to private and working environment. ENISA hopes that this paper will provide social mobile users with a valuable tool to understand the risks and threats scenario arising from the usage of social mobile and the related privacy issues, also providing a set of recommendations for raising awareness of users.



## Acronyms

<b>CJ</b>	Court of Justice of the European Communities
<b>DPD</b>	Directive 95/46/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector
<b>MSN</b>	Mobile social network
<b>RFID</b>	Radio Frequency Identification
<b>SNS</b>	Social networking site



## References and sources for further reading

20minutes.es, *Rajoy, Lucía Etxebarria o José Mota, suplantados en las redes sociales*, 6 July 2009, <http://www.20minutos.es/noticia/477404/0/internet/identidades/falsas/> (last visited on 9 November 2009).

20minutes.fr, *La RATP ouvre une enquête sur une vidéo d'agression dans un bus*, 7 April 2009, <http://www.20minutes.fr/article/318507/France-La-RATP-ouvre-une-enquete-sur-une-video-d-agression-dans-un-bus.php> (last visited on 9 November 2009).

Aleksandra Kuczerawy, *Facebook and its EU Users — Applicability of the EU Data Protection Law to US Based SNS*, in Bezzi M., Duquenoy P., Fischer-Hübner S., Hansen M. (eds.), *Post-Summer School Proceedings of the IFIP/PrimeLife Summer School on 'Privacy and Identity Management for Life'*, Nice, France, 7-11 September, Springer-Verlag (2010, forthcoming).

Alessandro Acquisti, Ralph Gross, *Imagined Communities: Awareness, Information sharing, and Privacy on the Facebook*, 12 December 2006, available at <http://www.springerlink.com/content/gx00n8nh88252822/?p=62d211a0d9c94b26bf709f93ddf44781&pi=0> (last visited on 19 November 2009).

Alexander Gostev, Denis Maslennikov, *Mobile malware evolution: An overview, Part 3*, 29 September 2009, available at <http://www.viruslist.com/en/analysis?pubid=204792080> (last visited on 9 November 2009)

Alexander Richter and Michael Koch, *Functions of social networking services*, in: *Proceedings of the 8th International Conference on the Design of Cooperative Systems*, Carry-le-rouet, France, Institut d'Etudes Politiques d'Aix-en-Provence, 2008, available at <http://www.kooperationssysteme.de/docs/pubs/RichterKoch2008-coop-sns.pdf> (last visited on 5 November 2009).

Art.29-Data Protection Working Party – *Opinion 1/2008 on data protection issues related to search engines*, of 04.04.2008 available at [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2008\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm) (last visited on 19 November 2009).

Art.29-Data Protection Working Party – *Opinion 4/2007 on the concept of personal data*, of 20.06.2007 available at [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2007\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm) (last visited on 19 November 2009).



Article 29 — Data Protection Working Party — *Opinion 1/2008 on data protection issues related to search engines*, of 4.4.2008, available at [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2008\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm) (last visited on 22 October 2009).

Article 29 — Data Protection Working Party — *Opinion 5/2009 on online social networking*, 12.6.2009, available at [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2009\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm) (last visited on 21 October 2009).

Article 29 — Data Protection Working Party — *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites*, 30.5.2002, available at [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2002\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2002_en.htm) (last visited on 22 October 2009).

AVG, *Bringing social security to the online community*, 26 August 2009, available at [www.avg.com.au/files/media/avg\\_socialsecurity\\_2009-08-26\\_au.pdf](http://www.avg.com.au/files/media/avg_socialsecurity_2009-08-26_au.pdf) (last visited on 19 November 2009).

Bernardo A. Huberman, Daniel M. Romero, Fang Wu, *Social networks that matter: Twitter under the microscope*, December 12 2008, available at <http://www.hpl.hp.com/research/scl/papers/twitter/> (last visited on 19 November 2009).

Blitz quotidiano, *Facebook, diffamazione contro una donna: indagati tutti i 67 Marco Girardi iscritti al network*, 6 September 2009, available at <http://www.blitzquotidiano.it/tag/marco-girardi/> (last visited on 1 November 2009).

Brendan Van Alsenoy, Joris Ballet et al., *Social networks and web 2.0: Are users also bound by data protection regulations?*, published online on 1 October 2009, available at <http://www.springerlink.com/content/u1161037506t68n/?p=3605a236b4e54d6f87bdcf40d6199825&pi=4> (last visited on 20 October 2009).

Charter of Fundamental Rights of the European Union, OJ C 364/1, 18.12.2000.

CNN.com, *Smartphone security threats likely to rise*, 29 October 2009, available at <http://edition.cnn.com/2009/TECH/10/25/smartphone.security/index.html> (last visited on 19 November 2009).



*Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification*, OJ L 122, 16.5.2009.

comScore press release, 15 April 2009, available at [http://www.comscore.com/layout/set/popup/Press\\_Events/Press\\_Releases/2009/4/Facebook\\_Top\\_Social\\_Network\\_in\\_Spain](http://www.comscore.com/layout/set/popup/Press_Events/Press_Releases/2009/4/Facebook_Top_Social_Network_in_Spain) (last visited on 5 November 2009).

comScore press release, 17 February 2009, available at [http://www.mediatrix.com/Press\\_Events/Press\\_Releases/2009/2/Social\\_Networking\\_France](http://www.mediatrix.com/Press_Events/Press_Releases/2009/2/Social_Networking_France) (last visited on 5 November 2009).

Corriere della sera.it, *Critiche all'azienda online, Licenziata per Facebook*, 21 May 2009, available at [http://milano.corriere.it/milano/notizie/cronaca/09\\_maggio\\_21/licenziata\\_facebook\\_critiche\\_azienda-1501380122088.shtml](http://milano.corriere.it/milano/notizie/cronaca/09_maggio_21/licenziata_facebook_critiche_azienda-1501380122088.shtml) (last visited on 9 November 2009).

Corriere della sera.it, *Pazienti intubati su Facebook, il Garante avvia un'istruttoria*, 14 May 2009, available at [http://www.corriere.it/cronache/09\\_maggio\\_14/garante\\_ospedale\\_udine\\_dc70f560-409b-11de-aa9a-00144f02aabc.shtml](http://www.corriere.it/cronache/09_maggio_14/garante_ospedale_udine_dc70f560-409b-11de-aa9a-00144f02aabc.shtml) (last visited on 9 November 2009).

Court of Justice, Case C-101/01, *Criminal proceedings against Bodil Lindqvist*, OJ C 7, 10.1.2004.

*Data protection in the European Union*, online guide available at [http://ec.europa.eu/justice\\_home/fsj/privacy/guide/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/guide/index_en.htm) (last visited on 20 October 2009).

Deloitte, *Losing Ground -2009 TMT Global Security Survey, Key findings*, 2 June 2009, available at [http://www.deloitte.com/view/en\\_US/us/Industries/MediaEntertainment/article/e510f6b085912210VgnVCM10000ba42f00aRCRD.htm](http://www.deloitte.com/view/en_US/us/Industries/MediaEntertainment/article/e510f6b085912210VgnVCM10000ba42f00aRCRD.htm) (last visited on 19 November 2009).

Deloitte, *Social networking and reputational risk in the workplace*, 28 May 2009, available at [http://www.deloitte.com/view/en\\_US/us/About/EthicsIndependence/article/8aa3cb51ed812210VgnVCM10000ba42f00aRCRD.htm](http://www.deloitte.com/view/en_US/us/About/EthicsIndependence/article/8aa3cb51ed812210VgnVCM10000ba42f00aRCRD.htm) (last visited on 19 November 2009).

*Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector*, OJ L 201, 31.7.2002.



*Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281, 23.11.1995.

EESC, *Opinion On The Impact of Social Networking Sites on Citizens*, September 23 2009, available at <http://www.edri.org/edri-gram/number7.18/eesc-social-networking-websites> (last visited on 19 November 2009).

Electronic Privacy information Center available at the website <http://epic.org/privacy/facebook/> (last visited on 5 November 2009).

elmundo.es, *Burlas y venganzas circulan por la Red detrás de identidades falsa*, 7 July 2009, available at <http://www.elmundo.es/elmundo/2009/07/05/navegante/1246809687.html> (last visited on 9 November 2009).

eMarketer, April 2008, available at [http://www.emarketer.com/Report.aspx?code=emarketer\\_2000489](http://www.emarketer.com/Report.aspx?code=emarketer_2000489) (last visited on 2 November 2009).

ENISA, *Security issues in the context of authentication using mobile devices (Mobile eID)*, 2008, available at [http://www.enisa.europa.eu/act/it/eid/mobile-eid/?searchterm=security issues mobile devices](http://www.enisa.europa.eu/act/it/eid/mobile-eid/?searchterm=security+issues+mobile+devices)

ENISA, *Presentation to the LIBE Committee of the European Parliament. How to strengthen the EU legislation, improve international cooperation and secure the growing market of internet service*, 2008, available at <http://www.enisa.europa.eu/act/it/library/pp/eu-leg>

ENISA, *Security Issues and Recommendations for Online Social Networks*, 2007, available at <http://www.enisa.europa.eu/act/it/oar/social-networks/security-issues-and-recommendations-for-online-social-networks>

ENISA, *Technology-induced challenges in Privacy & Data Protection in Europe*, 2008, available at [http://www.enisa.europa.eu/act/rm/files/deliverables/technology-induced-challenges-in-privacy-data-protection-in-europe/?searchterm=technology in](http://www.enisa.europa.eu/act/rm/files/deliverables/technology-induced-challenges-in-privacy-data-protection-in-europe/?searchterm=technology+in)

ESET, *Global Threats Trends – September 2009*, available at [http://www.eset.com/threat-center/threat\\_trends/Global\\_Threat\\_Trends\\_September\\_2009.pdf](http://www.eset.com/threat-center/threat_trends/Global_Threat_Trends_September_2009.pdf) (last visited on 19 November 2009).

Facebook press room, statistics available at <http://www.facebook.com/press/info.php?statistics> (last visited on 5 October 2009).

Facebook privacy policy available at <http://www.facebook.com/policy.php> (last visited on 22 October 2009).



Graham Cluley, *Social networks: The new frontier for Malware, Spam and Identity Theft*, ICT Forum 2009 Conference, 15 July, available at <http://www.ictf.ox.ac.uk/conference/2009/programme.html#Plenary3> (last visited on 19 November 2009).

Hanna Krasnova, Oliver Günther, Sarah Spiekermann, Ksenia Koroleva, *Privacy concerns and identity in online social networks*, published online 1 October 2009, available at <http://www.springerlink.com/content/1371174132178uwmm/?p=ef2d38c4f2ce4bd78341b65ed1ccd940&pi=1> (last visited on 19 November 2009).

ICT Statistics Newslog, *Email and Social Networking Most Popular Mobile Internet Activities*, 15 May 2009, available at <http://www.itu.int/ITU-D/ict/newslog/Email+And+Social+Networking+Most+Popular+Mobile+Internet+Activities.aspx> (last visited on 19 November 2009).

Il Corriere del mezzogiorno, *La camorra di Pomigliano cerca adepti: gruppo su Facebook fondato da giovani*, 28 September 2009, available at <http://corrieredelmezzogiorno.corriere.it/notizie/cronaca/2009/28-settembre-2009/camorra-pomigliano-cerca-adepti-il-gruppo-facebook-giovani-is-critti-1601817500073.shtml> (last visited on 2 November 2009).

InfoWorld, *Hackers put social networks such as Twitter in crosshairs*, 17 August 2009, available at [http://www.infoworld.com/d/security-central/hackers-put-social-networks-such-twitter-in-crosshairs-832?source=IFWNLE\\_nlt\\_sec\\_2009-08-17](http://www.infoworld.com/d/security-central/hackers-put-social-networks-such-twitter-in-crosshairs-832?source=IFWNLE_nlt_sec_2009-08-17) (last visited on 19 November 2009).

INTECO, *Study on the privacy of personal data and on the security of information in social networks*, February 2009, available at [http://www.inteco.es/Security/Observatory/Publications/Studies\\_and\\_Reports/estudio\\_re-des\\_sociales\\_en](http://www.inteco.es/Security/Observatory/Publications/Studies_and_Reports/estudio_re-des_sociales_en) (last visited on 24 November 2009).

INTECO, *Security in twitter clients*, November 2009, available at [http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert\\_inf\\_est\\_twitter\\_clients\\_securityen.pdf](http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_est_twitter_clients_securityen.pdf) (last visited on 7 January 2010).

Italian Data Protection Authority press release, available at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1614095> (last visited on 9 November 2009).

Italian Data protection Authority, *Social network: watch out for side effects*, May 2009, available at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1614258> (last visited on 9 November 2009).





Joseph Bonneau, Sören Preibusch, *The privacy jungle: On the market for data protection in social networks*, Eighth Workshop on the Economics of Information Security (WEIS 2009), 24–25 June 2009, available at <http://weis09.infosecon.net/files/156/index.html> (last visited on 5 November 2009).

Juniper Research, *Mobile advertising, because I'm worth it*, extract from *Mobile advertising delivery channels, strategies & forecasts 2008-2013*, 2008, available at [http://www.c2mweb.eu/files/Whitepaper\\_Mobile\\_Advertising.pdf](http://www.c2mweb.eu/files/Whitepaper_Mobile_Advertising.pdf) (last visited on 30 November 2009).

La Repubblica.it, Turin, *Taroccatto su Facebook il profilo del Professore*, 7 May 2009, available at <http://torino.repubblica.it/dettaglio/taroccatto-su-facebook-il-profilo-del-professore/1629649> (last visited on 9 November 2009).

La Stampa.it, *Facebook—Hospital infermiera fotografa sospesa 10 giorni le molinette: non prendera' lo stipendio il primo provvedimento disciplinare*, 9 January 2009, available at [http://archivio.lastampa.it:80/LaStampaArchivio/main/History/tmpl\\_viewObj.jsp?objid=9011456](http://archivio.lastampa.it:80/LaStampaArchivio/main/History/tmpl_viewObj.jsp?objid=9011456) (last visited on 10 November 2009).

La Stampa.it, *Facebook, rubata l'identita' a un Professore di Trento*, 5 January 2009 available at [http://www.lastampa.it/\\_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID\\_blog=30&ID\\_articolo=5580&ID\\_sezione=38&sezione=News](http://www.lastampa.it/_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=5580&ID_sezione=38&sezione=News) (last visited on 26 November 2009).

La Voce del Nord Est, Udine, *Infermiera carica su Facebook le foto dei pazienti intubati*, 14 May 2009, available at <http://www.lavocedelnordest.it/articoli/2009/05/14/2023/udine-infermiera-carica-su-facebook-le-foto-dei-pazienti-intubati> (last visited on 9 November 2009).

LaStampa.it, *Infermieri e medici pazzi di Facebook*, 6 January 2009, available at <http://www.lastampa.it/multimedia/multimedia.asp?p=38&pm=&Dmsezione=14&IDalbum=14701&tipo=FOTOGALLERY#mpos> (last visited on 19 November 2009).

Libération.fr, *Un policier soupçonné d'avoir diffusé la vidéo de l'agression dans un bus*, 8 April 2009, available at <http://www.liberation.fr/societe/0101560932-agression-dans-un-bus-la-police-des-polices-saisie> (last visited on 9 November 2009).

LinkedIn privacy policy available at [http://www.linkedin.com/static?key=privacy\\_policy#pri-top](http://www.linkedin.com/static?key=privacy_policy#pri-top) (last visited on 22 October 2009).



List of members of the Working Party, available at [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/members\\_en.htm#chairman](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/members_en.htm#chairman) (last visited on 21 October 2009).

MailOnline, *Second investigation launched after BA check-in staff post comments about 'smelly' passengers on Facebook*, 3 November 2008, available at <http://www.dailymail.co.uk/news/article-1082437/BA-check-staff-post-comments-smelly-passengers-Facebook.html> (last visited on 11 November, 2009).

MailOnline, *Teacher is suspended for jibe on Facebook about her class*, 1 August 2009, available at <http://www.dailymail.co.uk/news/article-1202210/Teacher-suspended-jibe-Facebook-class.html> (last visited on 26 November 2009).

Mariano Rajoy and Lucía Extebarrias's forged profiles available at <http://twitter.com/marianorajoy> and <http://twitter.com/luciaetxebarria> (last visited on 9 November 2009).

Martin Pekárek, Ronald Leenes, *Privacy and Social Network Sites: Follow the Money!* January 15-16, 2009, available at [www.w3.org/2008/09/msnws/papers/tilt.pdf](http://www.w3.org/2008/09/msnws/papers/tilt.pdf) (last visited on 24 November 2009).

Martin Pekárek, Stefanie Pöttsch, *A comparison of privacy issues in collaborative workspaces and social networks*, published online 28 July 2009, available at <http://www.springerlink.com/content/g54qk93430581554/?p=dae26d8123004cfc88e5004aa1aba269&pi=0> (last visited on 5 November 2009).

Mashable, *The social media guide, Exploring best practices for building and monetizing mobile social networks*, 3 October 2008, available at <http://mashable.com/2008/10/03/mobile-social-networking/> (last visited on 30 November 2009).

Myspace privacy policy available at <http://www.myspace.com/index.cfm?fuseaction=misc.privacy> (last visited on 22 October 2009).

news.bbc.co.uk, *Payout for false Facebook profile*, 24<sup>th</sup> July 2008, available at [http://news.bbc.co.uk/2/hi/uk\\_news/7523128.stm](http://news.bbc.co.uk/2/hi/uk_news/7523128.stm) (last visited on 16 November 2009).

Nick Lane, Nicky Walton-Flynn, Freda Benlamlih (Informa Telecoms & Media), *Mobile social networking*, July-September 2008 – available at [http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno\\_final-fmt-nl-3110-f.pdf](http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt-nl-3110-f.pdf) (last visited on 18 November 2009).



Overview of national data protection authorities, available at [http://ec.europa.eu/justice\\_home/fsj/privacy/nationalcomm/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm) (last visited on 21 October 2009).

*Privacy setting for social networks*, available at <http://blog.safetyclicks.com/2008/09/03/social-networks-and-privacy-settings/> (last visited on 5 November 2009).

Rebecca Wong, Joseph Savirimuthu, *All or nothing: this is the question?: The application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet*, John Marshall Journal of Computer & Information Law, Vol. 25, No 2, 2008, available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1003025#](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1003025#) (last visited on 20 October 2009).

Rebecca Wong, *Social networking: Anybody is a data controller*, posted online on 23 September 2008, last revised on October 3, 2008 available at [http://papers.ssrn.com/sol3/cf\\_dev/AbsByAuth.cfm?per\\_id=653673](http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=653673) (last visited on 23 October 2009).

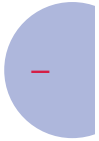
SafeLine Greek Hotline, website available at [www.safeline.gr](http://www.safeline.gr)

SearchSecurity.com, *Kaspersky system analyzes malicious URLs on Twitter for malware*, 29 October 2009, available at [http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180\\_gci1372955,00.html](http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180_gci1372955,00.html) (last visited on 19 November 2009).

Status of implementation of the DPD in each Member State available at [http://ec.europa.eu/justice\\_home/fsj/privacy/law/implementation\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm) (last visited on 20 October 2009).

Telegraph.co.uk, *Man sues friend over fake Facebook profile*, 1 July 2008, available at <http://www.telegraph.co.uk/news/2226803/Man-sues-friend-over-fake-Facebook-profile.html> (last visited on 16 November 2009).

The daily bit, *Un fenomeno chiamato mobile social networking*, September 2008, available at <http://www.thedailybit.net/index.php?method=section&action=zoom&id=2489> (last visited on 18 November 2009) and Lastampa.it, *In Europa il social network piace sul cellulare*, August 2008, available at [http://www.lastampa.it/\\_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID\\_blog=30&ID\\_articolo=5054&ID\\_sezione=38&sezione=News](http://www.lastampa.it/_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=5054&ID_sezione=38&sezione=News) (last visited on 18 November 2009).



The Nielsen Company, *Global faces and networked places*, March 2009, available at <http://blog.nielsen.com/nielsenwire/nielsen-news/social-networking-new-global-footprint/> (last visited on 5 October 2009).

The Nielsen Company, *Mobile media nei mercati emergenti e in Italia*, IAB Seminar, 16 July 2008, available at <http://www.iabseminar.it/video.aspx?IDSessione=12> (last visited on 5 November 2009).

The Nielsen Company, *To Mobile or Not to Mobile*, 15 September 2009, available at [en-us.nielsen.com/etc/medialib/nielsen\\_dotcom/en\\_us/documents/pdf/webinars.Par.81596.File.pdf](http://en-us.nielsen.com/etc/medialib/nielsen_dotcom/en_us/documents/pdf/webinars.Par.81596.File.pdf) (last visited on 19 November 2009).

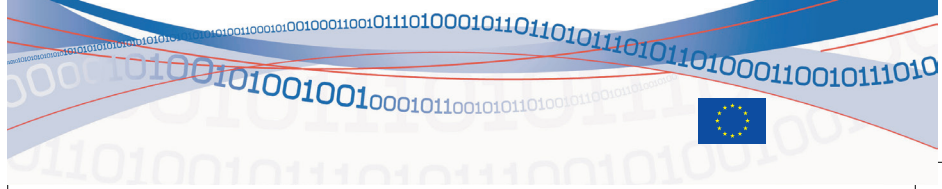
The Register, *Virgin probes Facebook safety, chav claims*, 24 October 2008, available at [http://www.theregister.co.uk/2008/10/24/virgin\\_facebook\\_investigation/](http://www.theregister.co.uk/2008/10/24/virgin_facebook_investigation/) and [http://www.theregister.co.uk/2008/11/03/virgin\\_sackings\\_ba\\_rudeness/](http://www.theregister.co.uk/2008/11/03/virgin_sackings_ba_rudeness/) (last visited on 11 November, 2009).

Thierry Nabeth, *Social web and identity: a likely encounter*, published online 1 October 2009, available at <http://www.springerlink.com/content/184mt42267347524/> (last visited on 19 November 2009).

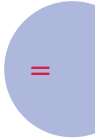
Thomas J., *What are Social Networking Services*, January 2008 - <http://www.digizen.org/socialnetworking/what.aspx> (last visited on 2 November 2009)

Twitter privacy policy available at <https://twitter.com/privacy> (last visited on 22 October 2009).

Zhu Cheng, *Mobile malware: Threats and prevention*, McAfee Inc. 2007, available at [http://www.mcafee.com/us/local\\_content/white\\_papers/threat\\_center/wp\\_malware\\_r2\\_en.pdf](http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_malware_r2_en.pdf) (last visited on 9 November 2009).







# **E-mail security: *Train the trainer reference guide***

*February 2010*

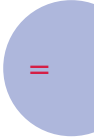






# Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>77</b>
<b>HOW TO USE THIS MANUAL .....</b>	<b>78</b>
STRUCTURE OF THE MANUAL .....	78
STRUCTURE OF THE PRESENTATION PAGES .....	78
<b>THE PRESENTATIONS SLIDES .....</b>	<b>79</b>
SLIDE 1 .....	79
SLIDE 2 .....	80
SLIDE 3 .....	81
SLIDE 4 .....	82
SLIDE 5 .....	83
SLIDE 6 .....	84
SLIDE 7 .....	85
SLIDE 8 .....	86
SLIDE 9 .....	88
SLIDE 10 .....	90
SLIDE 11 .....	92
SLIDE 12 .....	93
SLIDE 13 .....	95
SLIDE 14 .....	97
SLIDE 15 .....	99
SLIDE 16 .....	101
SLIDE 17 .....	103
SLIDE 18 .....	104
SLIDE 19 .....	106



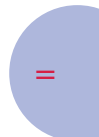


## Executive summary

This training reference guide has been created by ENISA in conjunction with presentation materials for small and medium enterprises to raise awareness with their employees about crucial and important issues regarding the secure use of e-mail.

These documents are designed to provide easy to understand information that focuses employees' attention on information security and encourages them to recognise and respond accordingly to threats.

This material may be used by individuals or presented in a classroom setting by instructors who are involved in their organisation's security awareness efforts. This reference guide provides additional notes and external references for trainers and presenters to utilize while performing security awareness training.



## How to use this manual

This manual is intended to be a guide for instructors of any security awareness course based on ENISA's E-mail Security presentation. This manual is only a guide, and instructors are welcome to use any portion of this material they deem appropriate. It is at the instructor's discretion how to conduct the course and which material to present.

It should be noted however that ENISA recommends that the instructor carefully consider the skills and knowledge of the students being taught in developing the course. The material should be tailored to fit the needs of the students including making it easy to understand, relevant to their position and responsibilities.

ENISA has chosen focus this material on the general user community outside of the Information Technology field. As such, this presentation focuses on the fundamentals of e-mail and avoids the use of complex technical terms to explain risks or solutions.

