E-mail security

February | 10

Train the trainer reference guide

enisa
European Network
and Information
Security Agency

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:

e-mail: Isabella Santa, Senior Expert Awareness Raising — 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 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.

enisa
European Network
and Information
Security Agency

E-mail security:
Train the trainer reference guide

February 2010

Contents

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

E-mail Security

Discussion points

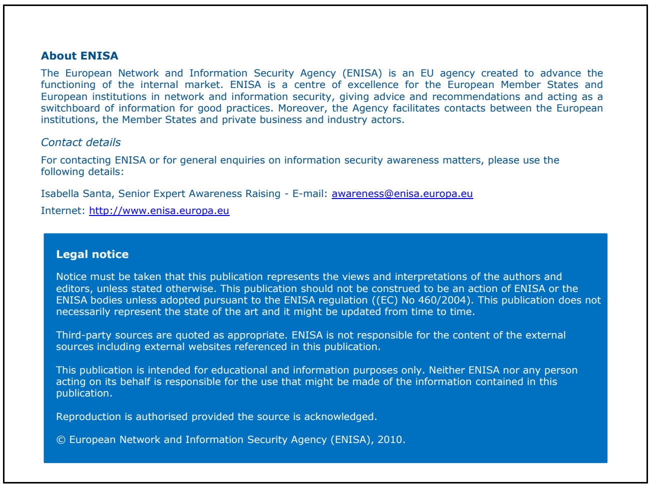
This is a good time to have the attendees introduce themselves.

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

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.

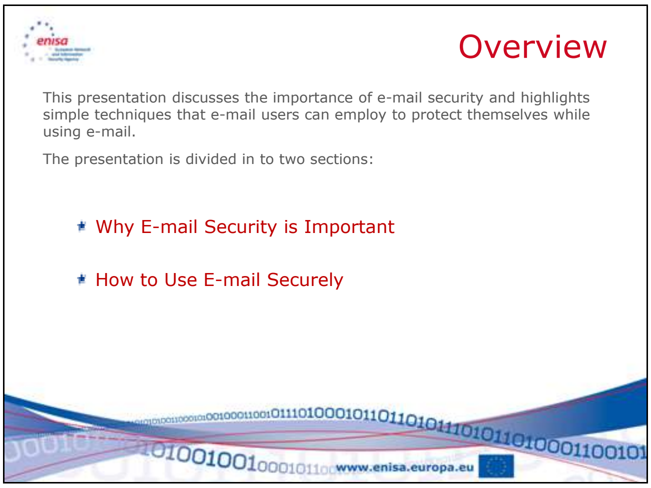
Discussion points

Introduce ENISA and their activities. Suggest that attendees should examining 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 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

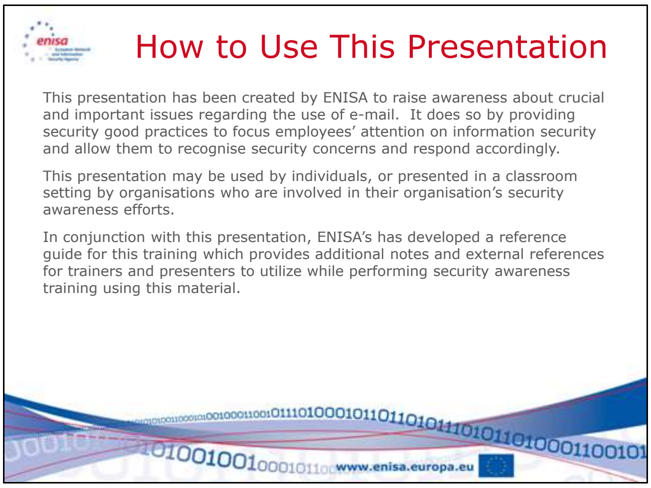
Discussion points

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

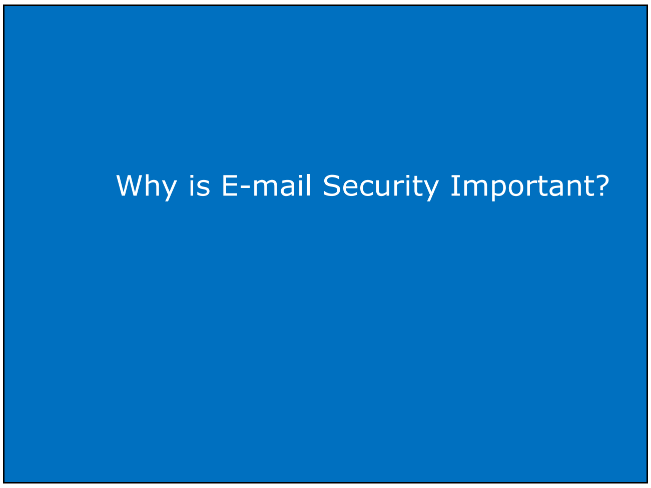
Discussion points

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?

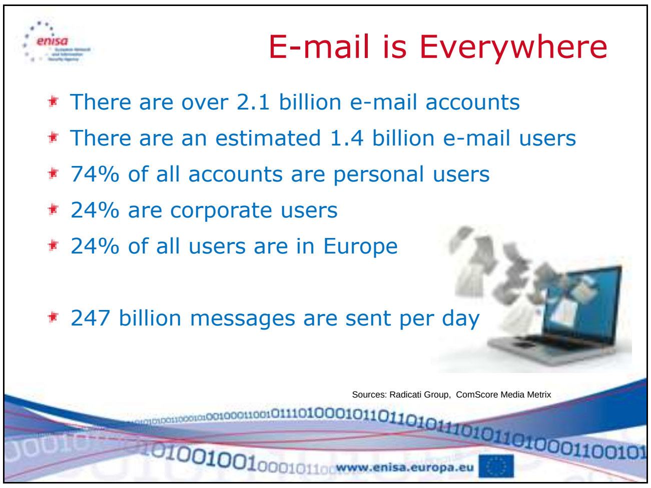
Discussion points

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

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.

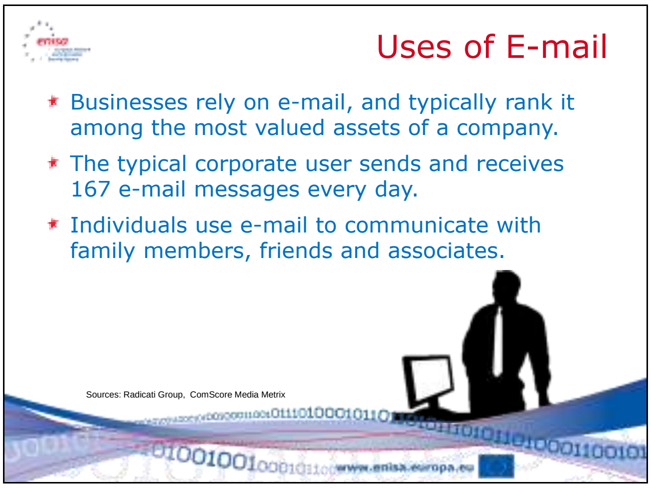
References

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 Metrix

www.enisa.europa.eu

Discussion points

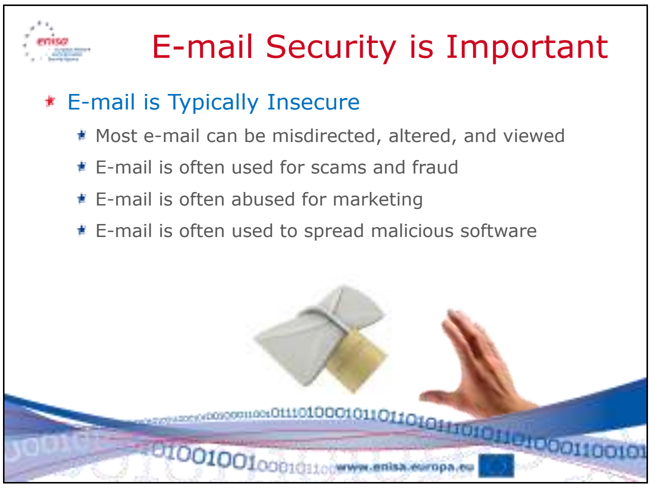
- Businesses use e-mail to communicate with future, current and past customers.
- Businesses use e-mail to provide customer service, product support, and ongoing communication about product or policy changes.
- Helpdesk applications receive e-mails to initiate trouble tickets.
- Computers and Applications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

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.