### Structure of the manual

This manual broken into two parts:

1. How to use this manual (this section)
2. The presentation slides with associated supporting material

### Structure of the presentation pages

Each of the presentation pages are broken in to three parts:

1. The thumbnail of the slide from the presentation
2. Suggested narratives that provide supporting information and discussion points
3. Reference materials that support the slide that can be used to do further research

## The presentations slides

### Slide 1



### Discussion points

This is a good time to have the attendees introduce themselves.

When everyone is introducing themselves, ask them to also say how they use e-mail, and what do they expect to get from the course. The answers will tell you what scenarios you can use as examples for this course, and what their expectations are for this course. This information is very useful so that you can adjust your discussions accordingly.

### References

N/A

### Slide 2

#### About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the Agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

#### Contact details

For contacting ENISA or for general enquiries on information security awareness matters, please use the following details:

Isabella Santa, Senior Expert Awareness Raising - E-mail: [isareniss@enisa.europa.eu](mailto:isareniss@enisa.europa.eu)

Internet: <http://www.enisa.europa.eu>

#### Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA regulation ((EC) No 460/2004). This publication does not necessarily represent the state of the art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2010.

### Discussion points

Introduce ENISA and their activities. Suggest that attendees should examine some of ENISA's other presentations on other aspects of network and information security.

### References

<http://www.enisa.europa.eu> – ENISA's website

### Slide 3



The slide features the ENISA logo in the top left corner. The title "Overview" is positioned in the top right. The main text describes the presentation's focus on e-mail security and lists two sections: "Why E-mail Security is Important" and "How to Use E-mail Securely". The slide has a decorative background with binary code and a blue wave pattern at the bottom. The ENISA website URL and the European Union flag are located at the bottom center.

**enisa**  
European Network  
and Information  
Security Agency

## Overview

This presentation discusses the importance of e-mail security and highlights simple techniques that e-mail users can employ to protect themselves while using e-mail.

The presentation is divided in to two sections:

- ★ Why E-mail Security is Important
- ★ How to Use E-mail Securely

[www.enisa.europa.eu](http://www.enisa.europa.eu)

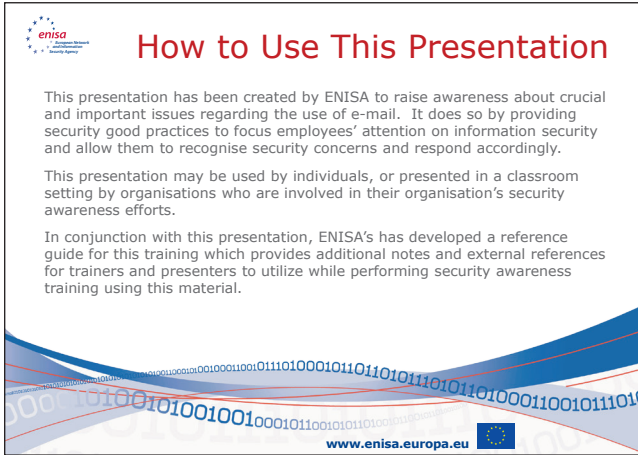
### Discussion points


Point out that this presentation is intended to make users aware of the most common and pervasive risks when using e-mail, and also simple techniques that can eliminate a large percentage of these risks. Point out that the course is intended for all users, and that it can help each of them use e-mail safely at work and at home.

### References

N/A

## Slide 4




 **How to Use This Presentation**

This presentation has been created by ENISA to raise awareness about crucial and important issues regarding the use of e-mail. It does so by providing security good practices to focus employees' attention on information security and allow them to recognise security concerns and respond accordingly.

This presentation may be used by individuals, or presented in a classroom setting by organisations who are involved in their organisation's security awareness efforts.

In conjunction with this presentation, ENISA's has developed a reference guide for this training which provides additional notes and external references for trainers and presenters to utilize while performing security awareness training using this material.

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

This slide is an introduction, and is intended to inform readers that a presentation guide (this document) exists to support instructors in their security awareness efforts.

## References

N/A



## Slide 5



Why is E-mail Security Important?

### Discussion points

This is the start of Section 1, 'Why is E-Mail Security Important?'

### References

N/A

## Slide 6



**E-mail is Everywhere**

- ★ There are over 2.1 billion e-mail accounts
- ★ There are an estimated 1.4 billion e-mail users
- ★ 74% of all accounts are personal users
- ★ 24% are corporate users
- ★ 24% of all users are in Europe
- ★ 247 billion messages are sent per day

Sources: Radicati Group, ComScore Media Metrix

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

E-mail is one of the most common methods of communication today. Social Networking sites have only recently started to overtake e-mail, but Social Networking is still primarily only used in private communications.

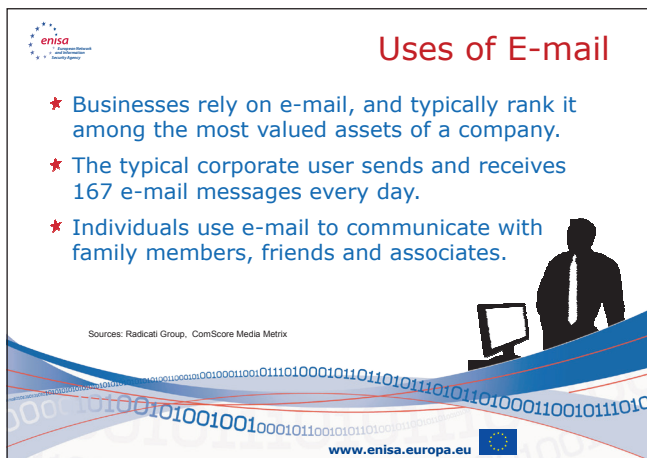
## References

These statistics have primarily come from the Radicati Group's 'Email Statistics Report, 2009-2013' at:

<http://www.radicati.com/wp/wp-content/uploads/2009/05/email-stats-report-exec-summary.pdf>

This and several other Internet reports highlight the extensive use of e-mail. It should be fairly evident from this information that e-mail is widely used, and a heavily used method of communication.

## Slide 7



**Uses of E-mail**

- ★ Businesses rely on e-mail, and typically rank it among the most valued assets of a company.
- ★ The typical corporate user sends and receives 167 e-mail messages every day.
- ★ Individuals use e-mail to communicate with family members, friends and associates.

Sources: Radicati Group, ComScore Media Matrix

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

- ✓ Businesses use e-mail to communicate with future, current and past customers.
- ✓ Businesses use e-mail to provide customer service, product support, and ongoing communication about product or policy changes.
- ✓ Helpdesk applications receive e-mails to initiate trouble tickets.
- ✓ Computers and Applications send e-mail alerts to administrators.

Ask the attendees how it would affect them if e-mail stopped working for one day. Then ask them how it would affect them if the phone stopped working for one day. You are more likely to find that e-mail is of greater value (a few exceptions should be noted – for example at call centres, and other telephone oriented operations).

## References

N/A

## Slide 8



**E-mail Security is Important**

- ★ **E-mail is Typically Insecure**
  - ★ Most e-mail can be misdirected, altered, and viewed
  - ★ E-mail is often used for scams and fraud
  - ★ E-mail is often abused for marketing
  - ★ E-mail is often used to spread malicious software

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

E-mail was not originally designed with security in mind. It was originally designed to just send text messages to designated people on a single machine, and then over simple networks. The design allows someone who is malicious to re-direct e-mail. It also allows someone who has access to a system that processes e-mail to modify an e-mail. Anyone who has access to a networks where e-mails are transmitted or computers where e-mails are processed can view the e-mails that are there. There is no built-in mechanism to make e-mail confidential (such as encryption), to verify the e-mail content hasn't been altered (such as a hash), or to verify who sent the e-mail (such as a digital signature).



*Instructors: Be cautious about using the technical terms in the narration as some audiences will not understand what they mean. Be prepared to explain these terms:*

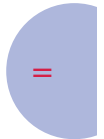
*Encryption: to make information unreadable to anyone who does not know the method to make it readable.*

*Hash: a mathematical way of creating a special digital value that represents a message and that is unique to each different message.*

*Digital Signature: the electronic equivalent of someone's 'wet' signature.*

Other risks in e-mail:

- ✓ E-mail is regularly used for scams and fraud – such as attempts to gather personal information or to get you to participate in activities which you later discover are illegal.
- ✓ E-mail is often abused for marketing purposes – called SPAM. A significant percentage of SPAM is in some way related to scams and fraudulent activities.
- ✓ E-mail is often used to spread malicious software – which is a technical problem that requires special care.



## Slide 9



 **Risk: Authenticity & Confidentiality**

- ★ **Spoofing: Authenticity of E-mail**  
E-mail has no built-in way to verify a sender's identity. It is very simple to send e-mail that appears to come from another user.
- ★ **Confidentiality of E-mail**  
E-mail has no built-in way to keep the content confidential and private. Anyone can read e-mail using some basic tools.
- ★ **Tools exist which can overcome these challenges**

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

*Instructor: This slide can be presented in two ways – one, as an overview for audiences that are not very technical, or two, in a technical manner for those who either understand the content, or those who choose to challenge these views.*

E-mail has no built-in method to verify a sender's identity. Even though we are trusted to input our correct identity into our e-mail programs, nothing stops us from using fraudulent addresses. Anyone can setup an e-mail program to send e-mails with fake addresses, and even without an e-mail program it is fairly trivial to use simple tools like Telnet to create fraudulent e-mail messages with fake sender addresses. Some e-mail providers attempt to address this issue with special configurations on their mail servers, but many others do not.



E-mail was never built to keep the content of an email confidential and private. The text of a message is transmitted in the clear which means anyone with a tool that can monitor the network can view the e-mail.

Basic tools such as a network monitoring or network sniffing tool can view emails. Basic tools such as ordinary e-mail clients and Telnet can be used to create fraudulent e-mails. The good news is that there are tools available that can overcome these challenges.

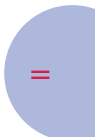
Tools that encrypt emails render the content of the e-mail unreadable, except for someone who has the right information to decrypt or make the message readable again. Most internal mail systems such as Microsoft Exchange and Lotus Notes contain these capabilities. Internet e-mail by default does not, however the use of tools such as PGP, S/MIME and other technology can make encryption available. These same tools can verify the user who sent the e-mail, and that verify the content hasn't been changed.

*Instructor: Point out what technology the company uses, and what tools the users have at their disposal. This is very important since the insecurity of e-mail will probably shock them, and they will try to use another technology which may be even less useful. There will be another chance to discuss the tools again in a later slide.*

## References

[http://www.cert.org/tech\\_tips/home\\_networks.html#III-B-8](http://www.cert.org/tech_tips/home_networks.html#III-B-8)

[http://www.cert.org/tech\\_tips/email\\_spoofing.html](http://www.cert.org/tech_tips/email_spoofing.html)



## Slide 10



### Security Risk: Fraud

- ★ **Phishing**  
Using E-mail to trick a user in to sending personal information via e-mail, or to visit a malicious website.
- ★ **SPAM**  
Unsolicited E-mail is called "SPAM"  
It accounts for over 80% of all E-mail traffic
- ★ **Malicious Software**  
Typically contained in E-mail attachments  
Can also be contained in HTML or images in the e-mail



www.enisa.europa.eu 

## Discussion points

Phishing is a very wide-spread problem. It is a technique that attempts to convince someone to send personal information that can be used for Identity Theft or fraud. Phishing emails come in many different forms, but the two most typical techniques are:

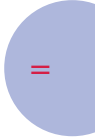
- ✓ Requesting assistance to recover a large sum of money, or requiring your personal information so they can transfer a large sum of money. The e-mail will entice you with an offer of reimbursement in large sums of money, and thanks you for your efforts. It may appear to be from a solicitor, a relative of a wealthy person or family, a company requiring assistance in collecting money or funds, or an organization looking to award you a prize or award.
- ✓ Informing you that your account has been compromised or urgently requesting that you verify your bank or payment card account. The email attempts to convince you that the situation is urgent, and that you need to confirm your account number, password, or your PIN of the account in order to ensure the account's security.





Many of the messages come from people you have never met before, or banks where you do not even do business.

SPAM is a very large problem. SPAM is any e-mail which comes from sources we did not ask to send us e-mails or that we did not give our consent. It accounts for over 80% of all e-mail traffic. Companies spend a large amount of time and money to combat SPAM and filtering it is considered a standard part of e-mail operations. SPAM consumes a large amount of resources (network traffic to handle these messages, disk space to store the messages, and processing power of the people who must view, roll their eyes, and delete the e-mail). SPAM can be another source of fraud as many of the advertisements and offers in SPAM e-mails is for websites that sell non-existent products, or entice you to visit sites which contain malicious programs.



Malicious software can be delivered in an e-mail message through infected e-mail attachments, images in the e-mail or in the HTML used in the e-mail. Criminals have figured out how to manipulate the content of images and HTML to take advantage of vulnerabilities and weaknesses in many popular e-mail programs. By taking advantage of these vulnerabilities and weaknesses, they are able to insert malicious software onto the victim's computer.

## References

- <http://en.wikipedia.org/wiki/Phishing>
- <http://ha.ckers.org/blog/20060609/how-phishing-actually-works/>
- [http://ec.europa.eu/information\\_society/policy/ecommm/todays\\_framework/privacy\\_protection/spam/](http://ec.europa.eu/information_society/policy/ecommm/todays_framework/privacy_protection/spam/)
- <http://www.spamlaws.com/eu.shtml>
- <http://spam.abuse.net/>
- <http://www.radicati.com/wp/wp-content/uploads/2009/05/email-stats-report-exec-summary.pdf>
- [http://www.cert.org/tech\\_tips/home\\_networks.html#III-B-6](http://www.cert.org/tech_tips/home_networks.html#III-B-6)



## Slide 11

# How to Use E-mail Securely

### Discussion points

This is the start of Section 2, 'How to Use E-Mail Securely'

### References

N/A

## Slide 12



**E-Mail Security Tip #1**

- ★ **Never Use E-mail to Send Confidential or Personal Information**

Never send payment card numbers, financial information, identification numbers, medical information, passwords or PINs via e-mail.

Never send company confidential information such as financial information, product plans, and other proprietary information outside the company via e-mail.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

*Instructor: It is important to provide backing information for these points – if your focus is on corporate awareness then be certain to define what company confidential information is. If you are focused on personal awareness, focus on what is personal information that should not be shared. The text in the slides covers the major items.*

If you send confidential information via e-mail, there is a very good chance it will be seen by someone you do not wish to see it. Putting personal information in e-mail can lead to Identity Theft and Fraud. Putting company confidential information in an e-mail can disclose confidential information to competitors, and people who would like to profit from insider information. In some locations, disclosing company financial information can become a legal issue.

## References

<http://en.wikipedia.org/wiki/Phishing>

<http://office.microsoft.com/en-us/outlook/HA011400021033.aspx>

[http://www.phishtank.com/what\\_is\\_phishing.php](http://www.phishtank.com/what_is_phishing.php)

<http://www.antiphishing.org/>

<http://www.ftc.gov/bcp/edu/multimedia/video/ogol/phishing/index.shtml>

## Slide 13



 **E-Mail Security Tip #2**

★ **Beware of E-mail Asking for Personal Information**

Never share personal information via E-mail no matter how enticing or urgent the message seems.

If the offer in an E-mail seems too good to be true, then it probably is.

A bank or payment card company will never request your personal information via an email.

If in doubt, always contact your bank or payment card company using methods you know to be correct.



[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

*Instructor: Point out that his slide refers to Phishing and SPAM.*

Any e-mail that asks for personal information should be treated very carefully or deleted.

When you receive an e-mail that appears too good to be true, it probably is. A good indication is if the e-mail is from someone you do not know. Most likely they have sent the same e-mail to hundreds of other unsuspecting people. The message will entice you with offers of money that are hard to resist and rewards that you can normally only dream of – an enticement that draws you into making decisions you wouldn't normally make.

Phishing e-mails may also attempt to scare you or rush you into action by telling you that your account has been compromised, or by insisting that you validate your account information for a new security system they are

putting in place. The message will convey a sense of urgency which is intended to rush you into making a decision you wouldn't normally make.

Keep in mind: no bank or payment card company will ever ask you to send personal information, passwords or PINs via email. These types of companies are typical targets for criminals using phishing. Many banks and payment card companies will post news of the newest phishing attacks. If you are unsure if the e-mail you received is a phishing e-mail, then contact the company that the e-mail allegedly came from using a phone number you know to be true. Do not use e-mail and do not use the address or phone number in the e-mail. If you need to, look up the phone number in a phone book. By using this method, you will ensure the authenticity of the company you are speaking to, and you can verify the authenticity of the original email.

## References

<http://en.wikipedia.org/wiki/Phishing>

<http://office.microsoft.com/en-us/outlook/HA011400021033.aspx>

[http://www.phishtank.com/what\\_is\\_phishing.php](http://www.phishtank.com/what_is_phishing.php)

<http://www.antiphishing.org/>

<http://www.ftc.gov/bcp/edu/multimedia/video/ogol/phishing/index.shtml>

## Slide 14



**E-Mail Security Tip #3**

★ **Handle E-mail with Care**

- Do not open E-mail attachments from unknown people.
- Do not click on links in E-mails. Use addresses you have verified and know to be legitimate.
- If you must click on a link, validate it before clicking it.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

E-mail is a very popular way to spread malicious software. Some e-mails are intentionally created to spread infected files and programs. Some e-mails are from friends who unintentionally spread malicious software by sending you files, videos, or music that is infected. You must be very careful since even these 'trusted' sources of e-mails can spread malicious software.

Never open e-mail attachments from people you do not know. Even if you do know them, think twice before opening the e-mail. Is the attachment a file you were expecting? Does it look like a file that could be a typical type of infected software (Zip files, videos, and files with strange names or file extensions)?

Make sure your anti-virus software is configured to scan your e-mail. Even with anti-virus software scanning the e-mail, not all malicious software can be identified. Some files contain types of malicious software that is unique or has never been seen before, and therefore would not be detected. If in doubt, do not open the attachment.

Do not click on links in e-mails. Links in emails are not always what they seem to be. The website address that displays in the e-mail is not necessarily the same as the link behind that is hidden behind that link. The link may read 'http://www.mybank.com' but the link is actually connected to 'http://goto.hackersite.com'. Many of these links direct you to malicious websites that will attempt to install malicious software onto your computer. Always examine the links in e-mails.

If you hold your cursor over the link in the e-mail the actual hyperlink will usually display in a small helper window. Examine the information that is displayed in the pop-up helper window to see if it indicates that the email is fraudulent. Some clues that will tell you if the e-mail is fraudulent:

- ✓ Is the link in the pop-up helper window different from the link displayed in the e-mail?
- ✓ Does the link appear to be misspelled?
- ✓ Is the link not relevant to the message?
- ✓ Are there misspellings in the e-mail?
- ✓ Is the e-mail specifically addressed to 'undisclosed-recipients' or someone else?

These items can help you identify a fraudulent e-mail. If you find these discrepancies, delete the e-mail. If you are still not sure if the e-mail is fraudulent or not, contact the sender through the phone, or through a method you know is legitimate. Do *\*not\** click on the link or respond directly to the e-mail.

*Instructor: A good demonstration would be to show an example of a link that has a display name, but the actual hyperlink behind it is different. Show the audience the 'pop-up' display that shows the actual hyperlink and how to read it.*

## References

- [http://www.phishtank.com/what\\_is\\_phishing.php](http://www.phishtank.com/what_is_phishing.php)
- <http://office.microsoft.com/en-us/outlook/HA011400021033.aspx>
- <http://portal.acm.org/citation.cfm?id=1242572.1242660>



## Slide 15



**E-Mail Security Tip #4**

★ **Use Tools to Help You**

Install a reputable anti-virus software that scans your email and attachments for malicious software.

Install and use a reputable anti-SPAM tool to manage unsolicited e-mails you receive.

If you must send confidential information via e-mail, use a tool that will encrypt the e-mail to keep the contents confidential and private.

Keep the tools up-to-date and check for patches.

Remember to Check for Updates Today!

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

*Instructor: The detail you discuss in this portion of the presentation will depend on the level of technical knowledge of your audience. Be aware of the level of knowledge your audience has before beginning any detailed technical presentation on this slide.*

It is important to install a reputable anti-virus program – many websites and pop-up windows will offer anti-virus and other security software. Some pop-up messages will warn you that your computer is already infected and that you need to install their software to clean your system. If you are presented with this type of pop-up window, do not install their software or click on any links on the page. Immediately quit your browser and ensure all windows are closed. There are many reputable software companies who make very good anti-virus software products. Some require payment for the software. It is important to compare the amount of time and money that would be lost if your computer were infected versus the cost of purchasing a reputable anti-virus tool.



An anti-SPAM tool will save you considerable amounts of time by filtering e-mail that appears to be SPAM. Users should be careful to check their SPAM filters, and not automatically delete all SPAM. There are many instances where legitimate e-mail has been mistakenly identified as SPAM, and critical messages do not arrive. Remember that the anti-SPAM tool is just a tool – and still should have human intervention to ensure it works properly.

If you need to send confidential information to someone, you can use some well known tools that will make the e-mail unreadable. They are called encryption tools. There are very good tools, and some are even included in the e-mail programs themselves. You can also encrypt any files or data you wish to send someone by using a program that also can compress the data. Programs such as WinZip, PKWARE, and WinRAR are some examples.

*Instructor: You can mention here if the company has a standard for encryption, and if it does, simple state how a user would request this feature or tool. Also let them know if e-mail is encrypted while it is inside the company. If you use Microsoft Exchange or Lotus Notes the encryption feature can be enabled so that it is transparent to the users. Emphasize with the audience that if you do have this feature enabled, it is only for e-mail that is inside the company. Remind the audience that sending confidential information outside the company is prohibited and can lead to legal issues for the company.*

## References

Some sources for the manufacturers:

<http://www.microsoft.com/exchange/2010/en/us/exchange-2007-features.aspx>

[http://www.ibm.com/developerworks/lotus/library/l5-Notes\\_Encryption/index.html](http://www.ibm.com/developerworks/lotus/library/l5-Notes_Encryption/index.html)

[http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp?topic=/com.ibm.help.domino.admin.doc/DOC/H\\_ENCRYPTING\\_OUTGOING\\_MAIL.html](http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp?topic=/com.ibm.help.domino.admin.doc/DOC/H_ENCRYPTING_OUTGOING_MAIL.html)



## Slide 16



**E-Mail Security Tip #5**

★ **If You Use Webmail**

- ★ Make sure you use a secure computer – avoid public computers.
- ★ Make sure the webmail site encrypts your webmail session including when you input your password.
- ★ Change your e-mail password on a periodic basis.
- ★ Make sure other people cannot view your computer screen and view your e-mail.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

There are a few additional items to be aware of if you use webmail or if your company supports webmail.

Avoid public computers because they can easily become infected with viruses and other malicious software by careless or malicious users. The malicious software can gather information from your webmail including your password. Use a laptop that has been provided to you, or a computer at one of your remote offices.

Make sure that the webmail service that you use encrypts your password and your email session using secure web services (HTTPS). For several years many webmail and public mail providers did not protect this information and webmail services were broken in to.

Change your email password on a periodic basis. Make your password complex, and make any password reset information complex to avoid

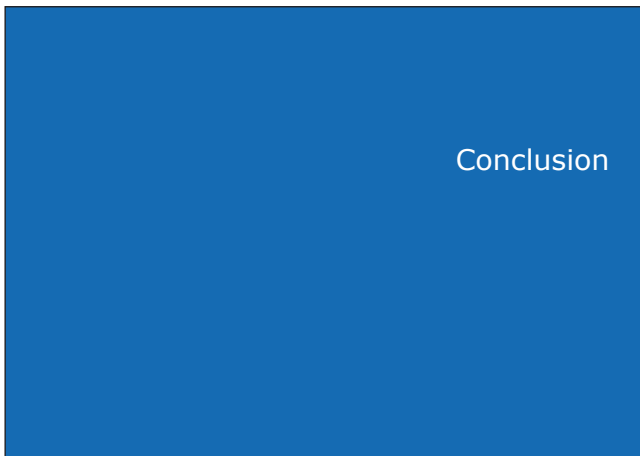
malicious outsiders from hijacking your email account. There are numerous cases of public e-mail and webmail services being taken over by unauthorized people.

When you are reading your e-mail – either through webmail or your normal e-mail client – make sure no one can view your computer screen. Some people will look over your shoulder (called shoulder-surfing) and view the confidential and personal information in your e-mail. Be careful where you read your e-mail. Choose isolated or private locations where you can be sure people cannot see your screen.

### References

<http://www.washingtonpost.com/wp-dyn/content/article/2009/09/06/AR2009090602238.html>

## Slide 17



### Discussion points

This is the conclusion of the presentation.

### References

N/A

## Slide 18



The slide features the ENISA logo in the top left corner. The title "E-mail Security is Important" is centered at the top in a large, bold, red font. Below the title, there is a bulleted list of five points, each preceded by a red star icon. The text of the list items is in blue. At the bottom of the slide, there is a silhouette of a person in a suit with their arms raised in a celebratory gesture, set against a background of blue and white wavy lines and binary code (0s and 1s). The ENISA logo, the website address "www.enisa.europa.eu", and the European Union flag are positioned at the bottom center of the slide.

**E-mail Security is Important**

- ★ E-mail is important to companies and individuals
- ★ There are many security risks to E-mail
- ★ Do not use E-mail to send confidential or personal information
- ★ Recognize and avoid fraudulent E-mails
- ★ Implement security tools to protect your E-mail

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

*Instructor: This is a summary slide that provides an opportunity to repeat the key themes of the presentation.*

As we talked about in the beginning, e-mail is important to both companies and individuals.

We also discussed the many security risks to e-mail including loss of confidentiality, authenticity, and risk of fraud.

We talked about key ways to protect yourself:

Don't send confidential or personal information via e-mail

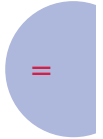
Recognise fraudulent e-mails including phishing, SPAM, and e-mails with malicious content.



Lastly, take advantage of the tools that are out there to protect your computer from fraudulent e-mails, malicious software, and SPAM.

## References

N/A



## Slide 19



## Discussion points

N/A

## References

N/A



*Train the trainer reference guide*







# **Malicious software: *Train the trainer reference guide***

*February 2010*





# Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>113</b>
<b>HOW TO USE THIS MANUAL .....</b>	<b>114</b>
STRUCTURE OF THE MANUAL .....	114
STRUCTURE OF THE PRESENTATION PAGES .....	114
<b>THE PRESENTATIONS SLIDES .....</b>	<b>115</b>
SLIDE 1 .....	115
SLIDE 2 .....	116
SLIDE 3 .....	117
SLIDE 4 .....	118
SLIDE 5 .....	119
SLIDE 6 .....	120
SLIDE 7 .....	122
SLIDE 8 .....	124
SLIDE 9 .....	126
SLIDE 10 .....	128
SLIDE 11 .....	130
SLIDE 12 .....	132
SLIDE 13 .....	133
SLIDE 14 .....	135
SLIDE 15 .....	136
SLIDE 16 .....	137
SLIDE 17 .....	138
SLIDE 18 .....	140
SLIDE 19 .....	142
SLIDE 20 .....	144
SLIDE 21 .....	146
SLIDE 22 .....	148
SLIDE 23 .....	149
SLIDE 24 .....	150
SLIDE 25 .....	151
SLIDE 26 .....	153





## Executive summary

This training reference guide has been created by ENISA in conjunction with presentation materials for small and medium enterprises to raise awareness with their employees about the critical risks due to malicious software.

These documents are designed to provide easy to understand information that focuses employees' attention on information security and how to recognise and respond accordingly to malicious software.

This material may be used by individuals or presented in a classroom setting by instructors who are involved in their organisation's security awareness efforts. This reference guide provides additional notes and external references for trainers and presenters to utilize while performing security awareness training.



## How to use this manual

This manual is intended to be a guide for instructors of any security awareness course based on ENISA's Malicious software presentation. This manual is only a guide, and instructors are welcome to use any portion of this material they deem appropriate. It is at the instructor's discretion how to conduct the course and which material to present.

It should be noted however that ENISA recommends that the instructor carefully consider the skills and knowledge of the students being taught in developing the course. The material should be tailored to fit the needs of the students including making it easy to understand, relevant to their position and responsibilities.

ENISA has chosen focus this material on the general user community outside of the Information Technology field. As such, this presentation focuses on the fundamentals of critical risks due to malicious software and avoids the use of complex technical terms to explain risks or solutions.

### Structure of the Manual

This manual broken into two parts:

1. How to use this manual (this section)
2. The presentation slides with associated supporting material

### Structure of the Presentation Pages

Each of the presentation pages are broken in to three parts:

1. The thumbnail of the slide from the presentation
2. Suggested narratives that provide supporting information and discussion points
3. Reference materials that support the slide that can be used to do further research



## The presentations slides

### Slide 1



### Discussion points

This is a good time to have the attendees introduce themselves.

When everyone is introducing themselves, ask them to also say what they expect to get from the course. The answers will tell you what scenarios you can use as examples for this course, and what their expectations are for this course. This information is very useful so that you can adjust your discussions accordingly.

### References

N/A

## Slide 2

### About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the Agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

#### Contact details

For contacting ENISA or for general enquiries on information security awareness matters, please use the following details:

Isabella Santa, Senior Expert Awareness Raising - E-mail: [isawareness@enisa.europa.eu](mailto:isawareness@enisa.europa.eu)

Internet: <http://www.enisa.europa.eu>

### Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA regulation ((EC) No 460/2004). This publication does not necessarily represent the state of the art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2010.

## Discussion points

Introduce ENISA and their activities. Suggest that attendees should examine some of ENISA's other presentations on other aspects of network and information security.

## References

<http://www.enisa.europa.eu> – ENISA's website



### Slide 3



The slide features the ENISA logo in the top left corner. The title "Overview" is in red. The main text describes the presentation's focus on malicious software risks and protection techniques. A bulleted list outlines the presentation's structure. The bottom of the slide has a decorative blue and white wave pattern with binary code, the website URL "www.enisa.europa.eu", and the European Union flag.

**enisa**  
European Network  
and Information  
Security Agency

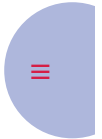
## Overview

This presentation discusses the ongoing risks associated with malicious software and highlights simple techniques that users can employ to protect themselves from malicious software.

The presentation is divided in to two sections:

- ★ What is Malicious Software?
- ★ How Malicious Software Can Affect You
- ★ Types of Malicious Software
- ★ How to Protect Yourself
- ★ Resources

[www.enisa.europa.eu](http://www.enisa.europa.eu)



### Discussion points


Point out that this presentation is intended to make users aware of the risks associated with malicious software, and also simple techniques that can eliminate a large percentage of these risks. Point out that the course is intended for all users, and that it offers best practices that can help protect each of them from malicious software at work and at home.

### References

N/A



## Slide 4




### How to Use This Presentation

This presentation has been created by ENISA to raise awareness about the critical risks due to malicious software. It does so by providing easy to understand information that focuses employees' attention on information security and allows them to recognise and respond accordingly to malicious software.

This presentation may be used by individuals, or presented in a classroom setting by instructors who are involved in their organisation's security awareness efforts.

In conjunction with this presentation, ENISA's has developed a reference guide for this training which provides additional notes and external references for trainers and presenters to utilize while performing security awareness training using this material.

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

This slide is an introduction, and is intended to inform readers that a presentation guide (this document) exists to support instructors in their security awareness efforts.

### References

N/A

## Slide 5



What is Malicious Software?


### Discussion points

This is the start of Section 1, 'What is Malicious Software?'

### References


N/A

## Slide 6




### What is Malicious Software?

- ★ A hostile or intrusive program designed to insert itself on to your computer without your consent.
  - ★ It is also called Malware from *MALicious softWARE*.
  - ★ The amount of Malicious Software increases every year.
    - Reportedly increased by 276% in 2008\*
  - ★ Malicious Software is continuously created by computer programmers from around the world.



\*Symantec Global Internet Security Threat Report April 2008

www.enisa.europa.eu 

## Discussion points

It is important to point out that a program is malware if it meets one of two criteria:

- ✓ Is it hostile or intrusive
- ✓ Is it inserted on to your computer without your consent

A program can be Malware if it inserted itself on to your computer without your consent. It also (obviously) is malicious software if it is hostile or intrusive; which means it will perform hostile activities – deleting data or files, attacking other computers, or performing any other actions you do not consent to.

Throughout the presentation we will use the term Malware since it is easier to say. Malware is a combination of two words: **Malicious** and **Software**.



Malware is a difficult problem because it is created by programmers around the world. Some are searching for fame; some are curious programmers who do not see any harm in what they do. However, in recent years the most frequent type of malware is used by criminals to steal information, disrupt computer systems, or perpetuate fraud. Malware has been increasing at a rapid pace year after year, and shows no sign of slowing down. Because programmers are constantly creating new malware it is virtually impossible to completely eliminate malware.

**Fun Fact:** First recorded virus: Creeper Virus in 1971

## References

<http://technet.microsoft.com/en-us/library/dd632948.aspx>

<http://en.wikipedia.org/wiki/Malware>

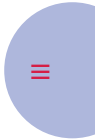
[http://malware.wikia.com/wiki/Main\\_Page](http://malware.wikia.com/wiki/Main_Page)

Good source for malicious software statistics:

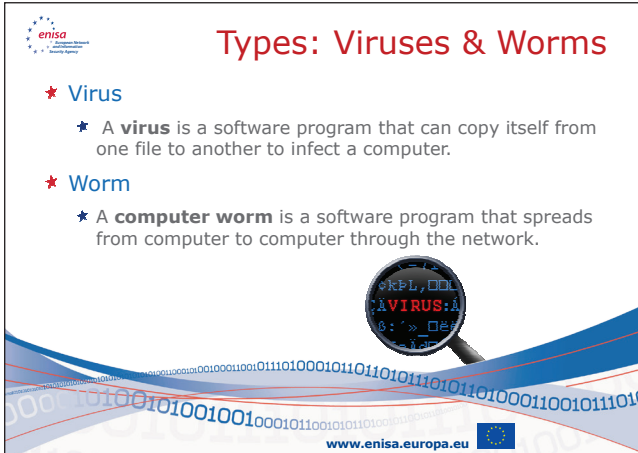
<http://www.symantec.com/business/theme.jsp?themeid=threatreport>


An excellent timeline showing the history of malicious software:

[http://malware.wikia.com/wiki/Timeline\\_of\\_noteworthy\\_computer\\_viruses,\\_worms\\_and\\_Trojan\\_horses](http://malware.wikia.com/wiki/Timeline_of_noteworthy_computer_viruses,_worms_and_Trojan_horses)





## Slide 7



 **Types: Viruses & Worms**

- ★ **Virus**
  - ★ A **virus** is a software program that can copy itself from one file to another to infect a computer.
- ★ **Worm**
  - ★ A **computer worm** is a software program that spreads from computer to computer through the network.

  
[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

*Instructor: It is very easy to become very technical as you present the different types of malicious software. Stay focused on simple examples of how malware spreads and simple examples of what malware can do. Do not allow the discussion to become very technical in nature. The subject of Malicious Software is a science on to itself and can spark intense debates. The objective of this section is to make people aware of the risks and ways that they can become a victim of Malware. This approach will make it easier to explain why certain prevention tactics are so important.*

There are several different types of malware that have been created. The next few slides will cover the most typical classifications. There are many types of malware which fall under multiple categories or change as they move from system to system. Malware is constantly evolving and new hybrid types of malware are created on a constant basis.





Viruses are typically programs that replicate themselves between files, memory, hard disks, or other data storage mediums. Typically viruses only spread when executing or copying a file that is already infected. Note that inserting a CDROM or thumb drive on some operating systems is equivalent to executing a program, and can also cause a virus to spread.

A worm is a program that spreads itself through a network and does not need to attach itself to an existing file or program. Worms spread themselves typically by exploiting existing vulnerabilities or weaknesses in an operating system or application. Some good examples are worms that exploited vulnerabilities in UNIX systems (the Morris Internet Worm of 1988) and worms that exploited vulnerabilities in Microsoft Windows (Mydoom of 2004). These worms spread rapidly through the Internet and continued until the vulnerabilities they exploited were fixed.



## References

[http://en.wikipedia.org/wiki/Computer\\_virus](http://en.wikipedia.org/wiki/Computer_virus)

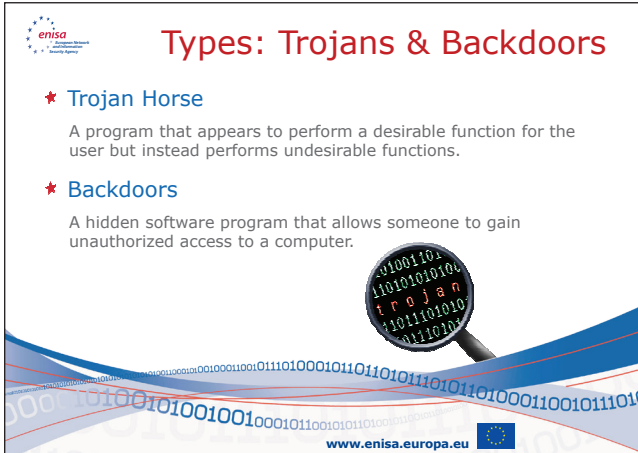
<http://malware.wikia.com/wiki/Virus>

[http://en.wikipedia.org/wiki/Morris\\_worm](http://en.wikipedia.org/wiki/Morris_worm)

<http://en.wikipedia.org/wiki/Mydoom>



## Slide 8



**Types: Trojans & Backdoors**

- ★ **Trojan Horse**  
A program that appears to perform a desirable function for the user but instead performs undesirable functions.
- ★ **Backdoors**  
A hidden software program that allows someone to gain unauthorized access to a computer.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

Trojan horses are named after the famous story of the Trojan Horse in the story of the Trojan War. Like the Trojan Horse in the story, the software Trojan Horse is designed to look like it is an innocent program. In some cases it may even use the name of an existing or standard file for an operating system. It may place itself in the same location as the standard file, or a different location. The software Trojan horse will, like its namesake, contain dangerous capabilities inside.

Backdoors are programs which allow an intruder or attacker to access a system in a way that bypasses normal authentication. Users normally have to log into a system using a username and password. A backdoor allows someone to not have to perform this process. Some backdoors are written by programmers to allow them access to software for problem solving, but can also be added to a computer to allow an attacker to access a system without needing a password, or in a way that cannot be detected. Backdoors may be created by installing a new program or by

modifying an existing program that gives access to a system. Backdoors can be inserted by an intruder, a virus, or a worm.

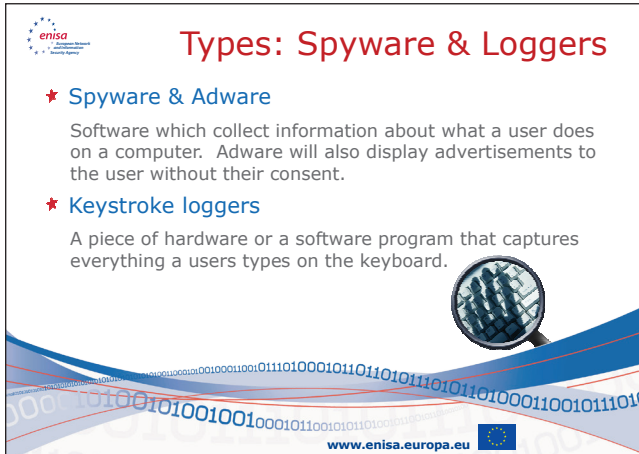
## References


[http://malware.wikia.com/wiki/Trojan\\_horse](http://malware.wikia.com/wiki/Trojan_horse)

<http://malware.wikia.com/wiki/Backdoor>





## Slide 9



 **Types: Spyware & Loggers**

- ★ **Spyware & Adware**  
Software which collect information about what a user does on a computer. Adware will also display advertisements to the user without their consent.
- ★ **Keystroke loggers**  
A piece of hardware or a software program that captures everything a users types on the keyboard.



[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

Spyware can be spread as a virus, worm, or through various other methods of delivering software (installing software from the Internet, visiting a malicious website). It has one goal – to track what you do on your computer and report that back to another system. Spyware may report what you type, what sites you visit on the Internet, and even what content is presented. This can include your banking information, passwords, and other confidential and personal information.

It can also cause your computer to become unstable and perform poorly as the adware and spyware send their information out to the Internet.

There are numerous keylogging methods, and can include spyware, or even pieces of hardware which are inserted into a system to monitor keystrokes. Like all other malicious software, it is place their without the user's consent.


## References

<http://en.wikipedia.org/wiki/Spyware>

<http://malware.wikia.com/wiki/Spyware>






## Slide 10



### Types: Botnets & Rootkits

- ★ **Botnets**  
Software programs that are installed without authorization on many different computers and are controlled remotely.
- ★ **Rootkits**  
A collection of software programs that allow an attacker to do many different undesirable things and also to hide from detection.



[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

Botnets refer to 'robot networks' and are a new evolution of malicious software and has become wide-spread. Botnets consist of software which infects a user's computer (called a robot or a zombie) and which is controlled by a remote system. Some popular botnets include Con-fiker from 2009. These botnets can be used for many different tasks. The software which infects the user's computer waits for instructions on what to do from the remote system. The remote system may instruct it to collect information from the infected system, or it may instruct it to attack other computers it finds. Some botnets have been identified to consist of millions of systems. Current numbers are hard to estimate but they are extensive.

Rootkits are collections of software that help an attacker or intruder hide from detection. They may hide files, conceal that an intruder is present on the system, or to hide any processes that are running. Rootkits are a

mix of tools that can include backdoors, keyloggers, and other tools that an intruder may find useful to hide their presence.

## References

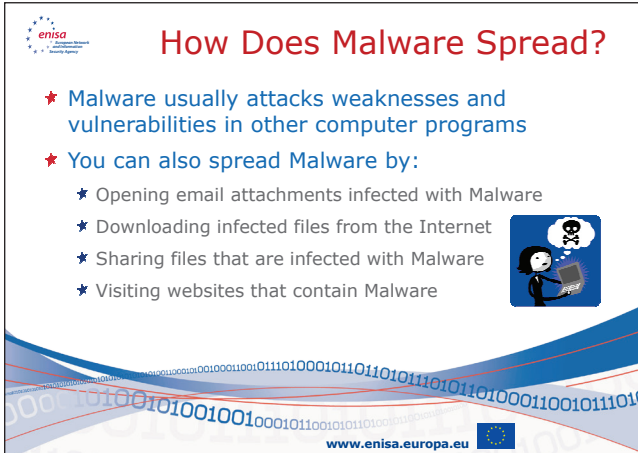
<http://en.wikipedia.org/wiki/Botnet>

<http://www.shadowserver.org/wiki/pmwiki.php/Information/Botnets>

<http://malware.wikia.com/wiki/Rootkit>



## Slide 11



### How Does Malware Spread?

- ★ Malware usually attacks weaknesses and vulnerabilities in other computer programs
- ★ You can also spread Malware by:
  - ★ Opening email attachments infected with Malware
  - ★ Downloading infected files from the Internet
  - ★ Sharing files that are infected with Malware
  - ★ Visiting websites that contain Malware

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

Malware typically will infect a system through weaknesses and vulnerabilities in other computer programs, but this usually requires some help from a user. Many virus infections are due to users who open attachments or visit websites which contain malware, or users who do not install or keep their anti-virus software up-to-date.

One of the most common methods of spreading malware is through downloading files from the Internet or opening e-Mail attachments. Even files sent to you by people you know can contain malware. They may not recognize it because the malware wasn't detected by their anti-virus tool, or they use a different type of computer than you do. The malware will still exist and can affect your computer. Someone might invite you to download a file that contains some enticing picture, music or program. These invitations are usually an attacker attempting to spread malware.





File sharing sites also contain a large percentage of infected files. While it can be enticing to be able to download the latest music, pictures or programs, the high probability and risk of infecting your system with malware should be considered.

The same issue applies to many pop-up windows that tell you that your computer is infected with a virus, and you need to quickly download the software they present you with to clean the infection. In reality the software will install the infection. Many sites which carry controversial content such as open 'hacker', violence, and pornography sites often contain malware as well.

Always be careful when you are asked to download or install a file. There is a strong possibility that it contains malware. The best recommendation? Avoid files from untrusted sources, and always be sceptical of suggestions or invitations to download files and programs.

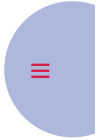
## References

<http://www.us-cert.gov/cas/tips/ST05-007.html>

<http://www.wired.com/techbiz/media/news/2004/01/61852>

[http://malware.wikia.com/wiki/Rogue\\_security\\_software](http://malware.wikia.com/wiki/Rogue_security_software)

<http://www.symantec.com/business/theme.jsp?themeid=threatreport>



## Slide 12

# How Can Malware Affect You?

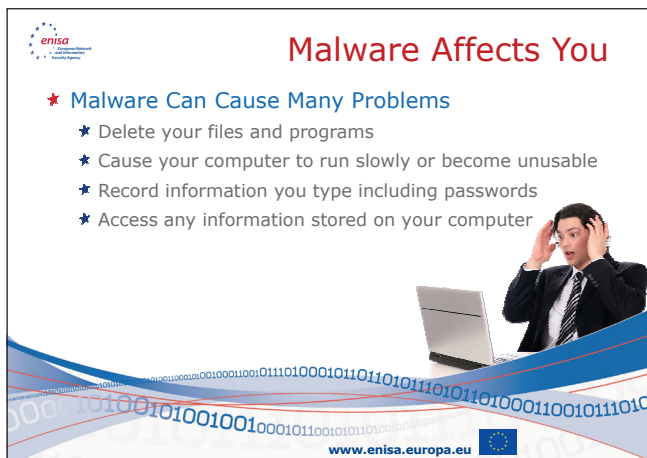
### Discussion points

This is the start of Section 2, 'How Can Malware Affect You?'

### References

N/A

## Slide 13



**Malware Affects You**

- ★ **Malware Can Cause Many Problems**
  - ★ Delete your files and programs
  - ★ Cause your computer to run slowly or become unusable
  - ★ Record information you type including passwords
  - ★ Access any information stored on your computer

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

Malware has a long history of causing damage to computers and networks.

Some famous malicious software:

**Jerusalem virus** – one of the first destructive viruses. It was discovered in 1988. It deletes files every Friday the 13th.

**ILOVEYOU** – a worm from 2000 that emails itself to everyone in the victim's address book. It is the most costly malware to date with estimates upwards of \$5.5 to \$10 billion (USD) in damages due to this worm.

**Code Red / Code Red II / Nimda** – a series of worms which exploited bugs in Microsoft IIS, and caused major Internet outages over three months in 2001.

**SQL Slammer** – an attack against vulnerabilities in Microsoft SQL that causes major outages on the Internet.

**MyDoom** – a worm from 2004 that spread quickly through email. It creates a way for a remote attacker to control the computer.

*Instructor: Ask the audience to think of things that could be damaged, lost, stolen, or impact them if malicious software infected their computer, and a computer at their work. Use this discussion to make the audience aware of the risks of malicious software. The risks will make them more aware and attuned to methods to prevent and block malicious software. Watch for the types of information that the audience discusses. Encourage people to think of the impact to the things they value:*

- ✓ *Personal information like their bank account information, passwords and PINs.*
- ✓ *Passwords to Internet services like e-Mail, social networking sites, online stores and auction sites.*
- ✓ *Some users are most concerned with their pictures and music (think of teenagers, youth who do not have bank accounts).*

Focus on what a person considers valuable – what they worry about that exists on their computer, and what would happen if it wasn't available because of Malware.

## References

[http://malware.wikia.com/wiki/Timeline\\_of\\_noteworthy\\_computer\\_viruses,\\_worms\\_and\\_Trojan\\_horses](http://malware.wikia.com/wiki/Timeline_of_noteworthy_computer_viruses,_worms_and_Trojan_horses)

## Slide 14



### Criminals Use Malware

- ★ **Criminals use Malware for financial gain.**
  - ★ Redirect your Internet traffic for "Pay-per-Click" schemes
  - ★ Send e-Mail SPAM
  - ★ Attack company or government computer systems
  - ★ Disable networks and websites



[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

Today, much of malware is driven by criminal activity. Malicious software is used to collect personal and confidential information that can be sold for profit. Internet browsing is re-directed for monetary gains – many advertising programs pay money for every visitor to a website. Redirecting traffic can generate money for the owner of a site.

Botnets are frequently used to distribute SPAM or phishing e-mails which can cause congestion of networks, and lead people to websites that propagate even more malware! Botnets have also been used to attack specific websites in an attempt to make them unusable or unreachable. Since botnets often consist of thousands of computers working together, they can cause serious disruption to networks and websites.

### References

<http://www.symantec.com/business/theme.jsp?themeid=threatreport>  
<http://www.honeynet.org/node/52>

## Slide 15



**What Can Malware Steal?**

- ★ Malware is used by criminals to infect your computer and look for valuable information.
  - ★ Personal information such as bank account or payment card numbers, passwords, PINs.
  - ★ Trade secrets and intellectual property
  - ★ Anything that is stored on your computer

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

The goal of most criminals is to find a way to steal money. There are cyber-crime groups which write malicious software for specific tasks. This type of malicious software will look for anything of value on your computer. It typically will search for personal information, or try to direct you to sites which ask you to input personal information. More sophisticated tools will look for certain keywords that may indicate trade secrets, new product designs, or other information that can be sold to competitors.

## References

<http://www.symantec.com/business/theme.jsp?themeid=threatreport>

## Slide 16

# How To Protect Yourself From Malware

## Discussion points

This is the start of Section 3, 'How to Protect Yourself From Malware'

## References

N/A

## Slide 17



**Protect Your Computer**

- ★ **Keep Your Computer and Backups Up to Date**
  - ★ Regularly apply patches from your operating system and application vendors.
  - ★ Configure your browser to block pop-up windows.
  - ★ Backup your files and programs regularly so you can recover if anything happens.

Remember to Check for Updates Today!

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

By regularly applying manufacturer's patches for your operating system and applications you eliminate the way that most malicious software infects your computer. Most malicious software looks for vulnerabilities and weaknesses that exist in operating systems and applications. By fixing these problems you can minimize the opportunity malware has to infect your system. Be aware that every operating system and application has some vulnerability, and that it is almost impossible to discover and correct every vulnerability or weakness. Sometimes people discover these vulnerabilities before the manufacturer finds them, and instead of telling the manufacturer, they write a program to exploit the vulnerability. Be aware that applying patches is not the only defence, and is only one step in protecting yourself.

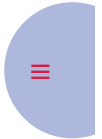
By configuring your browser to block pop-up windows you reduce the possibility of a site displaying a pop-up with malware embedded in it, or with links that will install malicious software. This, like patches is only a





partial fix to the problem. Blocking pop-ups only address one possible way that malware can be presented to a user. An attacker can still place the malware on a main page of a website and achieve the same results. The only advantage to a pop-up is that it makes the situation seem far more immediate and urgent to a user and encourages them to take action based on the pop-up window. By blocking pop-up windows you reduce one tool in an attacker's bag of tricks as they attempt to infect your computer with malware.

Backing up your file and programs regularly can help you avoid a disaster if your system ever is infected. If malware cannot be removed from your system you may have to re-install the entire system. Doing so may destroy all your files. A backup will ensure that you can restore these files. Be careful when restoring the files that you do not re-infect your system, as your backup may contain the file that contains the malware.



## References

<http://www.microsoft.com/windowsxp/using/networking/security/protect.msp>

<http://www.cert.org/homeusers/HomeComputerSecurity/>



## Slide 18



 **Protect Your Computer**

- ★ Install a reputable anti-virus, anti-spyware, browser filter, and personal firewall product.
  - ★ Update virus definition at least once a day
  - ★ Perform a full scan of your computer every week
  - ★ Alert you of dangerous websites
- ★ Beware of fake antivirus product offers



[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

Installing full featured personal computer security products that offer anti-virus, anti-malware, anti-spyware, browser filters, website alerting, and personal firewalls will give you a high level of protection. There are many reputable companies who produce these types of products.

In order for them to be effective however, they must be updated regularly. This includes virus definitions, and software updates as they are released. Configure the software carefully. The frequency suggested here are minimums. Updating your virus definitions more frequently can help address outbreaks quickly, and full scans (or scans performed when your computer is idle) help ensure ongoing protection.

Personal computer security and anti-virus products are not full-proof. They cannot detect all malware. Some malware is disguised as Trojans – programs that look normal but which really contain malicious software

inside. It is still important for you to be aware and avoid common user mistakes that result in malware infections.

Some sites will present pop-up windows that tell you that your computer is infected with a virus, and you need to download the software they offer to clean the infection. In reality their software will install the infection. Only use reputable anti-virus software vendors.

## References

<http://www.microsoft.com/windowsxp/using/networking/security/protect.aspx>

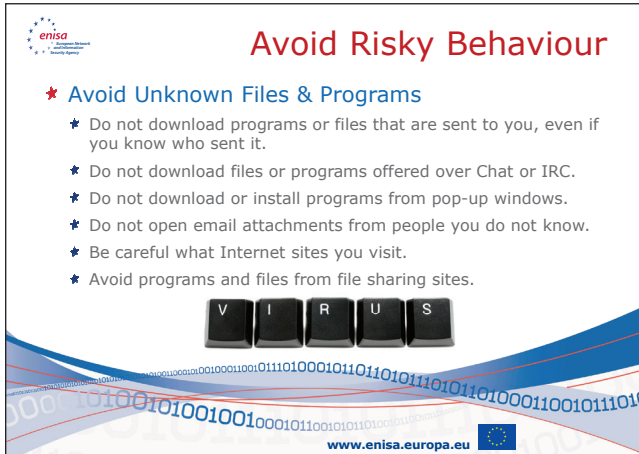
<http://www.cert.org/homeusers/HomeComputerSecurity/>

[http://malware.wikia.com/wiki/Rogue\\_security\\_software](http://malware.wikia.com/wiki/Rogue_security_software)

<http://www.symantec.com/business/theme.jsp?themeid=threatreport>



## Slide 19



### Avoid Risky Behaviour

- ★ **Avoid Unknown Files & Programs**
  - ★ Do not download programs or files that are sent to you, even if you know who sent it.
  - ★ Do not download files or programs offered over Chat or IRC.
  - ★ Do not download or install programs from pop-up windows.
  - ★ Do not open email attachments from people you do not know.
  - ★ Be careful what Internet sites you visit.
  - ★ Avoid programs and files from file sharing sites.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

One of the most common methods of spreading malware is through e-Mail attachments. Even files sent by people you know can contain malware. They may not recognize it because the malware wasn't detected by their anti-virus tool, or they use a different type of computer than you. But the malware still exists and can affect your computer.

You may be asked to download a file containing some enticing picture, music or program. These invitations are usually an attacker attempting to spread malware. The same applies to some pop-up windows that state your computer is infected with a virus, and you need to quickly download their software to remove the malware. In reality their software will install the malware. Many sites which carry controversial content also contain malware.

File sharing sites also contain a large percentage of infected files. While it can be enticing to be able to download the latest music, pictures or pro-

grams, the high probability and risk of infecting your system with malware should be considered.

Always be careful when you are asked to download or install a file. There is a good possibility that it contains malware. The best recommendation? Avoid files from untrusted sources, and always be sceptical.

## References

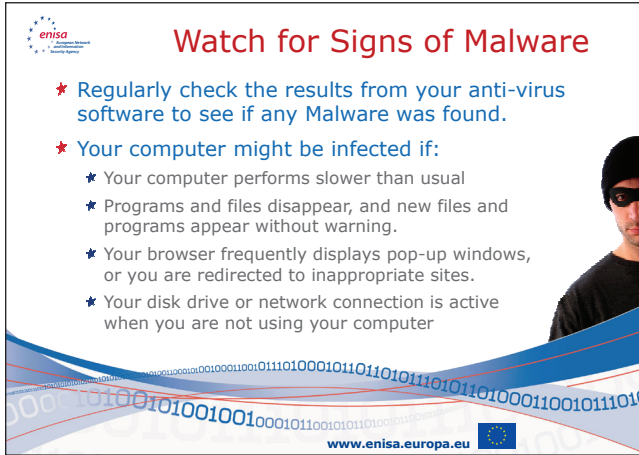
[http://malware.wikia.com/wiki/Rogue\\_security\\_software](http://malware.wikia.com/wiki/Rogue_security_software)

<http://www.us-cert.gov/cas/tips/ST05-007.html>

<http://www.wired.com/techbiz/media/news/2004/01/61852>



## Slide 20



### Watch for Signs of Malware

- ★ Regularly check the results from your anti-virus software to see if any Malware was found.
- ★ Your computer might be infected if:
  - ★ Your computer performs slower than usual
  - ★ Programs and files disappear, and new files and programs appear without warning.
  - ★ Your browser frequently displays pop-up windows, or you are redirected to inappropriate sites.
  - ★ Your disk drive or network connection is active when you are not using your computer

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

There are many signs that malware has infected your system. Some are very easy to see – check the logs and reports from your anti-virus software to see if it found any Malware. In some rare cases it may report that it could not fix or remove some malware. Usually it will report when malware was detected. Notice what when the infection happened and what file was infected, and if it corresponds to some activity you were doing. It may be associated with an email, a website you visited, software you ran, or a file you downloaded. Be very aware of what actions might have caused the infection and be careful not to repeat them.

Poor computer performance can be an indication of malware using computer resources (memory, processing time, and transmitting via the network). If your disk drive is active when you are not using your computer, it may be a sign of malicious software. Also note however that many anti-virus programs will scan you disks for malware automatically if you leave your computer idle for a period of time. If you frequently see undesirable

pop-up windows or are redirected to undesirable websites there is a good possibility that you are infected with Spyware, Adware or other Malware.

## References

<http://www.viruslist.com/en/viruses/encyclopedia?chapter=153280800>



## Slide 21



**If Your Computer is Infected**

- ★ If Your Computer is Infected
  - ★ Disconnect your computer from the network.
  - ★ Use a CD copy of Anti-Virus to scan and clean your computer.
  - ★ If you cannot remove the malicious software, take the computer to a professional who can help you.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

*Instructor: These are best practices for handling viruses and are directed at the average user. This example is applicable more for home users since in a company environment the user would have already engaged the helpdesk, incident response team, or any other applicable groups or individuals.*

It is our recommendation that you discuss with the security officer the current procedures within the company for handling an incident, and include those in the training.

Instruct the attendees to follow the company incident response procedures – e.g. who to notify, what other steps to take such as writing down what they were doing before the noticed the infection, what symptoms or issues they noticed before discovering their system was infected. While a good incident response plan is outside the scope of this paper, it is critical for any business to be able to respond to an incident like a virus outbreak.





If you find your computer is infected, always first disconnect the computer from the network. This will limit the ability of the malicious software to spread and limit the damage it can cause to other systems.

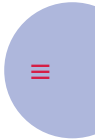
Use a CD copy of anti-virus to scan and clean your computer. By using a CD copy you can be certain that the anti-virus software has not been affected by the malicious software. Anti-virus software is one of the first things that malware will target in order to disable any attempt to remove or stop the malware. By using a copy of the malware that cannot be altered (on an original installation CD) you can be reasonably certain that the malware cannot alter the anti-virus software.

If the anti-virus software is unable to detect and remove the malware, contact a computer professional who can help you remove the software. Avoid attempting to remove the software yourself unless you are trained to do so. Many different types of malware are very resistant to removal. They will hide in different locations, and even avoid detection and removal after a new operating system removal. A professional can help identify the malware, and choose an appropriate response to eradicate it.

## References

<http://www.viruslist.com/en/viruses/encyclopedia?chapter=153280800>

<http://www.onguardonline.gov/topics/malware.aspx>



## Slide 22



Resources

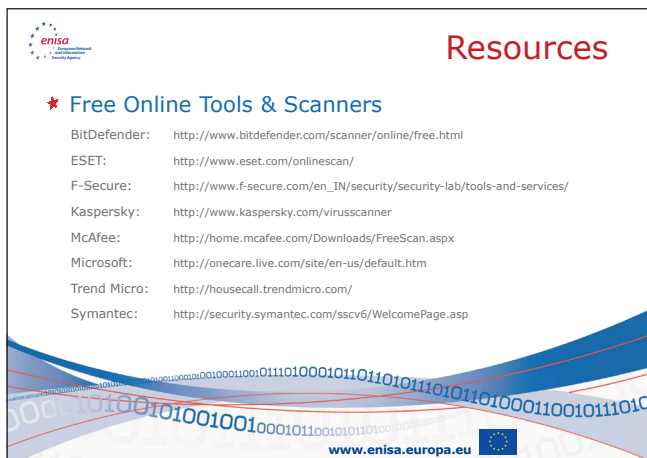
### Discussion points


This is the start of Section 4 which lists some resources if you are dealing with Malicious Software.

### References

N/A

## Slide 23



 **Resources**

★ **Free Online Tools & Scanners**

BitDefender: <http://www.bitdefender.com/scanner/online/free.html>

ESET: <http://www.eset.com/onlinescan/>

F-Secure: [http://www.f-secure.com/en\\_IN/security/security-lab/tools-and-services/](http://www.f-secure.com/en_IN/security/security-lab/tools-and-services/)


Kaspersky: <http://www.kaspersky.com/virusscanner>

McAfee: <http://home.mcafee.com/Downloads/FreeScan.aspx>

Microsoft: <http://onecare.live.com/site/en-us/default.htm>

Trend Micro: <http://housecall.trendmicro.com/>

Symantec: <http://security.symantec.com/sscv6/WelcomePage.asp>

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

*Instructor: This is a list of well known online virus scanning tools made available by various anti-virus vendors. This list is provided purely as an example of possible solutions, and does not constitute an endorsement or guarantee of any kind for that vendor.*

## References

N/A

## Slide 24



Conclusion

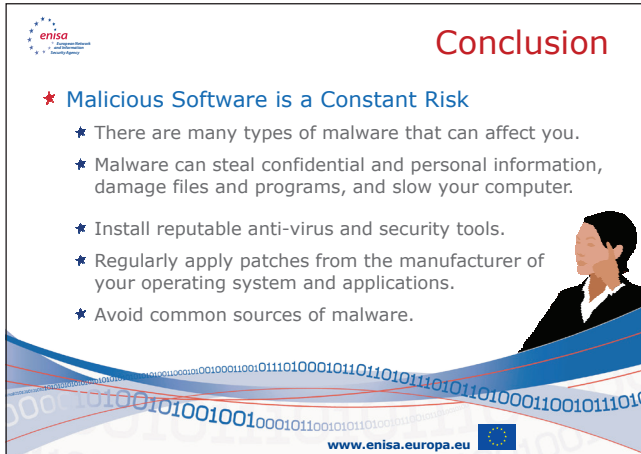
### Discussion points

This is the conclusion of the presentation.

### References

N/A

## Slide 25



### Conclusion

- ★ **Malicious Software is a Constant Risk**
  - ★ There are many types of malware that can affect you.
  - ★ Malware can steal confidential and personal information, damage files and programs, and slow your computer.
  - ★ Install reputable anti-virus and security tools.
  - ★ Regularly apply patches from the manufacturer of your operating system and applications.
  - ★ Avoid common sources of malware.

www.enisa.europa.eu

## Discussion points

*Instructor: This is a summary slide that provides an opportunity to repeat the key themes of the presentation.*

As we pointed out in this presentation, there are many different types of malicious software that can affect you and your computer.

We discussed how malware can steal confidential and personal information, can damage files and programs, and slow down, or even cause your computer to stop running.

And we talked about key ways to protect yourself:

Install reputable anti-virus and security tools.

Regularly apply patches from the manufacturer of your operating system and applications so you can stay up to date.

And lastly, avoid common sources of malware including fraudulent e-mails, malicious or suspicious websites, and free files offered through file sharing, chat or pop-up windows.

## References

N/A

## Slide 26



## Discussion points

N/A

## References

N/A





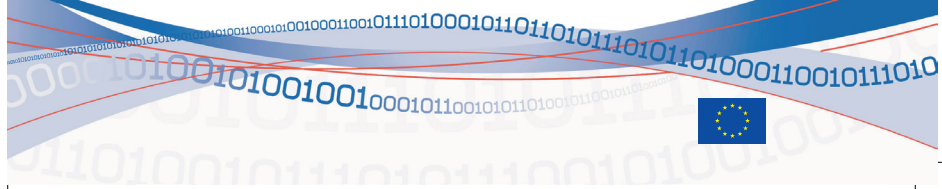


# Online security at home

---

## *Train the trainer reference guide*

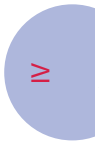
February | 10







# **Online security at home: Train the trainer reference guide**



*February 2010*





# Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>161</b>
<b>HOW TO USE THIS MANUAL .....</b>	<b>162</b>
STRUCTURE OF THE MANUAL .....	162
STRUCTURE OF THE PRESENTATION PAGES .....	162
<b>THE PRESENTATIONS SLIDES .....</b>	<b>163</b>
SLIDE 1 .....	163
SLIDE 2 .....	164
SLIDE 3 .....	165
SLIDE 4 .....	166
SLIDE 5 .....	167
SLIDE 6 .....	168
SLIDE 7 .....	169
SLIDE 8 .....	170
SLIDE 9 .....	171
SLIDE 10 .....	172
SLIDE 11 .....	174
SLIDE 12 .....	176
SLIDE 13 .....	178
SLIDE 14 .....	179
SLIDE 15 .....	180
SLIDE 16 .....	181
SLIDE 17 .....	183
SLIDE 18 .....	185
SLIDE 19 .....	187
SLIDE 20 .....	189
SLIDE 21 .....	191
SLIDE 22 .....	192
SLIDE 23 .....	193
SLIDE 24 .....	194
SLIDE 25 .....	195





## Executive summary

This training reference guide has been created by ENISA in conjunction with presentation materials for small and medium enterprises to raise awareness with their employees about crucial and important issues regarding the use of the Internet at home.

These documents are designed to provide easy to understand information that focuses employees' attention on information security and encourages them to recognise and respond accordingly to threats.

This material may be used by individuals or presented in a classroom setting by instructors who are involved in their organisation's security awareness efforts. This reference guide provides additional notes and external references for trainers and presenters to utilize while performing security awareness training.

## How to use this manual

This manual is intended to be a guide for instructors of any security awareness course based on ENISA's Online security at home presentation. This manual is only a guide, and instructors are welcome to use any portion of this material they deem appropriate. It is at the instructor's discretion how to conduct the course and which material to present.

It should be noted however that ENISA recommends that the instructor carefully consider the skills and knowledge of the students being taught in developing the course. The material should be tailored to fit the needs of the students including making it easy to understand, relevant to their position and responsibilities.

ENISA has chosen focus this material on the general user community outside of the Information Technology field. As such, this presentation focuses on the fundamentals of the use of Internet at home and avoids the use of complex technical terms to explain risks or solutions.

### Structure of the manual

This manual broken into two parts:

1. How to use this manual (this section)
2. The presentation slides with associated supporting material

### Structure of the presentation pages

Each of the presentation pages are broken in to three parts:

1. The thumbnail of the slide from the presentation
2. Suggested narratives that provide supporting information and discussion points
3. Reference materials that support the slide that can be used to do further research



## The presentations slides

### Slide 1



### Discussion points

This is a good time to have the attendees introduce themselves.

When everyone is introducing themselves, ask them what they use the internet for the most at home, and what do they expect to get from the course. The answers will tell you what scenarios you can use as examples for this course, and what their expectations are for this course. This information is very useful so that you can adjust your discussions accordingly.

### References

N/A

## Slide 2

### About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the Agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

### Contact details

For contacting ENISA or for general enquiries on information security awareness matters, please use the following details:

Isabella Santa, Senior Expert Awareness Raising - E-mail: [awareness@enisa.europa.eu](mailto:awareness@enisa.europa.eu)

Internet: <http://www.enisa.europa.eu>

### Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA regulation ((EC) No 460/2004). This publication does not necessarily represent the state of the art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2010.

## Discussion points

Introduce ENISA and their activities. Suggest that attendees should examine some of ENISA's other presentations on other aspects of network and information security.

## References

<http://www.enisa.europa.eu> – ENISA's website



### Slide 3



**enisa**  
European Network  
and Information  
Security Agency

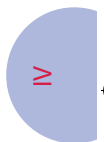
## Overview

This presentation discusses the importance of security while using the Internet at home and highlights simple techniques that individuals can employ to protect themselves and their families.

The presentation is divided into two sections:

- ★ **Why Security Is Important**
- ★ **How to Protect Yourself and Your Family**

[www.enisa.europa.eu](http://www.enisa.europa.eu)



### Discussion points

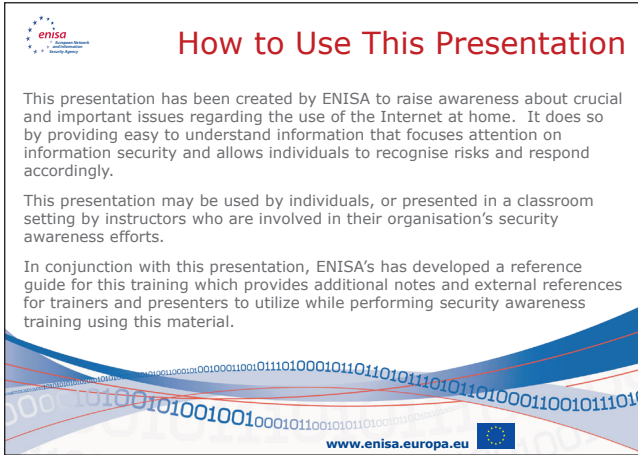
Point out that this presentation is intended to make users aware of the most common and pervasive risks when using the Internet at home, and also simple techniques that can eliminate a large percentage of these risks. Point out that the course is intended for all users, and that it can help each of them use the Internet at home.


### References

N/A



## Slide 4




 **How to Use This Presentation**

This presentation has been created by ENISA to raise awareness about crucial and important issues regarding the use of the Internet at home. It does so by providing easy to understand information that focuses attention on information security and allows individuals to recognise risks and respond accordingly.

This presentation may be used by individuals, or presented in a classroom setting by instructors who are involved in their organisation's security awareness efforts.

In conjunction with this presentation, ENISA's has developed a reference guide for this training which provides additional notes and external references for trainers and presenters to utilize while performing security awareness training using this material.

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

This slide is an introduction, and is intended to inform readers that a presentation guide (this document) exists to support instructors in their security awareness efforts.

## References

N/A

## Slide 5



Why is Security Important?

### Discussion points

This is the start of Section 1, 'Why is Security Important?'

### References

N/A

## Slide 6



**Using Internet at Home: Benefits**

- ★ We use our home computers for many tasks:
  - ★ Home businesses
  - ★ Online Banking
  - ★ Paying Bills
  - ★ Shopping
  - ★ Social Networking
  - ★ Music & Media downloads
  - ★ Information surfing

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

*Instructor: This is a good time to repeat the answers that were given at the beginning of the session - how the participants use the Internet at home.*

It is not difficult to recognize that the Internet is an important part of our personal lives. The statistics back this assumption. Most countries in the EU have more than 50% of their citizens as Internet users. The European region has the highest number of Internet users per 100 inhabitants than any other region in the world.

The most frequent use of the Internet is for communicating, followed by entertainment, informative, and social networking activities.

## References

[http://www.itu.int/dms\\_pub/itu-d/opb/ind/D-IND-RPM.EUR-2009-R1-PDF-E.pdf](http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-RPM.EUR-2009-R1-PDF-E.pdf)

<http://www.internetworldstats.com/stats.htm>

## Slide 7



 **Using Internet at Home: Risks**

★ With those benefits come risks:

- ★ Viruses
- ★ Malicious Websites
- ★ Spyware & Pop-Ups
- ★ Spam
- ★ Online Scams and Fraud
- ★ Inappropriate Content

[www.enisa.europa.eu](http://www.enisa.europa.eu) 


### Discussion points

These risks are among many that exist, and new ones appear all the time. Awareness is a critical step in being safe. Training like this course can make you aware of how to respond to these risks and threats. The more trained and aware you are, the better prepared you will be when you encounter one of these threats.

### References

N/A


## Slide 8




### Why Should I Worry?

“I don’t have anything valuable on my computer.”

- ★ Malicious programs and websites will collect any information they can find on your computer.
- ★ Infected computers are often used to attack other systems.
- ★ Viruses and other malicious software can make your computer stop working, delete important documents, programs, music, pictures, and any other files or data on your computer.
- ★ How valuable is your lost time and information?



www.enisa.europa.eu 

## Discussion points

*Instructor: Users may think they do not have anything valuable on their computer, but ask them this series of questions.*

- a) *What do you use your computer for?*
- b) *What if you couldn't use it to do that?*
- c) *What things do you save on your computer (i.e. music, pictures, email addresses)?*
- d) *What if you lost that information and all of it was destroyed?*
- e) *How frustrated would you be if the computer became unusable?*
- f) *How much of your time would be wasted if any of these things happened?*

*The realisation for most users is when they recognize the things that they actually value. Teenagers do not think they have something valuable on their computer until a virus destroys their music and pictures and disables the computer and making their social networking sites inaccessible.*

## References

N/A



## Slide 9



**enisa**  
European Network  
and Information  
Security Agency

### Everyone Needs Security

“But I use XYZ Operating System. I am okay.”

- ★ Every operating system (Mac OS , Linux, Windows) has weaknesses and is susceptible to malicious software.
- ★ Many attacks target web-browsers.
- ★ An attack or virus that does not work on one system can work on another, and you could infect your friends.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

In reality, every operating system and application has vulnerabilities. Each operating system has different types of issues, but in the end, they are all susceptible to outside attackers and malicious software. Different malicious software is designed for different operating systems and applications.

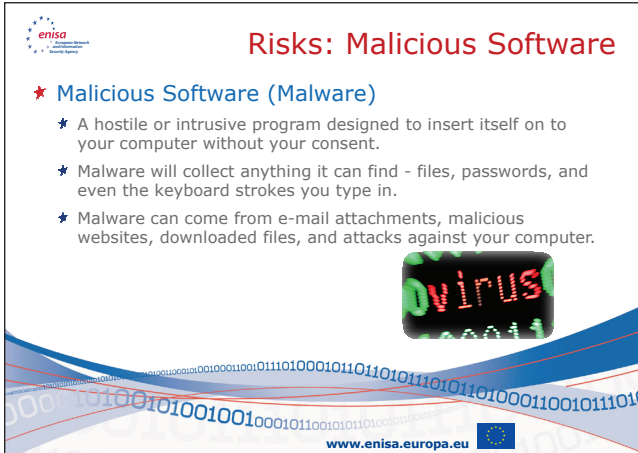
One point to note is that research of known and reported vulnerabilities for all operating systems shows a very interesting story. There is no clear winner, and all systems have issues, which is why everyone needs security.

### References

<http://web.nvd.nist.gov/view/vuln/statistics>

<http://blogs.zdnet.com/Ou/?p=165>


## Slide 10



**Risks: Malicious Software**

- ★ **Malicious Software (Malware)**
  - ★ A hostile or intrusive program designed to insert itself on to your computer without your consent.
  - ★ Malware will collect anything it can find - files, passwords, and even the keyboard strokes you type in.
  - ★ Malware can come from e-mail attachments, malicious websites, downloaded files, and attacks against your computer.

**Virus**

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

It is important to point out that a program is malware if it meets one of two criteria:

- ✓ Is it hostile or intrusive
- ✓ Is it inserted on to your computer without your consent

A program can be Malware if it inserted itself on to your computer without your consent. It also (obviously) is malicious software if it is hostile or intrusive; which means it will perform hostile activities – deleting data or files, attacking other computers, or performing any other actions you do not consent to.

Throughout the presentation we will use the term Malware since it is easier to say. Malware is a combination of two words: **Malicious** and **Software**.



Malware is a difficult problem because it is created by programmers around the world. Some are searching for fame; some are curious programmers who do not see any harm in what they do. However, in recent years the most frequent type of malware is used by criminals to steal information, disrupt computer systems, or perpetuate fraud. Malware has been increasing at a rapid pace year after year, and shows no sign of slowing down. Because programmers are constantly creating new malware it is virtually impossible to completely eliminate malware.

**Fun Fact:** First recorded virus: Creeper Virus in 1971

## References

<http://technet.microsoft.com/en-us/library/dd632948.aspx>

<http://en.wikipedia.org/wiki/Malware>

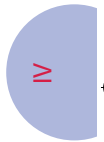
[http://malware.wikia.com/wiki/Main\\_Page](http://malware.wikia.com/wiki/Main_Page)

Good source for malicious software statistics:

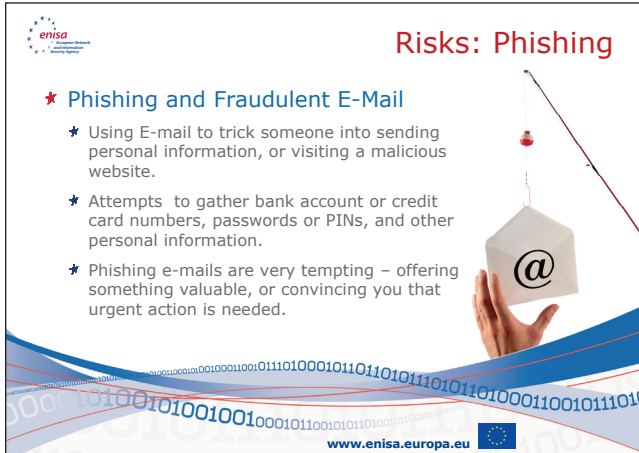
<http://www.symantec.com/business/theme.jsp?themeid=threatreport>

An excellent timeline showing the history of malicious software:

[http://malware.wikia.com/wiki/Timeline\\_of\\_noteworthy\\_computer\\_viruses,\\_worms\\_and\\_Trojan\\_horses](http://malware.wikia.com/wiki/Timeline_of_noteworthy_computer_viruses,_worms_and_Trojan_horses)



## Slide 11



**Risks: Phishing**

- ★ **Phishing and Fraudulent E-Mail**
  - ★ Using E-mail to trick someone into sending personal information, or visiting a malicious website.
  - ★ Attempts to gather bank account or credit card numbers, passwords or PINs, and other personal information.
  - ★ Phishing e-mails are very tempting – offering something valuable, or convincing you that urgent action is needed.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

Phishing is a very wide-spread problem. It is a technique that attempts to convince someone to send personal information that can be used for Identity Theft or fraud. Phishing emails come in many different forms, but the two most typical techniques are:

- ✓ Requesting assistance to recover a large sum of money, or requiring your personal information so they can transfer a large sum of money. The e-mail will entice you with an offer of reimbursement in large sums of money, and thanks you for your efforts. It may appear to be from a solicitor, a relative of a wealthy person or family, a company requiring assistance in collecting money or funds, or an organization looking to award you a prize or award.
- ✓ Informing you that your account has been compromised or urgently requesting that you verify your bank or payment card account. The email attempts to convince you that the situation is urgent, and that you need to confirm your account number, password, or your PIN of the account in order to ensure the account's security.



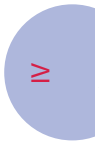
Many of the messages come from people you have never met before, or banks where you do not even do business.

SPAM is a very large problem. SPAM is any e-mail which comes from sources we did not ask to send us e-mails or that we did not give our consent. It accounts for over 80% of all e-mail traffic. Companies spend a large amount of time and money to combat SPAM and filtering it is considered a standard part of e-mail operations. SPAM consumes a large amount of resources (network traffic to handle these messages, disk space to store the messages, and processing power of the people who must view, roll their eyes, and delete the e-mail). SPAM can be another source of fraud as many of the advertisements and offers in SPAM e-mails is for websites that sell non-existent products, or entice you to visit sites which contain malicious programs.

Malicious software can be delivered in an e-mail message through infected e-mail attachments, images in the e-mail or in the HTML used in the e-mail. Criminals have figured out how to manipulate the content of images and HTML to take advantage of vulnerabilities and weaknesses in many popular e-mail programs. By taking advantage of these vulnerabilities and weaknesses, they are able to insert malicious software onto the victim's computer.

## References

- <http://en.wikipedia.org/wiki/Phishing>
- <http://hackers.org/blog/20060609/how-phishing-actually-works/>
- [http://ec.europa.eu/information\\_society/policy/ecom/todays\\_framework/privacy\\_protection/spam/](http://ec.europa.eu/information_society/policy/ecom/todays_framework/privacy_protection/spam/)
- <http://www.spamlaws.com/eu.shtml>
- <http://spam.abuse.net/>
- <http://www.radicati.com/wp/wp-content/uploads/2009/05/email-stats-report-exec-summary.pdf>
- [http://www.cert.org/tech\\_tips/home\\_networks.html#III-B-6](http://www.cert.org/tech_tips/home_networks.html#III-B-6)



## Slide 12



**Risks: Social Networks**

- ★ **The Internet is a Public Place**
  - ★ Information posted on social-networking sites is available to anyone who has access to it.
  - ★ Once information is posted, others can save it, and search engines can gather it and will save it for a long time.
  - ★ E-mail is not a secure method of communication and can be viewed by anyone.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

Social networks are, in themselves not necessarily a risk, but rather our behaviour in using them is what makes them a risk.

The information that is placed there is virtually impossible to remove. It also is collected by search engines, and can be viewed by almost anyone. Once it enters in to the world of the search engines, it is virtually impossible to remove.

The way we communicate using chat, instant messaging, and e-mail is susceptible to fraud, but also to people who would wish to collect the information we send. E-mail especially was never designed to be secure, and has no method to make sure the information we send is kept confidential, no method to validate the identity of the sender of an e-mail, and no way to ensure a message is not changed before we receive it.

## References

<http://www.enisa.europa.eu/act/it/oar/social-networks/security-issues-and-recommendations-for-online-social-networks>

<http://www.enisa.europa.eu/media/press-releases/instantly-online-17-golden-rules-for-mobile-social-networks>



## Slide 13



### Risks: File Sharing

- ★ Downloading or using illegal copies of software, movies, or music can result in serious consequences.
  - ★ The entertainment industry has been very aggressive about prosecuting people who illegally share and download copyright music and movies.
  - ★ Penalties for illegal use of copyright material include fines, legal fees, and potential jail time.
  - ★ Files downloaded from file sharing sites are a major source of malicious software.



[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

File sharing sites also contain a large percentage of infected files. While it can be enticing to be able to download the latest music, pictures or programs, the high probability and risk of infecting your system with malware should be considered.

Most importantly, many of the files may be subject to copyrights. Downloading them, even unknowingly could make you liable for fines and other legal action.

## References

<http://www.us-cert.gov/cas/tips/ST05-007.html>

<http://www.wired.com/techbiz/media/news/2004/01/61852>



## Slide 14



How Should I Protect Myself?

### Discussion points

This is the start of Section 2, 'How Should I Protect Myself?'

### References

N/A

## Slide 15



 **How Should I Protect Myself?**

- ★ **Be Vigilant and Cautious**
  - ★ Even some security experts have become victims
  - ★ The cause – a momentary lapse of vigilance
  - ★ Keep a reminder next to your computer – a poster, or a note
  - ★ Follow some common simple steps to stay secure

*Be Secure!*

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

Being aware of security risks and being vigilant are the most important steps. Many people, even experts have relaxed, and the result has been damaging and time consuming.

Learn what you can through these courses, and be secure at all times.

### References

N/A

## Slide 16



### Secure Your Computer

- ★ **Configure Your Computer Properly**
  - ★ Follow the manufacturer's suggestions for securing the system.
  - ★ Ask the company that sold you the computer for help.
  - ★ Always keep the operating system and any applications you have "patched" and updated.
  - ★ Backup your computer regularly.



[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

Follow the manufacturer's instructions – there are many sources, and they publish numerous guides on how to secure their operating systems, applications, and tools.

By regularly applying manufacturer's patches for your operating system and applications you eliminate the way that most malicious software infects your computer. Most malicious software looks for vulnerabilities and weaknesses that exist in operating systems and applications. By fixing these problems you can minimize the opportunity malware has to infect your system. Be aware that every operating system and application has some vulnerability, and that it is almost impossible to discover and correct every vulnerability or weakness. Sometimes people discover these vulnerabilities before the manufacturer finds them, and instead of telling the manufacturer, they write a program to exploit the vulnerability. Be aware that applying patches is not the only defence, and is only one step in protecting yourself.

By configuring your browser to block pop-up windows you reduce the possibility of a site displaying a pop-up with malware embedded in it, or with links that will install malicious software. This, like patches is only a partial fix to the problem. Blocking pop-ups only address one possible way that malware can be presented to a user. An attacker can still place the malware on a main page of a website and achieve the same results. The only advantage to a pop-up is that it makes the situation seem far more immediate and urgent to a user and encourages them to take action based on the pop-up window. By blocking pop-up windows you reduce one tool in an attacker's bag of tricks as they attempt to infect your computer with malware.

Backing up your file and programs regularly can help you avoid a disaster if your system ever is infected. If malware cannot be removed from your system you may have to re-install the entire system. Doing so may destroy all your files. A backup will ensure that you can restore these files. Be careful when restoring the files that you do not re-infect your system, as your backup may contain the file that contains the malware.

## References

<http://www.microsoft.com/windowsxp/using/networking/security/protect.msp>

<http://www.cert.org/homeusers/HomeComputerSecurity/>

## Slide 17



### Install Security Tools

- ★ **Install Security Tools to Protect Your System**
  - ★ Install a personal firewall to protect against attacks.
  - ★ Install anti-virus tools to detect and remove malicious software from your system and E-Mail.
  - ★ Use website advisory & parental controls tools to guide your family's Internet usage. These tools can control content, what programs are used, and when.
  - ★ Many products combine these tools together into one package.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

Installing computer security products that offer anti-virus, anti-malware, anti-spyware, browser filters, website alerting, and personal firewalls will give you a high level of protection. There are many reputable companies who produce these types of products.

In order for them to be effective however, they must be updated regularly. This includes virus definitions, and software updates as they are released. Configure the software carefully. The frequency suggested here are minimums. Updating your virus definitions more frequently can help address outbreaks quickly, and full scans (or scans performed when your computer is idle) help ensure ongoing protection.

Personal computer security and anti-virus products are not full-proof. They cannot detect all malware. Some malware is disguised as Trojans – programs that look normal but which really contain malicious software

inside. It is still important for you to be aware and avoid common user mistakes that result in malware infections.

Some sites will present pop-up windows that tell you that your computer is infected with a virus, and you need to download the software they offer to clean the infection. In reality their software will install the infection. Only use reputable anti-virus software vendors.

## References

<http://www.microsoft.com/windowsxp/using/networking/security/protect.mspix>

<http://www.cert.org/homeusers/HomeComputerSecurity/>

[http://malware.wikia.com/wiki/Rogue\\_security\\_software](http://malware.wikia.com/wiki/Rogue_security_software)

<http://www.symantec.com/business/theme.jsp?themeid=threatreport>

## Slide 18



**Handle E-Mail With Care**

- ★ **Links and attachments in e-mail are dangerous**
  - ★ Don't open e-Mail attachments from people you do not know.
  - ★ Make sure your anti-virus software scans your email.
  - ★ Do not click on links in e-Mails. Use addresses you have verified and know to be legitimate.
  - ★ If you must click on a link, check the link before clicking on it. Make sure it is legitimate. Attackers often make very subtle changes to confuse you.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

E-mail is a very popular way to spread malicious software. Some e-mails are intentionally created to spread infected files and programs. Some e-mails are from friends who unintentionally spread malicious software by sending you files, videos, or music that is infected. You must be very careful since even these 'trusted' sources of e-mails can spread malicious software.

Never open e-mail attachments from people you do not know. Even if you do know them, think twice before opening the e-mail. Is the attachment a file you were expecting? Does it look like a file that could be a typical type of infected software (Zip files, videos, and files with strange names or file extensions)?

Make sure your anti-virus software is configured to scan your e-mail. Even with anti-virus software scanning the e-mail, not all malicious software can be identified. Some files contain types of malicious software that is unique or has never been seen before, and therefore would not be detected. If in doubt, do not open the attachment.

Do not click on links in e-mails. Links in emails are not always what they seem to be. The website address that displays in the e-mail is not necessarily the same as the link behind that is hidden behind that link. The link may read 'http://www.mybank.com' but the link is actually connected to 'http://goto.hackersite.com'. Many of these links direct you to malicious websites that will attempt to install malicious software onto your computer. Always examine the links in e-mails.

If you hold your cursor over the link in the e-mail the actual hyperlink will usually display in a small helper window. Examine the information that is displayed in the pop-up helper window to see if it indicates that the email is fraudulent. Some clues that will tell you if the e-mail is fraudulent:

- ✓ Is the link in the pop-up helper window different from the link displayed in the e-mail?
- ✓ Does the link appear to be misspelled?
- ✓ Is the link not relevant to the message?
- ✓ Are there misspellings in the e-mail?
- ✓ Is the e-mail specifically addressed to 'undisclosed-recipients' or someone else?

These items can help you identify a fraudulent e-mail. If you find these discrepancies, delete the e-mail. If you are still not sure if the e-mail is fraudulent or not, contact the sender through the phone, or through a method you know is legitimate. Do *\*not\** click on the link or respond directly to the e-mail.

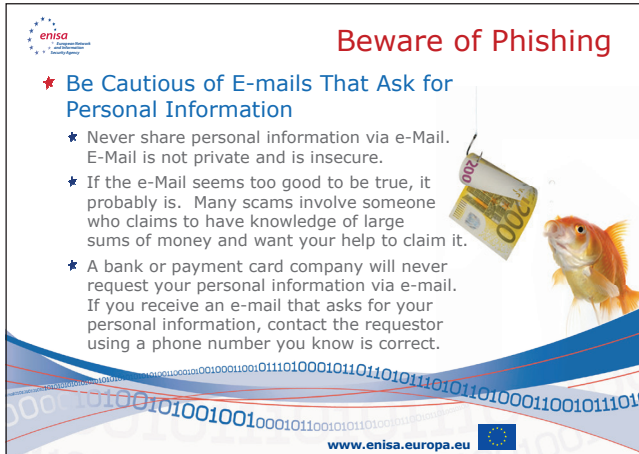
*Instructor: A good demonstration would be to show an example of a link that has a display name, but the actual hyperlink behind it is different. Show the audience the 'pop-up' display that shows the actual hyperlink and how to read it.*

## References

- [http://www.phishtank.com/what\\_is\\_phishing.php](http://www.phishtank.com/what_is_phishing.php)
- <http://office.microsoft.com/en-us/outlook/HA011400021033.aspx>
- <http://portal.acm.org/citation.cfm?id=1242572.1242660>



## Slide 19



### Beware of Phishing

- ★ **Be Cautious of E-mails That Ask for Personal Information**
  - ★ Never share personal information via e-Mail. E-Mail is not private and is insecure.
  - ★ If the e-Mail seems too good to be true, it probably is. Many scams involve someone who claims to have knowledge of large sums of money and want your help to claim it.
  - ★ A bank or payment card company will never request your personal information via e-mail. If you receive an e-mail that asks for your personal information, contact the requestor using a phone number you know is correct.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

*Instructor: Point out that his slide refers to Phishing and SPAM.*

Any e-mail that asks for personal information should be treated very carefully or deleted.

When you receive an e-mail that appears too good to be true, it probably is. A good indication is if the e-mail is from someone you do not know. Most likely they have sent the same e-mail to hundreds of other unsuspecting people. The message will entice you with offers of money that are hard to resist and rewards that you can normally only dream of – an enticement that draws you into making decisions you wouldn't normally make.

Phishing e-mails may also attempt to scare you or rush you into action by telling you that your account has been compromised, or by insisting that you validate your account information for a new security system they are

putting in place. The message will convey a sense of urgency which is intended to rush you into making a decision you wouldn't normally make.

Keep in mind: no bank or payment card company will ever ask you to send personal information, passwords or PINs via email. These types of companies are typical targets for criminals using phishing. Many banks and payment card companies will post news of the newest phishing attacks. If you are unsure if the e-mail you received is a phishing e-mail, then contact the company that the e-mail allegedly came from using a phone number you know to be true. Do not use e-mail and do not use the address or phone number in the e-mail. If you need to, look up the phone number in a phone book. By using this method, you will ensure the authenticity of the company you are speaking to, and you can verify the authenticity of the original email.

## References

<http://en.wikipedia.org/wiki/Phishing>

<http://office.microsoft.com/en-us/outlook/HA011400021033.aspx>

[http://www.phishtank.com/what\\_is\\_phishing.php](http://www.phishtank.com/what_is_phishing.php)

<http://www.antiphishing.org/>

<http://www.ftc.gov/bcp/edu/multimedia/video/ogol/phishing/index.shtml>

## Slide 20



**Think Before You Click**

- ★ **Think Before You Click**
  - ★ Be Cautious What Websites You Visit – if the subject matter is controversial or risqué, the risks are usually higher.
  - ★ File Sharing sites are often the source of malicious software.
- ★ **Use Available Tools to Give You Guidance**
  - ★ Parental Control tools can block inappropriate websites
  - ★ Website advisory tools can tell you when sites are dangerous

www.enisa.europa.eu

### Discussion points

One of the most common methods of spreading malware is through e-mail attachments. Even files sent by people you know can contain malware. They may not recognize it because the malware wasn't detected by their anti-virus tool, or they use a different type of computer than you. But the malware still exists and can affect your computer.

You may be asked to download a file containing some enticing picture, music or program. These invitations are usually an attacker attempting to spread malware. The same applies to some pop-up windows that state your computer is infected with a virus, and you need to quickly download their software to remove the malware. In reality their software will install the malware. Many sites which carry controversial content also contain malware.

File sharing sites also contain a large percentage of infected files. While it can be enticing to be able to download the latest music, pictures or pro-

grams, the high probability and risk of infecting your system with malware should be considered.

Always be careful when you are asked to download or install a file. There is a good possibility that it contains malware. The best recommendation? Avoid files from untrusted sources, and always be sceptical.

## References

[http://malware.wikia.com/wiki/Rogue\\_security\\_software](http://malware.wikia.com/wiki/Rogue_security_software)

<http://www.us-cert.gov/cas/tips/ST05-007.html>

<http://www.wired.com/techbiz/media/news/2004/01/61852>

## Slide 21



**enisa**  
European Network  
and Information  
Security Agency

### Help Your Family Be Safe

- ★ **Help Your Family Be Safe**
- ★ Be aware of what they are doing, communicate openly about how they should use the Internet, and discuss why.
- ★ Teach them to not share passwords, even with their best friend.
- ★ Teach your children to be careful and let you know about any communication from people they do not know.
- ★ Warn them about the penalties of downloading illegal copies of software, movies, or music.

[www.enisa.europa.eu](http://www.enisa.europa.eu)



### Discussion points

There are many good resources for talking to your children about their use of the Internet. The most important step is to talk to them openly about what is acceptable and what is not.

Teach them the same security habits and awareness that you are gathering, and teach them to be very wary of strangers.

### References

[http://www.enisa.europa.eu/act/ar/deliverables/2009/cop\\_initiative](http://www.enisa.europa.eu/act/ar/deliverables/2009/cop_initiative)

<http://www.us-cert.gov/cas/tips/ST05-002.html>

<http://www.staysafeonline.org/>

<http://www.microsoft.com/protect/familysafety/default.aspx>

## Slide 22



### Help Your Family Be Safe

- ★ Talk with your family about safe online habits
  - ★ Help your kids understand that the Internet is a public area.
  - ★ Help them understand what information should be kept private. Remind them that their address, age, schools, identification numbers, bank and payment card information, and phone numbers are all private.
  - ★ Discuss with them the right ways and wrong ways to communicate through e-Mail, social networking sites, and instant messaging.



[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

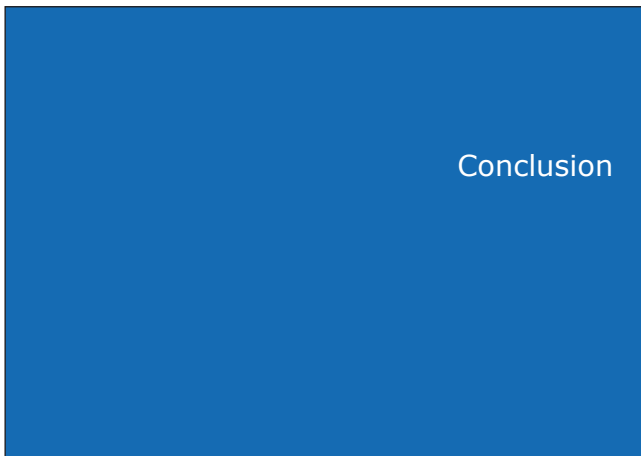
Children often do not recognize risks as we do since they are typically very trusting. The awareness you instil in them should consider the risks, and also good habits. These habits should not only include caution, but also good etiquette when using e-mail, social networks, and other communications.

Help your children understand the issues that are associated with using the Internet. Help them understand what personal information is and should be kept private. There are many good sources of information and presentations available through ENISA to help you in this task.

## References

<http://www.enisa.europa.eu/media/press-releases/2008-prs/children-on-virtual-worlds>

## Slide 23



### Discussion points

This is the conclusion of the presentation.

### References

N/A

## Slide 24



 **Online Security is Important**

- ★ **Online Security while at home is important**
  - ★ Be aware of how to be safe and secure
  - ★ Be vigilant and always cautious
  - ★ Secure your computer
  - ★ Handle e-mail with care
  - ★ Surf the Internet carefully
  - ★ Teach your family to also be secure

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

*Instructor: This is a summary slide that provides an opportunity to repeat the key themes of the presentation.*

Awareness is the most important step in being secure when using the Internet at Home. Your awareness will help you be vigilant and cautious.

Take basic steps to protect yourself and prevent issues.

Secure your computer by configuring it properly, keeping it updated, and all security tools installed and enabled.

Handle e-mail and surf the Internet with care. Be cautious and aware.

Lastly, teach your family the same skills – how to be aware and careful. Your whole family will benefit from this information.

## References

N/A



## Slide 25



## Discussion points

N/A

## References

N/A





# Preventing identity theft

February | 10

*Train the trainer reference guide*







## **Preventing identity theft: *Train the trainer reference guide***



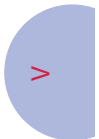
*February 2010*





# Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>203</b>
<b>HOW TO USE THIS MANUAL .....</b>	<b>204</b>
STRUCTURE OF THE MANUAL .....	204
STRUCTURE OF THE PRESENTATION PAGES .....	204
<b>THE PRESENTATIONS SLIDES .....</b>	<b>205</b>
SLIDE 1 .....	205
SLIDE 2 .....	206
SLIDE 3 .....	207
SLIDE 4 .....	208
SLIDE 5 .....	209
SLIDE 6 .....	210
SLIDE 7 .....	212
SLIDE 8 .....	214
SLIDE 9 .....	216
SLIDE 10 .....	218
SLIDE 11 .....	220
SLIDE 12 .....	221
SLIDE 13 .....	222
SLIDE 14 .....	223
SLIDE 15 .....	224
SLIDE 16 .....	226
SLIDE 17 .....	227
SLIDE 18 .....	228
SLIDE 19 .....	229
SLIDE 20 .....	231
SLIDE 21 .....	232
SLIDE 22 .....	233
SLIDE 23 .....	234
SLIDE 24 .....	235
SLIDE 25 .....	236
SLIDE 26 .....	237
SLIDE 27 .....	238
SLIDE 28 .....	240







## Executive summary

This training reference guide has been created by ENISA in conjunction with presentation materials for small and medium enterprises to raise awareness with their employees about crucial and important issues regarding identity theft.

These documents are designed to provide easy to understand information that focuses attention on the security of personal information and helps individuals to recognise and respond accordingly to threats.

This material may be used by individuals or presented in a classroom setting by instructors who are involved in their organisation's security awareness efforts. This reference guide provides additional notes and external references for trainers and presenters to utilize while performing security awareness training.



## How to use this manual

This manual is intended to be a guide for instructors of any security awareness course based on ENISA's Preventing Identity Theft presentation. This manual is only a guide, and instructors are welcome to use any portion of this material they deem appropriate. It is at the instructor's discretion how to conduct the course and which material to present.

It should be noted however that ENISA recommends that the instructor carefully consider the skills and knowledge of the students being taught in developing the course. The material should be tailored to fit the needs of the students including making it easy to understand, relevant to their position and responsibilities.

ENISA has chosen focus this material on the general user community outside of the Information Technology field. As such, this presentation focuses on the fundamentals of identity theft and avoids the use of complex technical terms to explain risks or solutions.

### Structure of the Manual

This manual broken into two parts:

1. How to use this manual (this section)
2. The presentation slides with associated supporting material

### Structure of the Presentation Pages

Each of the presentation pages are broken in to three parts:

1. The thumbnail of the slide from the presentation
2. Suggested narratives that provide supporting information and discussion points
3. Reference materials that support the slide that can be used to do further research

## The presentations slides

### Slide 1



### Discussion points

This is a good time to have the attendees introduce themselves.

When everyone is introducing themselves, ask them if they think they have ever been a victim of identity theft, and what do they expect to get from the course. The answers will tell you what scenarios you can use as examples for this course, and what their expectations are for this course. This information is very useful so that you can adjust your discussions accordingly.

### References

N/A

## Slide 2

### About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the Agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

### Contact details

For contacting ENISA or for general enquiries on information security awareness matters, please use the following details:

Isabella Santa, Senior Expert Awareness Raising - E-mail: [awareness@enisa.europa.eu](mailto:awareness@enisa.europa.eu)

Internet: <http://www.enisa.europa.eu>

### Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA regulation ((EC) No 460/2004). This publication does not necessarily represent the state of the art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2010.

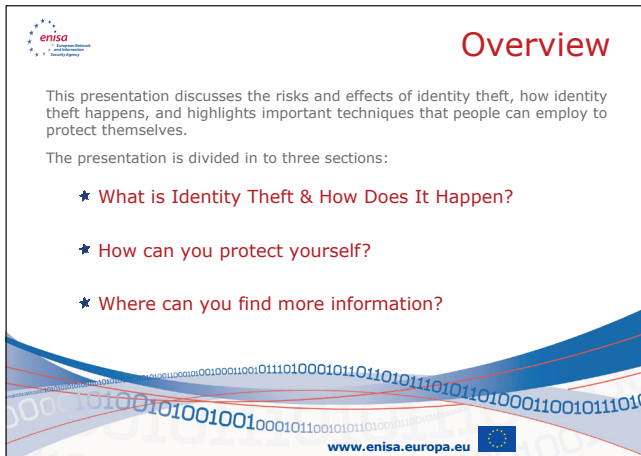
## Discussion points

Introduce ENISA and their activities. Suggest that attendees should examine some of ENISA's other presentations on other aspects of network and information security.

## References

<http://www.enisa.europa.eu> – ENISA's website

### Slide 3



**enisa**  
European Network  
and Information  
Security Agency


## Overview

This presentation discusses the risks and effects of identity theft, how identity theft happens, and highlights important techniques that people can employ to protect themselves.

The presentation is divided in to three sections:

- ★ What is Identity Theft & How Does It Happen?
- ★ How can you protect yourself?
- ★ Where can you find more information?

[www.enisa.europa.eu](http://www.enisa.europa.eu)




### Discussion points

Point out that this presentation is intended to make users aware of the most common and pervasive risks from identity theft, and also simple techniques that can eliminate a large percentage of these risks. Point out that the course is intended for all users, and that it can help protect each of them from identity theft.

### References

N/A

## Slide 4





### How to Use This Presentation

This presentation has been created by ENISA to raise awareness about crucial and important issues regarding the use of e-mail. It does so by providing security good practices to focus employees' attention on information security and allow them to recognise security concerns and respond accordingly.

This presentation may be used by individuals, or presented in a classroom setting by organisations who are involved in their organisation's security awareness efforts.

In conjunction with this presentation, ENISA's has developed a reference guide for this training which provides additional notes and external references for trainers and presenters to utilize while performing security awareness training using this material.



[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

This slide is an introduction, and is intended to inform readers that a presentation guide (this document) exists to support instructors in their security awareness efforts.

## References

N/A

## Slide 5



What is Identity Theft?

### Discussion points


This is the start of Section 1, 'What is Identity Theft?'

### References

N/A





## Slide 6



### What is Identity Theft?

- ★ Someone uses your identity or pretends to be you, usually to commit fraud or other crimes
- ★ They will use your identification to:
  - ★ Open new credit card or bank accounts
  - ★ Obtain mobile, telecom or utility services
  - ★ Make fraudulent purchases in your name
  - ★ Obtain fraudulent identification papers
  - ★ Claim rights or privileges to which you are entitled



www.enisa.europa.eu 

### Discussion points

*Instructor: Point out to everyone that they may have already been a victim of identity theft and not thought of it that way. Use the examples below to demonstrate the different types of identity theft. Ask people in the room to raise their hand if they have every had this done to them.*

Identity theft is not just a complete assumption of someone else's identity, but also the fraudulent use of their credentials and financial information. Fraudulent use of someone else's payment card is a very prevalent type of identity theft.

Once someone has the ability to use your identity, the most likely things they will do are:

**Credit Card fraud (26%):** when someone acquires your credit card number and uses it to make a purchase.



**Utilities fraud (18%):** utilities accounts are opened in someone else's name.

**Bank fraud (17%):** check/bank draft theft, altering check, theft of ATM access codes.

**Employment fraud (12%):** using someone else's identity to obtain a job.

**Loan fraud (5%):** applying for a loan using someone else's identity.

**Government fraud (9%):** fraudulently acquiring tax benefits or refunds, government benefits, identification documents, and driver licenses.

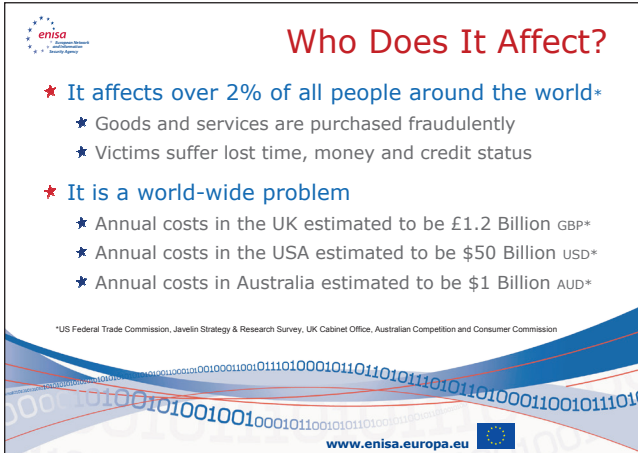
**Other (13%)**

## References

<http://www.spendonlife.com/guide/2009-identity-theft-statistics>




## Slide 7



**Who Does It Affect?**

- ★ It affects over 2% of all people around the world\*
  - ★ Goods and services are purchased fraudulently
  - ★ Victims suffer lost time, money and credit status
- ★ It is a world-wide problem
  - ★ Annual costs in the UK estimated to be £1.2 Billion GBP\*
  - ★ Annual costs in the USA estimated to be \$50 Billion USD\*
  - ★ Annual costs in Australia estimated to be \$1 Billion AUD\*

\*US Federal Trade Commission, Javelin Strategy & Research Survey, UK Cabinet Office, Australian Competition and Consumer Commission

www.enisa.europa.eu 

## Discussion points

The Javelin Strategy & Research Survey, CERT surveys and US Federal Trade Commission estimate that between 2 to 4% of all people around the world are affected by Identity Theft.

The victims of identity theft suffer lost time in addressing the debts and loans the thief has put in their name, and correcting their credit status. The time spent is time away from work, from families and things that are important in their lives.

Fraud also costs businesses who must absorb the costs of the fraud. These costs, coupled with the costs to the victims are extremely large.

## References

<http://www.spendonlife.com/guide/identity-theft-statistics>

[http://www.idtheftcenter.org/artman2/publish/m\\_press/Identity\\_Theft\\_The\\_Aftermath\\_2008.shtml](http://www.idtheftcenter.org/artman2/publish/m_press/Identity_Theft_The_Aftermath_2008.shtml)

<http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf>

<http://www.identity-theft.org.uk/>

[http://www.cifas.org.uk/default.asp?edit\\_id=968-56](http://www.cifas.org.uk/default.asp?edit_id=968-56)

<http://www.crimereduction.homeoffice.gov.uk/theft1.htm>



## Slide 8



**What Information Is Stolen?**

- ★ An Identity Thief wants any information that allows him to impersonate someone else
  - ★ Home Address and Phone number
  - ★ Date of Birth
  - ★ Government identification numbers
  - ★ Financial account numbers
  - ★ Payment card numbers
  - ★ Account Passwords or PINs
  - ★ Medical Information

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

Thieves are interested in any information that grants access to financial benefits. Home addresses and phone numbers give information that can be used to impersonate someone.

Date of Birth and identification numbers can be used to copy or forge a new identity that can be used to establish new credit, open accounts, or even transfer and steal money from the real person.

Financial account numbers and payment card numbers coupled with account passwords and PIN's give criminals direct access to money which is ultimately their goal.

Medical information, government identification, and other information can be used to collect services to which you are entitled.


The identity thief will use this information to impersonate you by knowing enough information to be able to convince someone that they are indeed you.

## References

N/A





## Slide 9



### How Does It Happen?

- ★ **Thieves will gather information from many places**
  - ★ Stolen wallets, checkbooks, and payment cards
  - ★ Theft of postal mail
  - ★ Digging through garbage (Dumpster diving)
  - ★ Dishonest employees who sell information
  - ★ Theft of computers and computer equipment
  - ★ Tampering with payment card terminals or ATMs
  - ★ Social Engineering
  - ★ Computer break-ins by Cyber-Criminals
  - ★ Viruses, Malicious Websites and Spyware



www.enisa.europa.eu 

### Discussion points

According to surveys performed in several countries, stolen wallets, checkbooks and payment cards are the primary source of personal information when the victim can identify the source of the identity theft. 43% of victims knew the person who stole their identity.

Thieves will go through people's mailboxes looking for checks, bank statements, and payment card applications. They will use this information to forge checks, change addresses, and apply for payment cards.

Thieves will rummage through garbage bins of people and companies looking for any information that is useful such as discarded documents, bills, or anything else that contains personal information. Many documented cases occur every year where thieves will dig through garbage bins and find personal or confidential information. What is more surprising is that this information is so easy to find.

The market for personal information is very profitable and large. Criminals around the world are eager to pay for this information, and thieves are eager to steal it for them. The money is enticement to dishonest employees who will sell it to make money. Thieves will tamper with payment card terminals and ATMs and place devices in them to collect payment card numbers and PINs. Some ingenious thieves will use social engineering – which is the technique of persuading someone to do something they wouldn't normally do, such as give you their personal information, account numbers, passwords, and information needed to perform identity theft.

There are also technical attacks that collect information from computers and servers. These computers that are compromised can be a user's personal computer, or can be large company systems. Several recent examples of computer incidents have resulted in significant loss of personal information.

## References

<http://www.spendonlife.com/guide/identity-theft-statistics>

<http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf>

[http://www.cifas.org.uk/default.asp?edit\\_id=968-56](http://www.cifas.org.uk/default.asp?edit_id=968-56)

<http://www.crimereduction.homeoffice.gov.uk/theft1.htm>



## Slide 10



### Risk: Mail and Garbage

- ★ **Stealing Postal Mail or**

Thieves will steal postal mail for the personal information.

Thieves will also steal postal mail to collect offers for bank accounts and payment cards and then submit the offers with fraudulent addresses.
- ★ **Searching Garbage Bins**

Thieves will search garbage bins to find personal information that is thrown away.

A survey in the UK found that 96% of all garbage bins contained personal information that could be used by identity thieves.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

Thieves will actually lie in wait for postal mail delivery and collect the mail from postal boxes. They will search for anything that looks like it might contain personal information, or any offers for payment cards, loans or other financial services. They will fill out applications for financial services and forge the information to redirect the services to themselves.

Searching garbage bins is not only an issue for individuals, but also for companies. Many highly publicised incidents have occurred where competitors have hired investigators to search through a company's garbage for information about operations, new product designs, and any competitive knowledge or trade secrets. The documents that they find give them a considerable amount of valuable insight.

## References

<http://www.identitytheft.info/securingmail.aspx>





Preventing identity theft:  
Train the trainer reference guide

---



219

<http://www.deseretnews.com/article/1,5143,600129714,00.html>

<http://www.msnbc.msn.com/id/4460349/>

[http://en.wikipedia.org/wiki/Dumpster\\_diving](http://en.wikipedia.org/wiki/Dumpster_diving)

<http://www.combat-identity-theft.com/uk-identity-theft-statistics.html>



## Slide 11



### Risk: Phishing & E-Mail

- ★ **Phishing**  
Using e-Mail to trick someone in to sending personal information or visiting a malicious website.
- ★ **Phishing e-mails are very creative**
  - ★ Someone requests you to help them collect a large sum of money, and requesting banking information from you.
  - ★ An alert from a bank, payment card company or online site that claims your account has been compromised and you need to verify your PIN, or reset your password.
  - ★ Mortgage or loan company offering low rates if you provide your detailed financial information.





[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points


Phishing is a type of social engineering. It is a method of convincing someone to do something they wouldn't otherwise do. By using various types of enticements they convince people to send them confidential and personal information. The enticement of a large amount of money, or the urgency of your bank account being affected causes some people to make rash and unwise choices. These types of emails circulate on a daily basis.

*Instructor: Bring some examples of phishing e-mails either that you have received, or that you can collect from the sources we provide in the references.*

## References


- <http://antivirus.about.com/od/emailscams/ss/phishing.htm>
- <http://en.wikipedia.org/wiki/Phishing>
- <http://www.irs.gov/newsroom/article/0,,id=155682,00.html>
- <http://www.technicalinfo.net/papers/Phishing.html>


## Slide 12



### Risk: Malware

- ★ **Malicious Software**
  - ★ Many types of malicious software will collect personal information from a victim's computer.
  - ★ Some malicious software will monitor what the user types, or what sites he visits.



[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

Malicious software are programs that are installed on your computer without your knowledge or consent. The programs that collect personal information is typically called spyware or keyloggers. This type of software is specifically designed to search for personal information, and in fact many modern versions of malicious software are specifically designed to focus only on personal information.

### References

- <http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=219400767>
- [http://www.antiphishing.org/reports/APWG\\_CrimewareReport.pdf](http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf)
- <http://www.spywareguide.com/articles/identity-theft-spyware-2.php>
- <http://blogs.zdnet.com/security/?p=1598>
- <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>

## Slide 13



### Risk: Hijacked ATMs

- ★ Tampering with ATM or Payment Card Terminals
  - ★ Thieves will attach devices to ATMs or Payment Card Terminals that will record the Payment Card Number.
  - ★ Thieves will install cameras or watch people as they use ATMs and Payment Card Terminals to collect their PINs.



[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

Tampering with ATM or Payment Card Terminals is a worldwide problem. Thieves will use a wide variety of tools such as skimmers, key and data loggers, and cameras to gather data from ATMs and Payment Card Terminals. Some will even use simple tactics of distraction and observation to watch you input your payment card information. New technology has reduced the amount of fraud, but thieves have responded with new tactics.

## References

<http://www.enisa.europa.eu/act/ar/deliverables/2009/atmcrime>  
<http://www.snopes.com/fraud/atm/atmcamera.asp>  
[http://www.schneier.com/blog/archives/2010/01/atm\\_skimmer.html](http://www.schneier.com/blog/archives/2010/01/atm_skimmer.html)  
<http://www.krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/>

## Slide 14



### Discussion points

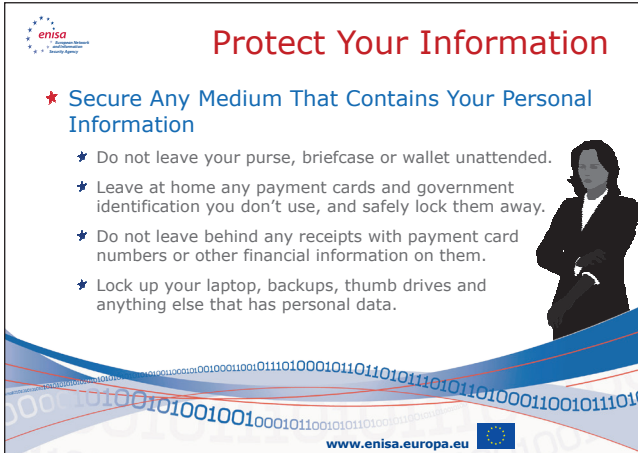
This is the start of Section 1, 'How to Protect Yourself'

### References

N/A




## Slide 15



**Protect Your Information**

- ★ **Secure Any Medium That Contains Your Personal Information**
  - ★ Do not leave your purse, briefcase or wallet unattended.
  - ★ Leave at home any payment cards and government identification you don't use, and safely lock them away.
  - ★ Do not leave behind any receipts with payment card numbers or other financial information on them.
  - ★ Lock up your laptop, backups, thumb drives and anything else that has personal data.

[www.enisa.europa.eu](http://www.enisa.europa.eu)



### Discussion points

Based on the information presented earlier, it is clear that any medium that contains our personal information should be protected. Since most instances of identity theft are the result of stolen wallets, purses and check books, it would seem sensible to reduce the opportunity for someone to steal them.

If you don't need a document or a payment card, reduce your risk and leave it at home locked away safely. This will minimize the opportunity for a thief to steal your information, and if your wallet or purse is stolen, the time you will need to cancel those cards and recover from any damage is greatly reduced.

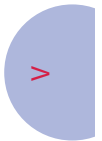
Paper receipts often have payment card numbers printed on them. This information is highly sensitive and should be carefully protected. Never leave a receipt behind at a store, restaurant or terminal. A thief can use

this information to perform identity theft, or even make charges using your number.

Lock up any device that has personal data on it. Never leave it lying about. Make a list of all the devices on which you keep personal data. Reduce the number of devices to only those that are necessary to contain that information. Those that are necessary (actual computer hard disks, and computer backups) should be locked away when they are not in use. In the case of computer backups, ensure they remain secure, as they can potentially hold multiple copies of your personal information if you perform frequent backups.

## References

[http://www.cifas.org.uk/default.asp?edit\\_id=552-56](http://www.cifas.org.uk/default.asp?edit_id=552-56)



## Slide 16



**Secure Your Computer**

- ★ **Install & Maintain Appropriate Security Tools**
  - ★ Anti-Virus & Anti-Spyware Software
  - ★ Anti-SPAM and Anti-Phishing e-Mail Filtering Tools
  - ★ Personal Firewall
  - ★ Web Browser tool that alerts you of malicious sites
  - ★ Regularly install the latest operating system and application patches.
- ★ **Check the security at websites that ask for personal or payment card information.**

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

The appropriate use of security tools will limit your exposure to malicious software which will search out your personal information. It will also limit the ability of an attacker to compromise your system and search for the information themselves. These tools will also help you identify malicious websites that can be the source of malicious software, or are known sites that are targets for phishing scams.

### References

[http://www.cifas.org.uk/default.asp?edit\\_id=552-56](http://www.cifas.org.uk/default.asp?edit_id=552-56)



## Slide 17



**Secure Postal Mail & Garbage**

- ★ **Secure your postal mail**
  - ★ Secure and lock your personal mailbox
  - ★ Don't leave mail in the mailbox for long periods of time
  - ★ Send your outgoing mail from a post office
- ★ **Shred all personal records you discard**
  - ★ Bank and payment card statements
  - ★ Bank or credit card offers
  - ★ Any documents that contain personal information

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

Eliminate the opportunity for someone to find personal information in your garbage bins. Shred any personal information, expired or cancelled payment cards, financial documents, or any other documents that contain personal information. The purchase of a reliable shredder is a worthwhile investment.

Talk to your post office to determine what are good ways to secure your mailbox. If it can't be locked, consider using a postal box at the post office.

Leaving incoming mail, or placing outgoing mail in our mailbox can attract thieves who will collect bills, payment checks, and any documents that contain personal information. Thieves will even take checks and alter them so that they can cash them for themselves.

## References

<http://www.identitytheft.info/securingmail.aspx>

## Slide 18



### Keep Information Private

- ★ **Never give out your personal information**

Companies will never ask you to send the password or PIN to your account via email.

If someone calls and asks for personal information, ask if you can call them back. Then call them back using a telephone number you know to be legitimate.

Unless it is required, do not write down any payment card or government identification numbers on any documents.

Never lend someone your payment cards or government identification.




[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

While it might seem simple enough not to give out our personal information, you would be surprised how often we actually do it. Remember the statistic that 43% of all identity theft is perpetrated by someone we know? How often do you give someone your password, or lend them your payment card? How often do you tell friends information about you that could be used for identity theft. Keep this information private. Information like passwords and PINs should never be shared with anyone.

Never leave behind personal information on documents. Never put them on websites. Think carefully before posting personal information on social networking sites. Ask yourself, what could someone do with this information. Ask yourself, would I normally tell this information to a stranger. The best advice is to keep your personal information private.

### References

N/A

## Slide 19



**Protect Your Passwords**

- ★ **Keep Passwords and PINs private**
  - ★ Do not share passwords or PINs with anyone!
  - ★ Change your account passwords often.
  - ★ Do not use common or easy to guess information as your password or your PIN.
  - ★ Do not keep passwords or PINs in your wallet.
  - ★ Do not let other people watch over your shoulder while you input your password or PIN.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

While it might seem simple enough not to give out our personal information, you would be surprised how often we actually do it. Remember the statistic that 43% of all identity theft is perpetrated by someone we know? How often do you give someone your password, or lend them your payment card? Information like passwords and PINs should never be shared with anyone.

Do not keep this information somewhere that someone could access it. Since wallets and purses are a desirable target for thieves, they are a very bad place to store passwords or PINs. Keeping them in the same place as the payment card is an invitation for an identity thief to instantly get access to your accounts.

Be very careful of people looking over your shoulder or crowding you when you are using an ATM or payment card terminal. If you find that you cannot input your information in privacy, move to another terminal or

ATM where you can have privacy. The inconvenience will be simpler than the inconvenience you could have from identity theft.

## References

N/A

## Slide 20



### Monitor Your Accounts

- ★ Monitor your bank and payment card accounts
  - ★ Save receipts from all charges
  - ★ Review monthly statements immediately
  - ★ Check for unauthorized or suspicious activity
- ★ Monitor your credit history
  - ★ Check for new accounts or debts
  - ★ Check for new enquiries
  - ★ Check for new addresses or names

www.enisa.europa.eu

### Discussion points

While you may behave very securely, there are still situations where your personal information can be stolen and used. There are many publicized situations where companies have lost their customer's personal information.

The best way to protect yourself against these situations is to regularly monitor all your accounts and credit history. Your credit history will inform you of accounts, enquiries, and other activity that may indicate identity theft.

Each country in the EU has their own method of monitoring credit history. Some are set up by the central bank, others through private entities. Identify the one that is most relevant to your area.

### References

[http://ec.europa.eu/internal\\_market/consultations/docs/2009/credit\\_histories/egch\\_report\\_en.pdf](http://ec.europa.eu/internal_market/consultations/docs/2009/credit_histories/egch_report_en.pdf)

## Slide 21



### Report Any Fraud Early

- ★ **As soon as you suspect a problem:**
  - ★ Contact the fraud department at the major credit bureaus and inform them that you're an identity theft victim.
  - ★ Request that a "fraud alert" be placed in your file, along with a victim's statement asking creditors to call you before opening any new accounts or changing existing accounts.
  - ★ File a report with the police and obtain a report number.
  - ★ Keep records of all your efforts, including copies of written correspondence and records of telephone calls.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

Report fraud as soon as you identify it. The earlier you identify it, the earlier it can be stopped, and the damage can be minimized.

Contact the credit agency in your region and determine what steps they can take to help you protect your identity. Each agency has steps they can take ranging from providing reports to putting flags on your profile to alert you if additional situations appear.

### References

[http://www.cifas.org.uk/default.asp?edit\\_id=701-79](http://www.cifas.org.uk/default.asp?edit_id=701-79)

## Slide 22



**Report Financial Fraud Early**

- ★ **If your Bank or Payment Card is affected**
  - ★ Report suspicious items to your bank or payment card company immediately.
  - ★ Request your payment cards be changed.
  - ★ Immediately change your passwords and PINs.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

If you notice fraud through your financial institution, bank, or payment card, notify them immediately. Request that any further charges or drafts be blocked and that all passwords, PINs, and card numbers be changed.

Early notification will limit the impact of the fraud.

### References

N/A

## Slide 23



Resources

### Discussion points

This section presents some resources that people can use to assist with any Identity Theft issues or questions they might have.

### References

N/A



## Slide 24



**Resources: Protect Yourself**

- ★ **Credit Report Resources in the UK**
- ★ Experian Ltd  
Consumer Help Service  
PO Box 9000  
Nottingham  
NG80 7WP
- ★ Equifax Plc  
Credit File Advice Centre  
PO Box 1140  
Bradford  
BD1 5US
- ★ **CIFAS Protective Registration**  
Consider registering with the CIFAS Protective Registration Service. CIFAS Protective Registration may be placed by individuals against their own address when they have good reason to believe it may be used by a fraudster, for example, when a passport has been stolen. For a full explanation of the CIFAS Protective Registration Service, go to [www.cifas.org.uk/pr](http://www.cifas.org.uk/pr)
- ★ Callcredit Ltd  
Consumer Services Team  
PO Box 491  
Leeds  
LS3 1WZ

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

N/A

## References

N/A



## Slide 25



### Resources: Research

- ★ **The EU Fraud Prevention Expert Group** has prepared a report on identity theft and fraud in the financial sector.  
[http://ec.europa.eu/internal\\_market/fpeg/docs/id-theft-report\\_en.pdf](http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf)
- ★ **UK – Home Office Identity Fraud Steering Committee:** This site containing useful information for consumers and traders on identity fraud.  
<http://www.identity-theft.org.uk/>
- ★ **CIFAS** (UK Fraud Prevention Service). In the United Kingdom, the fraud prevention service CIFAS operates a database which is used by the majority of the British financial services industry.  
<http://www.cifas.org.uk/>
- ★ **Cardwatch** is a UK banking industry initiative that aims to raise awareness of card fraud prevention. It is managed by APACS, the UK payments association. The Cardwatch site contains a section on tips for cardholders to avoid identity fraud.  
<http://www.cardwatch.org.uk/>

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

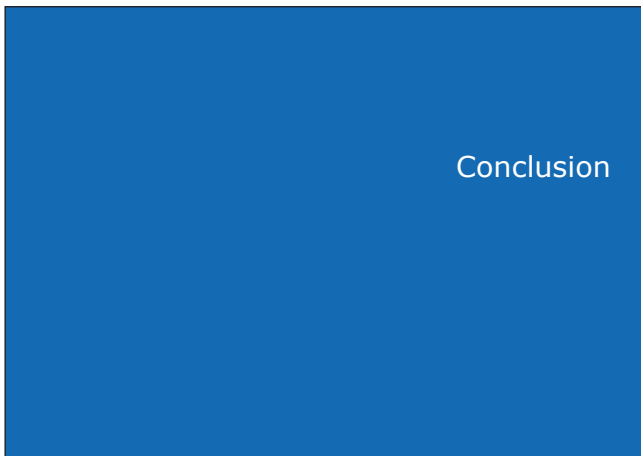
## Discussion points

N/A

## References

N/A

## Slide 26



### Discussion points

This is the conclusion of the presentation.

### References

N/A



## Slide 27



 **You Can Stop Identity Theft**

- ★ Protect Your Personal Documents & Information
- ★ Secure Your Computer
- ★ Protect Your Postal Mail and Garbage
- ★ Keep Personal Information Private
- ★ Protect Your Passwords
- ★ Monitor Your Accounts
- ★ Report Any Suspicious Activity Early

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

*Instructor: This is a summary slide that provides an opportunity to repeat the key themes of the presentation.*

As we talked about in the beginning, Identity Theft is a serious problem with serious consequences. You can reduce the risk associated with Identity Theft by taking some simple precautions.

Protect your personal documents and information by keeping them locked away if they are not needed.

Secure your computer to protect against malicious programs and intruders who look for personal information you store there.

Keep your personal information private and do not share it. This includes passwords, PINs, account numbers, and identification numbers.

Monitor your accounts, and report any suspicious activity early to minimize the damage.

## References

N/A



## Slide 28



## Discussion points

N/A

## References

N/A

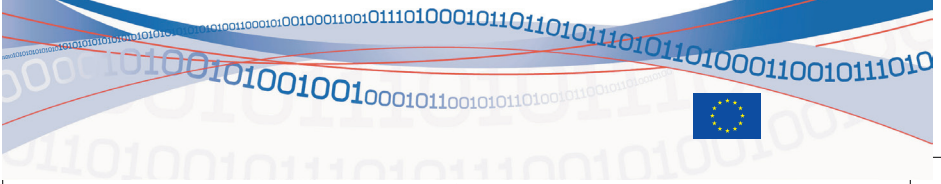


# Security when working remotely

February

10

## Train the trainer reference guide

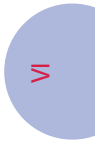








## **Security when working remotely: *Train the trainer reference guide***



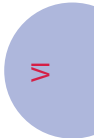
*February 2010*





# Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>247</b>
<b>HOW TO USE THIS MANUAL .....</b>	<b>248</b>
STRUCTURE OF THE MANUAL .....	248
STRUCTURE OF THE PRESENTATION PAGES .....	248
<b>THE PRESENTATIONS SLIDES .....</b>	<b>249</b>
SLIDE 1 .....	249
SLIDE 2 .....	250
SLIDE 3 .....	251
SLIDE 4 .....	252
SLIDE 5 .....	253
SLIDE 6 .....	254
SLIDE 7 .....	255
SLIDE 8 .....	257
SLIDE 9 .....	258
SLIDE 10 .....	260
SLIDE 11 .....	262
SLIDE 12 .....	263
SLIDE 13 .....	265
SLIDE 14 .....	267
SLIDE 15 .....	269
SLIDE 16 .....	270
SLIDE 17 .....	271
SLIDE 18 .....	273





## Executive summary

This training reference guide has been created by ENISA in conjunction with presentation materials for small and medium enterprises to raise awareness with their employees about how to be secure when working remotely.

These documents are designed to provide easy to understand information that focuses employees' attention on information security and encourages them to recognise and respond accordingly to threats.

This material may be used by individuals or presented in a classroom setting by instructors who are involved in their organisation's security awareness efforts. This reference guide provides additional notes and external references for trainers and presenters to utilise while performing security awareness training.

## How to use this manual

This manual is intended to be a guide for instructors of any security awareness course based on ENISA's Security while working remotely presentation. This manual is only a guide, and instructors are welcome to use any portion of this material they deem appropriate. It is at the instructor's discretion how to conduct the course and which material to present.

It should be noted however that ENISA recommends that the instructor carefully consider the skills and knowledge of the students being taught in developing the course. The material should be tailored to fit the needs of the students including making it easy to understand, relevant to their position and responsibilities.

ENISA has chosen focus this material on the general user community outside of the Information Technology field. As such, this presentation focuses on the fundamentals of how to be secure when working remotely and avoids the use of complex technical terms to explain risks or solutions.

### Structure of the manual

This manual broken into two parts:

1. How to use this manual (this section)
2. The presentation slides with associated supporting material

### Structure of the presentation pages

Each of the presentation pages are broken in to three parts:

1. The thumbnail of the slide from the presentation
2. Suggested narratives that provide supporting information and discussion points
3. Reference materials that support the slide that can be used to do further research

## The presentations slides

### Slide 1



**Security  
when working  
remotely**



enisa  
European Network  
and Information  
Security Agency

### Discussion points

This is a good time to have the attendees introduce themselves.

When everyone is introducing themselves, ask them to also say how they use e-mail, and what do they expect to get from the course. The answers will tell you what scenarios you can use as examples for this course, and what their expectations are for this course. This information is very useful so that you can adjust your discussions accordingly.

### References

N/A

### Slide 2

#### About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the Agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

#### Contact details

For contacting ENISA or for general enquiries on information security awareness matters, please use the following details:

Isabella Santa, Senior Expert Awareness Raising - E-mail: [awareness@enisa.europa.eu](mailto:awareness@enisa.europa.eu)

Internet: <http://www.enisa.europa.eu>

#### Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA regulation ((EC) No 460/2004). This publication does not necessarily represent the state of the art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2010.

### Discussion points

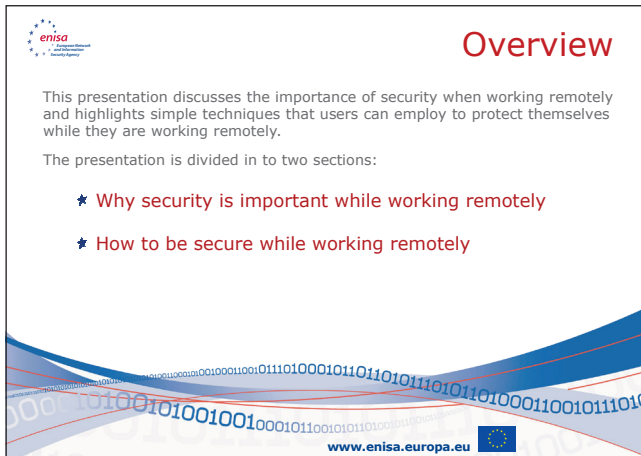
Introduce ENISA and their activities. Suggest that attendees should examine some of ENISA's other presentations on other aspects of network and information security.


### References

<http://www.enisa.europa.eu> – ENISA's website



### Slide 3




 **Overview**

This presentation discusses the importance of security when working remotely and highlights simple techniques that users can employ to protect themselves while they are working remotely.

The presentation is divided in to two sections:

- ★ Why security is important while working remotely
- ★ How to be secure while working remotely

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

The slide features a decorative background with a blue and white wavy pattern and binary code (0s and 1s) overlaid.


### Discussion points

Point out that this presentation is intended to make users aware of the most common and pervasive risks when working remotely, and also simple techniques that can eliminate a large percentage of these risks. Point out that the course is intended for all users, and that it can help each of them work safely and securely while they are remote.

### References

N/A

## Slide 4




### How to Use This Presentation

This presentation has been created by ENISA to raise awareness about crucial and important issues regarding working remotely. It does so by providing easy to understand information that focuses employees' attention on information security and allows them to recognise and respond accordingly to threats while working remotely.

This presentation may be used by individuals, or presented in a classroom setting by instructors who are involved in their organisation's security awareness efforts.

In conjunction with this presentation, ENISA's has developed a reference guide for this training which provides additional notes and external references for trainers and presenters to utilize while performing security awareness training using this material.

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

This slide is an introduction, and is intended to inform readers that a presentation guide (this document) exists to support instructors in their security awareness efforts.

### References

N/A

## Slide 5

# Why Security is Important While Working Remotely

## Discussion points

This is the start of Section 1, 'Why Security is Important While Working Remotely?'

## References

N/A

>

## Slide 6



**Why Be Secure**

- ★ Working Remote Presents Many Risks
  - ★ You are responsible for your own security
  - ★ Public places can have criminals and competitors
  - ★ Lack of preparation can make you an easy target
- ★ Good preparation can limit the risks!

www.enisa.europa.eu 

## Discussion points

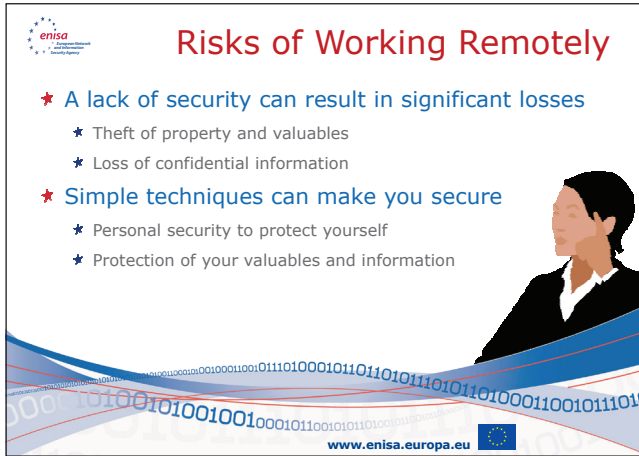
When you work remotely, you are responsible for ensuring the security of yourself, your belongings, and your information. When you work remotely, you do not have the benefit of the security you have in your office. You typically do not often have control over your environment or the people you are around. This makes working remotely more of a risk than your environment at work or at home. Lack of preparation for working remotely can make you an easy target for thieves, pick-pockets, unscrupulous competitors, and other criminals.

Good preparation however can significantly reduce your risks and make your experience far more relaxing and productive.

## References

<http://www.itpro.co.uk/126695/remote-working-is-major-network-security-concern>  
<http://www.itpro.co.uk/187986/remote-working-is-the-chink-in-the-network-armour>

## Slide 7



### Risks of Working Remotely

- ★ A lack of security can result in significant losses
  - ★ Theft of property and valuables
  - ★ Loss of confidential information
- ★ Simple techniques can make you secure
  - ★ Personal security to protect yourself
  - ★ Protection of your valuables and information

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

If you do not have good security habits, you can suffer a significant loss. You can have your property or valuables stolen. This might include your wallet, money, jewellery, and identification documents. You may also lose confidential information you're carrying. The theft of wallets, check books, and the identification cards, payment cards, and bank account information they contain is the main methods of identity theft. The loss of these items can also hamper any plans or travel.

The theft may include a briefcase or a laptop. The information that they contain can include confidential company product plans, customer names, proprietary knowledge, and other items that can be very valuable to a competitor. Even the personal information that is stored there is valuable to a thief. The inconvenience that results can spoil your work and your travel.

What can seem like a simple incident can actually result in a significant problem.

Simple techniques can, however, protect you against many of these security risks. These simple techniques should focus on your personal security to protect yourself, how to protect your valuables and confidential information, knowing where to find assistance when you need it, and having contingency plans in case of emergencies.

### References

N/A

## Slide 8



# How to Be Secure While Working Remotely

## Discussion points

This is the start of Section 2, 'How to Be Secure While Working Remotely'

## References

N/A



<

## Slide 9



**Prepare Yourself**

- ★ Prepare yourself and your materials for any remote work
  - ★ Only take documents that you absolutely need
  - ★ Travel with as few valuables as possible.
  - ★ Lock away any other confidential documents, identification, payment cards, or other personal information you don't need.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

It is important to prepare for any remote work – whether just working from home, or while on the road.

When you are preparing, only pack what you need. Avoid taking any data, documents, information, or valuables that you do not absolutely need while you are away from the office. This will reduce the risk and amount of data that is lost if something does happen to your computer while you are working remotely. It will also reduce the number of things you must worry about and secure.

Know what information is the most sensitive and avoid taking that type of information if at all possible. Information such as your personal identification, customer confidential or personal data, protected information (by law, or regulation), sensitive business plans, and proprietary data should be left at the office. There are numerous examples of employees losing valuable data after taking it home or while working remotely.





By locking away any payment cards, identification or other personal information, you ensure it is safe while you are gone.

## References

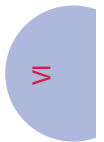
[http://www.cio.com.au/article/184746/fragility\\_road-warrior\\_security](http://www.cio.com.au/article/184746/fragility_road-warrior_security)

<http://www.securityfocus.com/infocus/1186>

<http://fcw.com/Articles/2008/03/03/Stolen-VA-laptop-caught-in-safety-net.aspx>

<http://www.dodbuzz.com/2009/12/22/top-secret-brit-laptop-stolen/>

<http://www.securityfocus.com/news/11393>



## Slide 10



### Prepare Your Computer

- ★ Check that you have prepared your computer to work securely while you are remote
  - ★ Ensure you have a physical computer lock
  - ★ Ensure your operating system is patched, and all security tools and anti-virus are enabled and up-to-date
  - ★ Only take the information that you absolutely need
  - ★ Encrypt the data on your computer
  - ★ Perform a computer data backup before you leave the office

[www.enisa.europa.eu](http://www.enisa.europa.eu)



### Discussion points

If you are taking your computer, it is important to ensure that it is secure. Not only is the computer itself valuable to a thief, but the data contained on it is also valuable to thieves and competitors. Many people have been the victim of computer theft which has resulted in the loss of sensitive company secrets, millions of personal records and information, and government secrets. Proper preparation might have prevented these losses.

A good computer lock will allow you to secure your computer while you are working on it, and will prevent most snatch-and-grab thefts.

Patching your computer and making sure it is up-to-date gives you the most recent security tools before you go on the road. It will minimize the exposure to malware, and attacks when your ability to make updates may be limited.

If you must take confidential or sensitive information and data on your laptop, encrypt it. Your company should be able to provide you with a solution, as many newer operating systems include disk encryption technology, and many third party tools are available as well.

Performing a data backup allows you to restore information if your system is stolen, damaged or has an accident while you are remote. Knowing that any damage to your computer can be mitigated by having a backup of your data can make you breathe a little bit easier.

## References

<http://www.securityfocus.com/infocus/1187>

<http://technet.microsoft.com/en-us/windows/aa905065.aspx>

<http://docs.info.apple.com/article.html?path=Mac/10.4/en/mh1877.html>

<http://www.truecrypt.org/>

<http://www.pgp.com/products/wholediskencryption/>

## Slide 11



**Communicate**

- ★ **Communicate frequently**
  - ★ Communicate your plans and itinerary with office associates and family members
  - ★ Inform them of any changes or status
  - ★ Observe and read any notices from your company or other news sources regarding risks in your area

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

Frequent communication with family members and office associates can ensure that if anything happens to you, there is someone with knowledge of your plans and your itinerary.

Also observe any notices from your company about new policies, procedures, security issues, and other information about how to work remotely. The communication between you, your office, and your co-workers is one of the most important parts about working remotely. Without this communication it is easy to lose touch with important changes, and not hear about necessary information.

### References

[http://homebusiness.about.com/od/workingathome/a/telework\\_gas.htm](http://homebusiness.about.com/od/workingathome/a/telework_gas.htm)  
<http://www.bizjournals.com/stlouis/stories/2009/10/26/smallb1.html?q=telecommuting%20communication>

## Slide 12



**Physical Surroundings**

- ★ Be aware of your physical surroundings
  - ★ Make sure doors to locked areas close behind you
  - ★ Lock your room or office when you step away
  - ★ Do not leave valuables, your computer or important documents unattended in public places, in hotel rooms, or in your car.
  - ★ Be aware of people or activities occurring around you

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

Your physical surroundings can have a very big impact on the security of yourself, your computer, and your belongings. Ensure physical security is in place when you are working. Having locked doors and safe places to work can reduce your stress and allow you to focus on your task at hand.

If you step away, even for a moment, make sure the room or area where you are working is secure. Do not leave doors to rooms open or unlocked.

Never leave valuables such as computers, your mobile phone, thumb drives and other storage devices unattended in a public place. Even when you think an area is secure, still protect these items by keeping them locked up and out of sight. Never leave these items in hotel rooms as staff and outsiders can gain access to your room and remove these items while you are away.

Be aware of your surroundings and the activities occurring around you – they can be good indications if an unsafe situation may be occurring, or of any impending security threats. It is not necessary to be paranoid, but awareness is part of a good defence.

## References

<http://www.securityfocus.com/infocus/1186>

## Slide 13



**Protect Information**

- ★ **Protect your confidential information**
  - ★ Do not work on confidential information in public places
  - ★ Keep information you are not using locked away and out of sight from others around you
  - ★ Do not use public computers for viewing any confidential or personal information
  - ★ Do not let others use your computer

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

If you are carrying confidential or personal information, it is important to protect at all times – when you are using it, or when you are just carrying or storing it.

Public places can be full of people interested in the information you may be working on. Some could be thieves, and others could be your competitor. Some information you may be carrying may be protected by laws and regulations and must be kept confidential. Working on this data in public places exposes it to disclosure. You or your company could be held liable for disclosing that information.

Public computers are not well protected. Previous users may not have used safe habits to surf the Internet, or may have intentionally installed malicious software that collects any sites you visit, any screens you view, or anything you type – including usernames, passwords, bank account

numbers, or any other confidential information. Avoid public computers for any work that involves personal or confidential information.

If you are travelling with your office computer, it is important to not let others use that computer. They can view confidential information that you have stored on it. They can visit malicious websites and install software (intentionally or by accident) that compromise the computer. They may also simply steal the computer from you. Never allow anyone, even family members to use your office computer. It is your responsibility to protect the company's confidential information, and if there is information that is protected by law or regulation, you can be liable for its safety.

## References

<http://www.microsoft.com/atwork/security/laptopsecurity.aspx>


[http://www.cio.com.au/article/184746/fragility\\_road-warrior\\_security](http://www.cio.com.au/article/184746/fragility_road-warrior_security)

[http://holton.it-online.co.za/index.php?option=com\\_content&view=article&id=23%3Akeeping-systems-and-data-safe-and-secure-while-working-remotely&Itemid=1](http://holton.it-online.co.za/index.php?option=com_content&view=article&id=23%3Akeeping-systems-and-data-safe-and-secure-while-working-remotely&Itemid=1)

[http://www.cisco.com/web/CA/pdf/Understanding\\_Remote\\_Worker\\_Security\\_A\\_survey\\_of\\_User\\_Awareness\\_vs\\_Behaviour.pdf](http://www.cisco.com/web/CA/pdf/Understanding_Remote_Worker_Security_A_survey_of_User_Awareness_vs_Behaviour.pdf)






## Slide 14



### Protect Your Computer

- ★ **Protect and secure any device that is valuable or contains confidential information**
  - ★ Use a physical cable lock to secure your computer
  - ★ Never leave your computer, mobile phone, storage devices, or documents unattended
  - ★ Ensure your computer has a screen-saver enabled
  - ★ Install a privacy screen on the computer display
  - ★ Only use company approved secure network connections



[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

Never leave your computer unsecured or unattended. This invites a thief to steal the computer, to attempt to access it, and to not only benefit from the value of the computer, but also the information it contains. Leaving documents or a computer in your car, your hotel room, or any other public place is an invitation for a thief. A single laptop in the United States was stolen from a government employee's home and resulted in the loss of over 1 million personal records and information.

By ensuring your security tools are up-to-date you can minimize the risk while travelling by knowing you have the most recent updates available.

Configuring screensavers and installing privacy screens on your computer display can provide some limited protection when working in public areas where others might be able to see your screen. It will not protect your computer if you leave it unattended. A thief or attacker may still

sneak up to your computer before the screensaver engages and steal or view information.

Avoid connecting to wireless networks – while some may seem secure, there are many locations where wireless networks are actually spoofed sites and malicious sites which monitor everything you do over the network. They will monitor your Internet usage, any messages or information you send, and attempt to intercept connections to secure websites.

*Instructor: Take note of the remote access tools that are available. Identify how a user would request remote access, and what policies and procedures the user must follow.*

To help protect your security while working remotely, only use the company provide secure network connection – which is often referred to as the 'VPN' (Virtual Private Network). If configured correctly, this network will allow you to transmit data securely to and from your company. It does not provide any additional security for your computer, but it will limit the ability of anyone else on the public network (including thieves and attackers) to view your confidential data as it is sent to and from your computer.