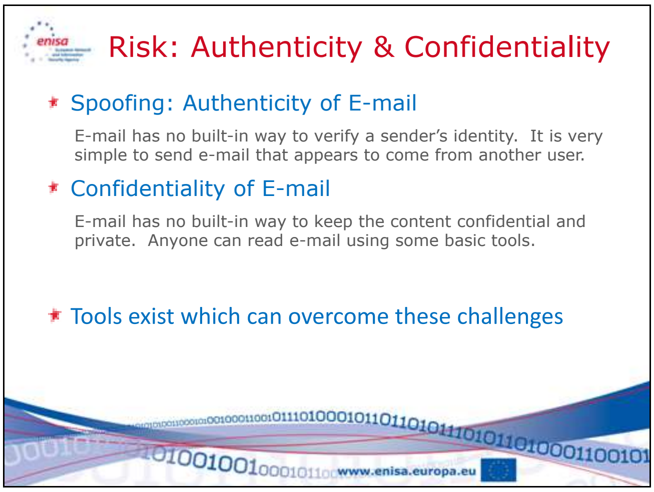
Hash: a mathematical way of creating a special digital value that represents a message and that is unique to each different message.

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

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.

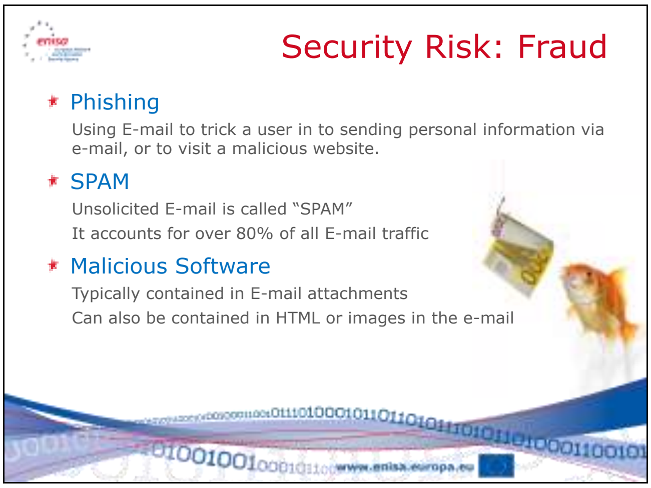
Tools that encrypt emails render the content of the e-mail unreadable, except for someone who has the right information to decrypt or make the message readable again. Most internal mail systems such as Microsoft Exchange and Lotus Notes contain these capabilities. Internet e-mail by default does not, 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/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

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.

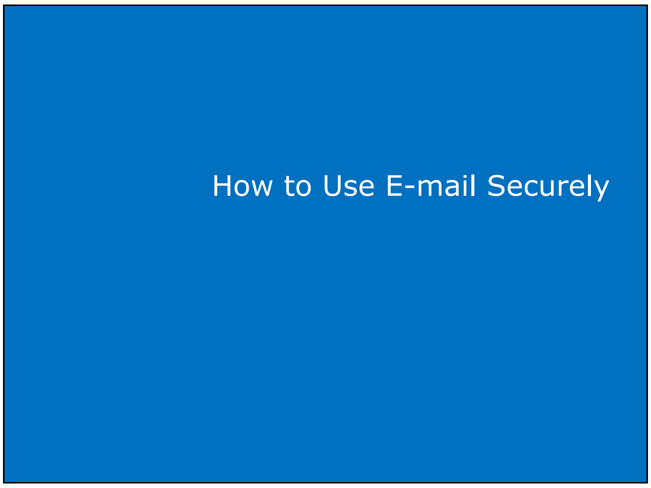
SPAM is a very large problem. SPAM is any e-mail which comes from sources we did not ask to send us e-mails or that we did not give our consent. It accounts for over 80% of all e-mail traffic. Companies spend a large amount of time and money to combat SPAM and filtering it is considered a standard part 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/ecomm/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

Slide 11



How to Use E-mail Securely

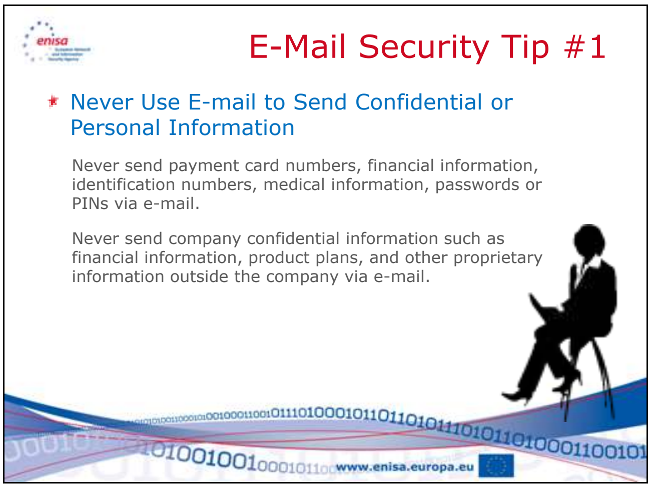
Discussion points

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

Discussion points

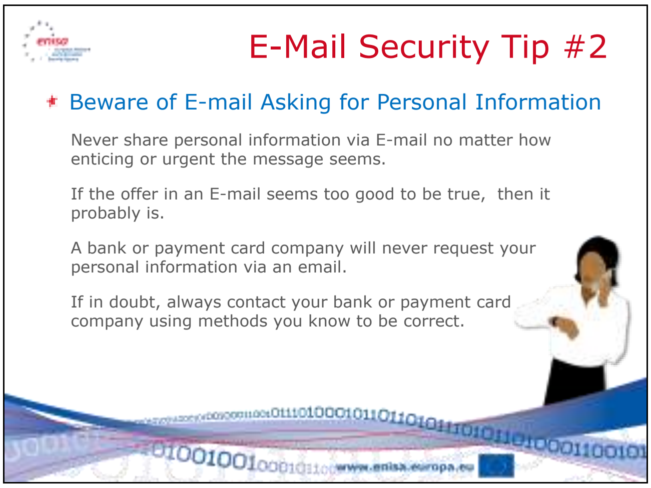
Instructor: It is important to provide backing information for these points – if your focus is on corporate awareness then be certain to define what company confidential information is. If you are focused on personal awareness, focus on what is personal information that should not be shared. The text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

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 un-suspecting 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.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.

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?

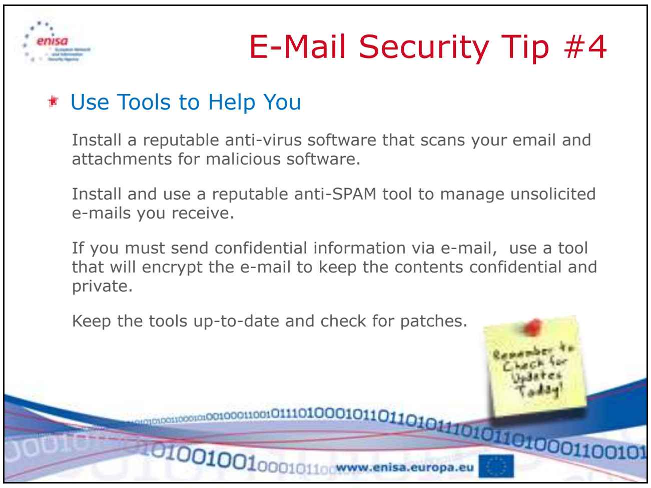
These items can help you identify a fraudulent e-mail. If you find these discrepancies, delete the e-mail. If you are still not sure if the e-mail is fraudulent or not, contact the sender through the phone, or through a method you know is legitimate. Do *not* click on the link or respond directly to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

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 ant-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.