## References

<http://www.onguardonline.gov/topics/laptop-security.aspx>

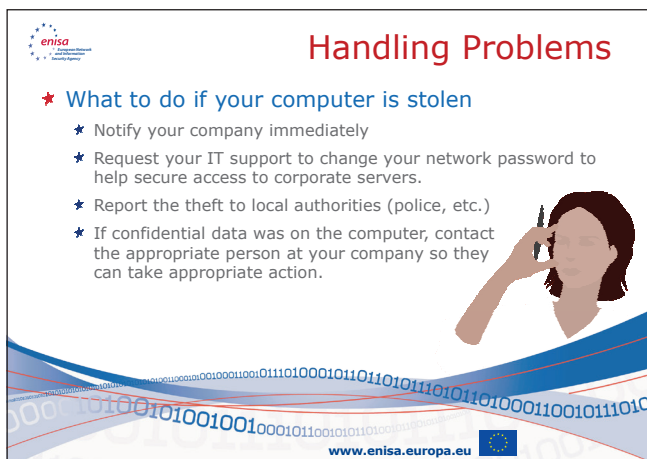
<http://www.microsoft.com/atwork/security/laptopsecurity.aspx>

<http://technet.microsoft.com/en-us/library/cc722662.aspx>

<http://blogs.techrepublic.com.com/10things/?p=335>

<http://www.securityfocus.com/brief/910>

## Slide 15




**enisa**  
European Network  
and Information  
Security Agency

### Handling Problems

- ★ **What to do if your computer is stolen**
  - ★ Notify your company immediately
  - ★ Request your IT support to change your network password to help secure access to corporate servers.
  - ★ Report the theft to local authorities (police, etc.)
  - ★ If confidential data was on the computer, contact the appropriate person at your company so they can take appropriate action.

[www.enisa.europa.eu](http://www.enisa.europa.eu)



### Discussion points

*Instructor: Identify the incident response procedures for the organisation and what steps a user should take if their laptop is stolen.*

If your computer is stolen it is important to report it immediately. Any delay in reporting the laptop theft can create liability for you and the company. Reporting it immediately allows your company and the authorities to respond to the theft quickly and appropriately. Let your company know what information you had on it, when it was stolen and any other facts they need for their investigation.

### References

N/A

## Slide 16



Conclusion

### Discussion points

This is the conclusion of the presentation.

### References

N/A

## Slide 17



**Security is Important**

- ★ Security while working remotely is important
  - ★ Preparation is important so you can protect
    - Yourself
    - Your valuables
    - Your information
  - ★ Be aware of how to be safe and secure

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

*Instructor: This is a summary slide that provides an opportunity to repeat the key themes of the presentation.*

As we talked about in the beginning, E-mail is important to both companies and individuals.

We also discussed the many security risks to E-mail including loss of confidentiality, authenticity, and risk of fraud.

We talked about key ways to protect yourself:

Don't send confidential or personal information via E-mail

Recognise fraudulent E-mails including phishing, SPAM, and E-mails with malicious content.

Lastly, take advantage of the tools that are out there to protect your computer from fraudulent E-mails, malicious software, and SPAM.

## References

N/A

## Slide 18

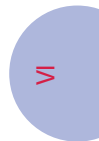


## Discussion points

N/A

## References

N/A









# Security while travelling

February | 10

## *Train the trainer reference guide*



VII







## **Security while travelling: Train the trainer reference guide**

VII

*February 2010*





# Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>281</b>
<b>HOW TO USE THIS MANUAL .....</b>	<b>282</b>
STRUCTURE OF THE MANUAL .....	282
STRUCTURE OF THE PRESENTATION PAGES .....	282
<b>THE PRESENTATIONS SLIDES .....</b>	<b>283</b>
SLIDE 1 .....	283
SLIDE 2 .....	284
SLIDE 3 .....	285
SLIDE 4 .....	286
SLIDE 5 .....	287
SLIDE 6 .....	288
SLIDE 7 .....	289
SLIDE 8 .....	290
SLIDE 9 .....	292
SLIDE 10 .....	293
SLIDE 11 .....	294
SLIDE 12 .....	295
SLIDE 13 .....	296
SLIDE 14 .....	298
SLIDE 15 .....	300
SLIDE 16 .....	301
SLIDE 17 .....	302
SLIDE 18 .....	303
SLIDE 19 .....	305
SLIDE 20 .....	307
SLIDE 21 .....	308
SLIDE 22 .....	309
SLIDE 23 .....	310





## Executive summary

This training reference guide has been created by ENISA in conjunction with presentation materials for small and medium enterprises to raise awareness with their employees about the importance of security while travelling.

These documents are designed to provide easy to understand information that focuses employees' attention on information security and encourages them to recognise and respond accordingly to threats.

This material may be used by individuals or presented in a classroom setting by instructors who are involved in their organisation's security awareness efforts. This reference guide provides additional notes and external references for trainers and presenters to utilise while performing security awareness training.

## How to use this manual

This manual is intended to be a guide for instructors of any security awareness course based on ENISA's Security while travelling presentation. This manual is only a guide, and instructors are welcome to use any portion of this material they deem appropriate. It is at the instructor's discretion how to conduct the course and which material to present.

It should be noted however that ENISA recommends that the instructor carefully consider the skills and knowledge of the students being taught in developing the course. The material should be tailored to fit the needs of the students including making it easy to understand, relevant to their position and responsibilities.

ENISA has chosen focus this material on the general user community outside of the Information Technology field. As such, this presentation focuses on the fundamentals of security while travelling and avoids the use of complex technical terms to explain risks or solutions.

### Structure of the manual

This manual broken into two parts:

1. How to use this manual (this section)
2. The presentation slides with associated supporting material

### Structure of the presentation pages

Each of the presentation pages are broken in to three parts:

1. The thumbnail of the slide from the presentation
2. Suggested narratives that provide supporting information and discussion points
3. Reference materials that support the slide that can be used to do further research



## The presentations slides

### Slide 1



### Discussion points

This is a good time to have the attendees introduce themselves.

When everyone is introducing themselves, ask them to also say if they currently or will travel for business, and what do they expect to get from the course. The answers will tell you what scenarios you can use as examples for this course, and what their expectations are for this course. This information is very useful so that you can adjust your discussions accordingly.

### References

N/A

## Slide 2

### About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the Agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

#### Contact details

For contacting ENISA or for general enquiries on information security awareness matters, please use the following details:

Isabella Santa, Senior Expert Awareness Raising - E-mail: [awareness@enisa.europa.eu](mailto:awareness@enisa.europa.eu)

Internet: <http://www.enisa.europa.eu>

### Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA regulation ((EC) No 460/2004). This publication does not necessarily represent the state of the art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2010.

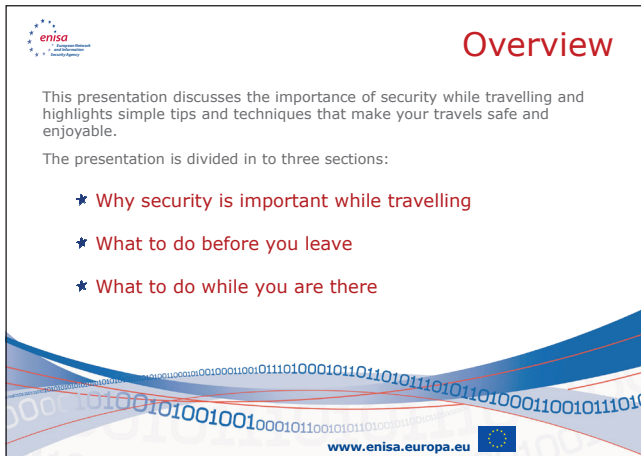
## Discussion points

Introduce ENISA and their activities. Suggest that attendees should examine some of ENISA's other presentations on other aspects of network and information security.

## References

<http://www.enisa.europa.eu> – ENISA's website

### Slide 3



The slide features the ENISA logo in the top left corner. The title "Overview" is positioned in the top right. The main text describes the presentation's focus on security while travelling and lists three sections: "Why security is important while travelling", "What to do before you leave", and "What to do while you are there". The slide has a decorative background with binary code and a blue wave pattern. The ENISA website URL and the European Union flag are at the bottom.

**enisa**  
European Network  
and Information  
Security Agency

## Overview

This presentation discusses the importance of security while travelling and highlights simple tips and techniques that make your travels safe and enjoyable.

The presentation is divided in to three sections:

- ★ Why security is important while travelling
- ★ What to do before you leave
- ★ What to do while you are there

[www.enisa.europa.eu](http://www.enisa.europa.eu)


### Discussion points

Point out that this presentation is intended to make users aware of the most common and pervasive risks when travelling, and also simple techniques that can eliminate a large percentage of these risks. Point out that the course is intended for all users, and that it can help each of them travel safely for work and personal travel.

### References

N/A

## Slide 4




### How to Use This Presentation

This presentation has been created by ENISA to raise awareness about crucial and important issues regarding security while travelling. It does so by providing easy to understand information that focuses employees' attention on security while travelling and allows them to recognise and respond accordingly to risks.

This presentation may be used by individuals, or presented in a classroom setting by instructors who are involved in their organisation's security awareness efforts.

In conjunction with this presentation, ENISA's has developed a reference guide for this training which provides additional notes and external references for trainers and presenters to utilize while performing security awareness training using this material.

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

This slide is an introduction, and is intended to inform readers that a presentation guide (this document) exists to support instructors in their security awareness efforts.

### References

N/A

## Slide 5



# The Importance of Security While Travelling

## Discussion points

This is the start of Section 1, 'The Importance of Security While Travelling'

## References

N/A

## Slide 6



 **Why Be Secure**

- ★ **Travelling Can Present Many Risks**  
A simple incident can make a trip a disaster if you are not prepared.  
Incidents can happen anywhere – near your home, or while you are thousands of kilometers away.  
Lack of preparation can make you an easy target.
- ★ **Good preparation can limit the risks!**

  
  
[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

When you travel, you are responsible for ensuring the security of yourself, your belongings, and your information. A simple incident can create a cascading effect and ruin travel plans. Incidents can happen anywhere – close to home or far away. The difference is when they happen near your home, you feel more secure because you are familiar with your surroundings. When we are not familiar with our surroundings, and unprepared, a simple incident can cascade into a more significant problem.

Lack of preparation can make you an easy target for thieves, pick-pockets, unscrupulous competitors, and other criminals.

Good preparation however can significantly reduce your risks and make your experience far more relaxing and productive.

## Reference

N/A

## Slide 7



### What Could Happen

- ★ Simple issues are more difficult when travelling.

A flat tire, a small accident, missed connecting flights, train delays, storms and bad weather can leave you stranded.

Stolen wallet, lost passport, lost tickets, stolen laptop or lost luggage can leave you stranded and without identification.

A small injury or illness, lost medicine or broken glasses can limit your ability to enjoy your trip or do your work.



[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

Broken glasses, a small cold, lost tickets, or unforeseen delays are all potential problems if you are not prepared.

If you are prepared with a spare set of vision glasses, broken glasses will not affect you. If you are familiar with local laws, a minor car accident can be quickly handled with minimal consequence.

Good preparation however can significantly reduce your risks and make your experience far more relaxing and productive.

*Instructor: You can ask the participants to discuss situations they encountered when travelling that could have been prevented with good preparation.*

### References

N/A

## Slide 8



### Why Be Secure

- ★ Most risks can be avoided by taking a few simple steps and being prepared
- ★ Simple techniques can improve your security
  - ★ Personal security to protect yourself
  - ★ Protection of your valuables
  - ★ Protection of your information

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

## Discussion points

If you do not have good security habits, you can suffer a significant loss. You can have your property or valuables stolen. This might include your wallet, money, jewellery, and identification documents. You may also lose confidential information you're carrying. The theft of wallets, check books, and the identification cards, payment cards, and bank account information they contain is the main methods of identity theft. The loss of these items can also hamper any plans or travel.

The theft may include a briefcase or a laptop. The information that they contain can include confidential company product plans, customer names, proprietary knowledge, and other items that can be very valuable to a competitor. Even the personal information that is stored there is valuable to a thief. The inconvenience that results can spoil your work and your travel.



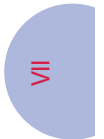


What can seem like a simple incident can actually result in a significant problem.

Simple techniques can, however, protect you against many of these security risks. These simple techniques should focus on your personal security to protect yourself, how to protect your valuables and confidential information, knowing where to find assistance when you need it, and having contingency plans in case of emergencies.

## References

N/A



## Slide 9

# How to Prepare for Travelling

### Discussion points

This is the start of Section 2, 'How to Prepare for Travelling'

### References

N/A

## Slide 10



### Prepare: Secure Your Home

- ★ **Make your home look lived in while you are away**
  - ★ Set timers for lights and radios to give the impression that someone is home
  - ★ Arrange with your neighbors to watch your house
  - ★ Arrange with the post office to hold your mail
  - ★ Make sure your trash bins are not left out



[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

Thieves look for easy targets. If they suspect someone is around, they will more likely look for an easier target.

Lights that go on randomly, noise from radios or televisions, and other signs of activity are great ways to give the impression you are home.

### References

<http://www.state.gov/m/ds/rls/rpt/19773.htm>

## Slide 11



### Prepare: Packing

- ★ **Travel with only what you need**
  - ★ Use travelers checks whenever possible and store the check receipts separately
  - ★ Travel with as few valuables as possible
  - ★ Lock away any payment cards, identification or other personal information you don't need
  - ★ Carry an emergency flashlight, water, weather protection, first aid kit, and an extra set of glasses






### Discussion points

Travel with only what you need. Avoid taking any data, documents or information that you do not absolutely need while you are away from the office. The same applies to valuables. Because you have many more things to worry about, reduce the number of things you need to protect. This also reduces the impact if something does happen. By locking away any payment cards, identification or other personal information, you ensure it is safe while you are gone.

If you are travelling or will be gone for some time, prepare yourself with items that may be useful. For shorter trips pack some water, some weather protection, and any minor items that may be of assistance if you are delayed. For longer trips a small first aid kit, copies of any travel documents, a small emergency flashlight, and an extra set of eyeglasses or contacts can become very useful if there are any interruptions to your trip.

### References

<http://www.travel-security-and-safety.com/travel-packing-tips.html>

## Slide 12



**enisa**  
European Network  
and Information  
Security Agency

### Prepare: Travel Documents

- ★ Prepare your travel documents
  - ★ Make sure your travel documents and identification are up to date and will not expire while you are travelling
  - ★ Keep copies of your passport, itinerary, emergency contacts, as well as phone numbers for banks and payment cards in different pieces of your luggage.
  - ★ Leave a copy of your itinerary with family or co-workers

www.enisa.europa.eu



### Discussion points

Many travel plans have been interrupted due to expiring travel documents or identification. Check these documents before you leave to prevent this costly interruption.

Keep copies of critical documents stored safely in an alternate location in your luggage in case you lose your originals. This should include emergency phone numbers, itineraries, and identification. This should also include travellers check receipts.

### References

<http://www.travel-security-and-safety.com/travel-packing-tips.html>

## Slide 13



### Prepare: Research

- ★ Know your destination before you leave
  - ★ Learn the local customs and laws
  - ★ Know how to get around at your destination including what types of transportation are available
  - ★ Know where emergency facilities are located
  - ★ Make sure your medical insurance covers you when you travel or that your destination can provide you with medical care if you need it.





[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

It is also very helpful to know your destination before you leave.

Know the local customs and laws. This information can be very important to avoid problems with local authorities, and also to make it easier to not stand out for criminals who target travellers.

Know how to get around at your destination, including what modes of transportation are available.

Know where important facilities like hospitals and police stations are located. You may even wish to buy a map. This can help you know where to go if there are any detours, construction, or you need to find food, shelter from the weather, gasoline, or emergency facilities. Simple preparation like this can make you more relaxed and pay more attention to other tasks and security prevention.

## References

<http://security.tipcentral.net/travelsecurity.html>

[http://europa.eu/travel/index\\_en.htm](http://europa.eu/travel/index_en.htm)

<http://www.livesecure.org/category/advice/travel/>

<http://ec.europa.eu/idabc/en/document/4070/5926>

## Slide 14



### Prepare: Your Computer

- ★ Check that you have prepared your computer
  - ★ Ensure you have a physical computer lock
  - ★ Ensure your operating system is patched, and all security tools and anti-virus are up-to-date
  - ★ Only take the information that you absolutely need
  - ★ Encrypt the data on your computer before you leave
  - ★ Perform a data backup of your computer before you leave

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

If you are taking your computer, it is important to ensure that it is secure. Not only is the computer itself valuable to a thief, but the data contained on it is also valuable to thieves and competitors. Many people have been the victim of computer theft which has resulted in the loss of sensitive company secrets, millions of personal records and information, and government secrets. Proper preparation might have prevented these losses.

A good computer lock will allow you to secure your computer while you are working on it, and will prevent most snatch-and-grab thefts.

Patching your computer and making sure it is up-to-date gives you the most recent security tools before you go on the road. It will minimise the exposure to malware, and attacks when your ability to make updates may be limited.





By only taking the information you absolutely need, you are reducing the exposure if something does go wrong. Know what information is the most sensitive and avoid taking that type of information if at all possible. Information such as your personal identification, customer confidential or personal data, protected information (by law, or regulation), sensitive business plans, and proprietary data should be left at the office. Encrypt the data that you do take with you. Your company should be able to provide you with a solution, as many newer operating systems include disk encryption technology, and many third party tools are available as well.

Performing a data backup allows you to restore information if your system is stolen, damaged or has an accident while you are remote. Knowing that any damage to your computer can be mitigated by having a backup of your data can make you breathe a little bit easier.

And remember to secure your office and your home before you leave. There is critical data still there, and it needs to be protected while you work remotely.

## References

<http://www.securityfocus.com/infocus/1186>

<http://fcw.com/Articles/2008/03/03/Stolen-VA-laptop-caught-in-safety-net.aspx>

<http://www.dodbuzz.com/2009/12/22/top-secret-brit-laptop-stolen/>

<http://technet.microsoft.com/en-us/windows/aa905065.aspx>

<http://docs.info.apple.com/article.html?path=Mac/10.4/en/mh1877.html>

<http://www.truecrypt.org/>

<http://www.pgp.com/products/wholediskencryption/>



## Slide 15

# How to Be Secure While Travelling

## Discussion points

This is the start of Section 3, 'How to Be Secure While Travelling'

## References

N/A

## Slide 16



 **Communicate**

- ★ **Communicate frequently**
  - ★ Communicate your plans and itinerary with office associates and family members.
  - ★ Inform them of any changes
  - ★ Contact them frequently to inform them of your status

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

Frequent communication with family members and office associates can ensure that if anything happens to you, there is someone with knowledge of your plans and your itinerary. This step can help authorities render assistance if you need it, and in the right locations. Many situations have been resolved quickly because authorities knew where and when someone would be and were able to locate the person safely because they could arrive quickly at the right location.

### References

N/A

## Slide 17



### Be Aware

- ★ **Be aware of your surroundings**
  - ★ Only meet in familiar or very public places.
  - ★ Observe your surroundings and others around you.
  - ★ Be cautious of strangers. Do not accept invitations, open your door, or invite strangers to your room.
  - ★ Vary your travel routes and routines.



www.enisa.europa.eu 

## Discussion points

Thieves are interested in two things – profiting from their efforts, and not getting caught. If they spot a target they are more likely to attempt to their crime in non-public areas where they will not be seen.

Strangers who ask to come visit you in your room are more likely interested in the valuables that are there than in meeting you. Choose another location to meet that is public.

Vary your travel routes and routines in order to make it harder for someone to target you. Many crimes are pre-meditated and planned. Changing your routine can make those plans fail, and make you safer and more secure.

## Reference

<http://information-security-resources.com/2010/01/04/physical-security-tips-for-international-travel/>

## Slide 18



**enisa**  
European Network  
and Information  
Security Agency

# Security At Your Hotel

- ★ Observe simple security guidelines
  - ★ Know the emergency exits wherever you go
  - ★ Make sure doors to locked areas close behind you
  - ★ Do not leave valuables, your computer, your mobile phone or important documents unattended in public places, in hotel rooms, or in your car.

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Discussion points

Your physical surroundings can have a very big impact on the security of yourself, your computer, and your belongings. Ensure physical security is in place at your hotel, and where you are working. Having locked doors and safe places to work can reduce your stress and allow you to focus on your task at hand.

If you step away, even for a moment, make sure the room or area where you are working is secure. Do not leave doors to rooms open or unlocked.

Never leave valuables such as computers, your mobile phone, thumb drives and other storage devices unattended in a public place. Even when you think an area is secure, still protect these items by keeping them locked up and out of sight. Never leave these items in hotel rooms as staff and outsiders can gain access to your room and remove these items while you are away.

Be aware of your surroundings and the activities occurring around you – they can be good indications if an unsafe situation may be occurring, or of any impending security threats. It is not necessary to be paranoid, but awareness is part of a good defence.

## References

<http://www.securityfocus.com/infocus/1186>

## Slide 19



 **Protect Your Information**

- ★ **Protect your confidential information**
  - ★ Do not work on confidential information in public places
  - ★ Do not use public computers for viewing any confidential or personal information
  - ★ Do not share your travel plans or personal information with strangers
  - ★ Do not let others use your computer

[www.enisa.europa.eu](http://www.enisa.europa.eu) 

### Discussion points

If you are carrying confidential or personal information, it is important to protect at all times – when you are using it, or when you are just carrying or storing it.

Public places can be full of people interested in the information you may be working on. Some could be thieves, and others could be your competitor. Some information you may be carrying may be protected by laws and regulations and must be kept confidential. Working on this data in public places exposes it to disclosure. You or your company could be held liable for disclosing that information.

Public computers are not well protected. Previous users may not have used safe habits to surf the Internet, or may have intentionally installed malicious software that collects any sites you visit, any screens you view, or anything you type – including usernames, passwords, bank account

numbers, or any other confidential information. Avoid public computers for any work that involves personal or confidential information.

Do not share your travel plans or personal information with strangers. Because you do not know their intentions, or their background, you could be giving a thief an opportunity to steal from you, take advantage of a brief moment of insecurity, or target you for a scam. Protect this information and only share it with your family and trusted co-workers.

If you are travelling with your office computer, it is important to not let others use that computer. They can view confidential information that you have stored on it. They can visit malicious websites and install software (intentionally or by accident) that compromise the computer. They may also simply steal the computer from you. Never allow anyone, even family members to use your office computer. It is your responsibility to protect the company's confidential information, and if there is information that is protected by law or regulation, you can be liable for its safety.

## References

[http://www.cisco.com/web/CA/pdf/Understanding\\_Remote\\_Worker\\_Security\\_A\\_survery\\_of\\_User\\_Awareness\\_vs\\_Behaviour.pdf](http://www.cisco.com/web/CA/pdf/Understanding_Remote_Worker_Security_A_survery_of_User_Awareness_vs_Behaviour.pdf)



## Slide 20



**enisa**  
European Network  
and Information  
Security Agency

### Handling Problems

- ★ What to do if you have an emergency
  - ★ Do not over-react. Be calm and get away from danger.
  - ★ Contact the appropriate authorities – police or medical.
  - ★ Explain any facts to the appropriate authorities.
  - ★ Contact family members or office associates to notify them of any issues or problems.

[www.enisa.europa.eu](http://www.enisa.europa.eu)



### Discussion points

It is important to remain calm, and follow these few important steps:

Do not over-react. Overreaction can cause panic, which can result in poor decisions. Calmly move away from any danger.

Contacting the appropriate authorities as soon as possible can limit your exposure – whether to a dangerous criminal situation, or to a medical situation.

When the authorities arrive, explain the facts – those facts that you have direct knowledge of. Avoid speculation and theories.

Communicate with family members or trusted office associates about any problems you encounter when you communicate with them. This information could be useful later if you need to remember, or need their assistance.

### References

N/A

## Slide 21



Conclusion

### Discussion points

This is the conclusion of the presentation.

### References

N/A

## Slide 22



**Travel Security is Important**

- ★ Being secure while travelling can make your trip more enjoyable.
  - ★ Preparation is important so you can protect
    - Yourself
    - Your valuables
    - Your information
  - ★ Be aware of how to be safe and secure

[www.enisa.europa.eu](http://www.enisa.europa.eu)

### Discussion points

*Instructor: This is a summary slide that provides an opportunity to repeat the key themes of the presentation.*

Being secure can help make your trip more enjoyable, and preparation is the key

Preparation allows you to protect yourself, your valuables, and your information. More importantly, it allows you to enjoy your travels and be productive.

### References

N/A

## Slide 23



## Discussion points

N/A

## References

N/A



My notes



---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---



---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---



My notes

---



---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---



---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---







## HOW TO OBTAIN EU PUBLICATIONS

### **Free publications:**

- via EU Bookshop (<http://bookshop.europa.eu>);
- at the European Union's representations or delegations. You can obtain their contact details on the Internet (<http://ec.europa.eu>) or by sending a fax to +352 2929-42758.

### **Priced publications:**

- via EU Bookshop (<http://bookshop.europa.eu>).

### **Priced subscriptions (e.g. annual series of the *Official Journal of the European Union* and reports of cases before the Court of Justice of the European Union):**

- via one of the sales agents of the Publications Office of the European Union ([http://publications.europa.eu/others/agents/index\\_en.htm](http://publications.europa.eu/others/agents/index_en.htm)).





European Network and Information Security Agency

**Promoting information security as a cultural and behavioural change**

Luxembourg: Publications Office of the European Union

2010 — 310 pp. — 12 x 17.4 cm

ISBN 978-92-9204-048-2

doi:10.2824/19099