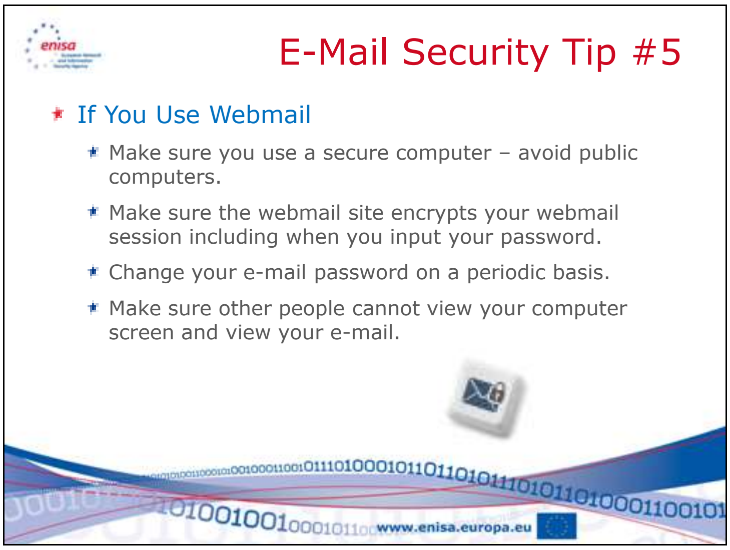
Instructor: You can mention here if the company has a standard for encryption, and if it does, simple state how a user would request this feature or tool. Also let them know if e-mail is encrypted while it is inside the company. If you use Microsoft Exchange or Lotus Notes the encryption feature can 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/ls-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

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

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.

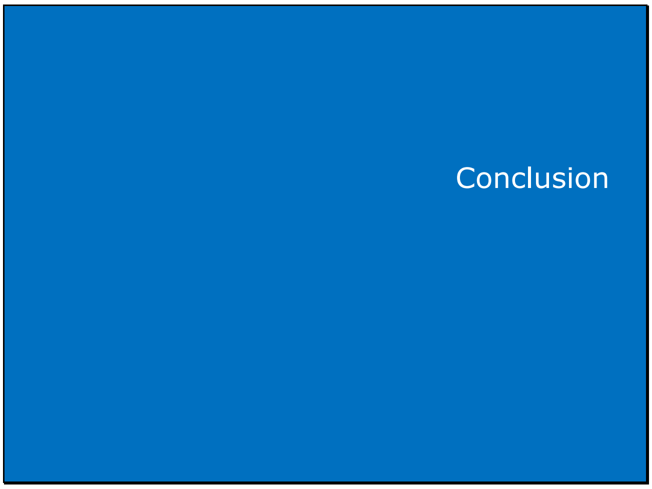
Change your email password on a periodic basis. Make your password complex, and make any password reset information complex to avoid malicious outsiders from hijacking your email account. There are numerous cases of public e-mail and webmail services being taken over by unauthorized people.

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



Conclusion

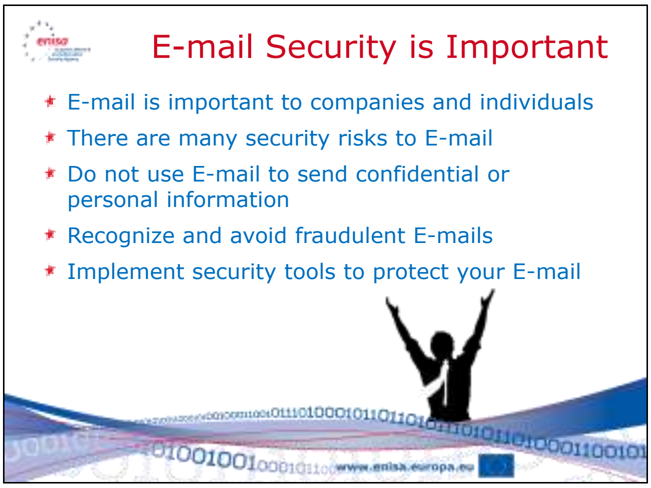
Discussion points

This is the conclusion of the presentation.

References

N/A

Slide 18



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

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

European Network and Information Security Agency
P.O. Box 1309
71001 Heraklion
Greece
www.enisa.europa.eu

Discussion points

N/A

References

N/A

enisa

European Network
and Information
Security Agency

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu