Preventing identity theft

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

Preventing identity theft:

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 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

Preventing Identity Theft

enisa
European Network and Information Security Agency

Discussion points

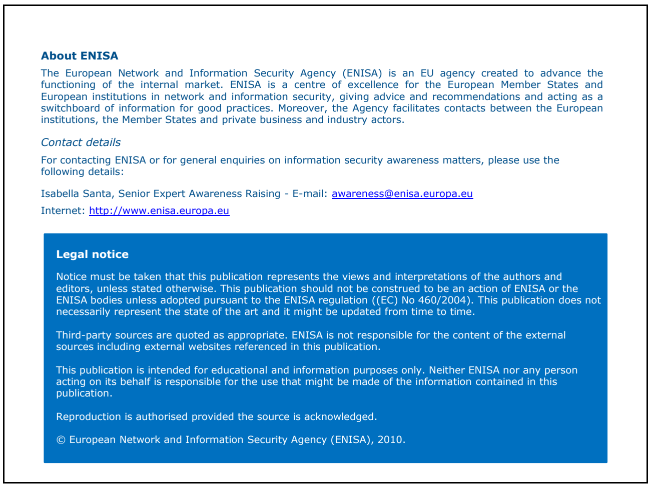
This is a good time to have the attendees introduce themselves.

When everyone is introducing themselves, ask them 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

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.

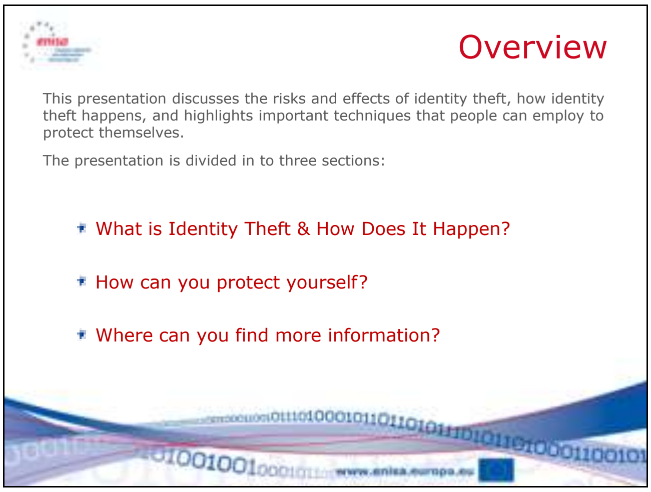
Discussion points

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 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

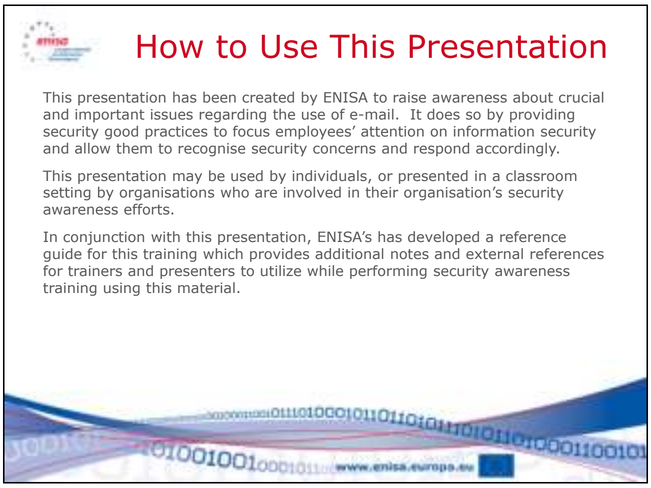
Discussion points

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

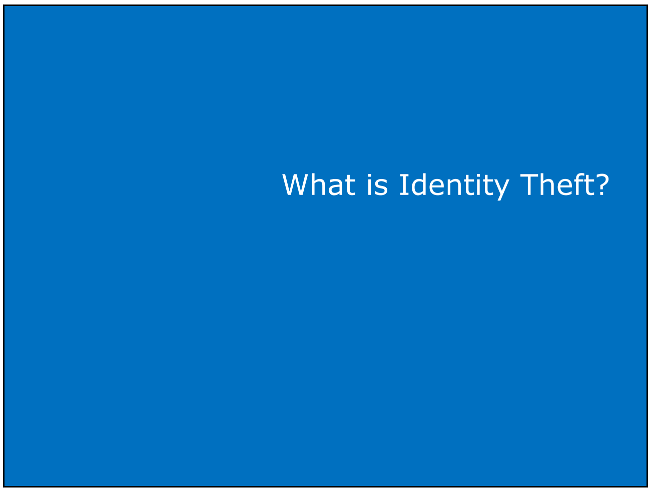
Discussion points

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?

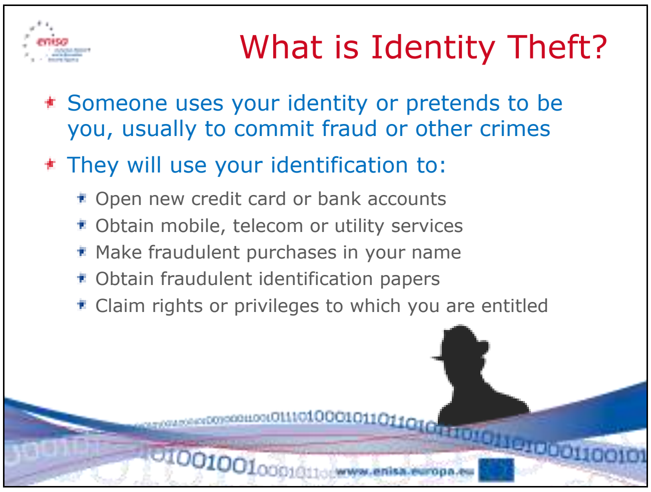
Discussion points

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

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.

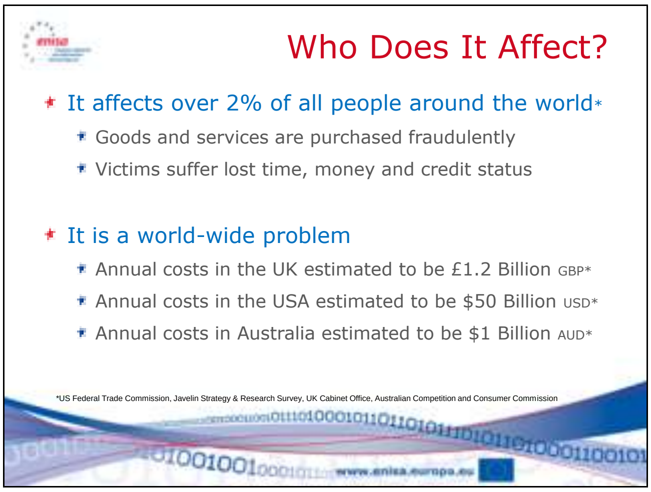
Government fraud (9%): fraudulently acquiring tax benefits or refunds, government benefits, identification documents, and driver licenses.

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.

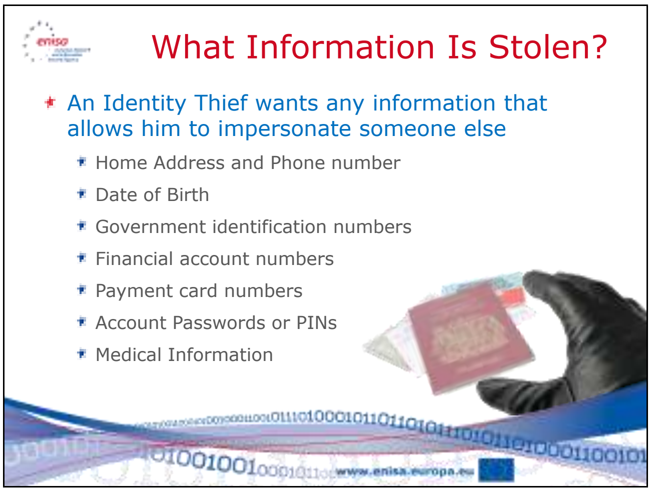
The victims of identity theft suffer lost time in addressing the debts and loans the thief has put in their name, and correcting their credit status. The time spent is time away from work, from families and things that are important in their lives.

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.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.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

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.

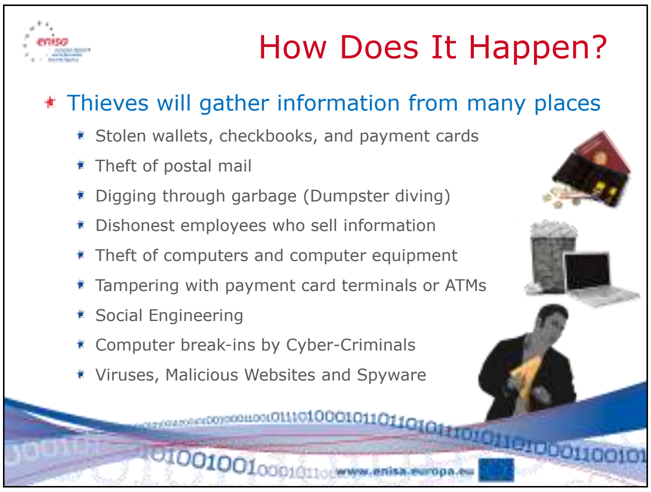
Medical information, government identification, and other information can be used to collect services to which you are entitled.

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

Discussion points

According to surveys performed in several countries, stollen 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.

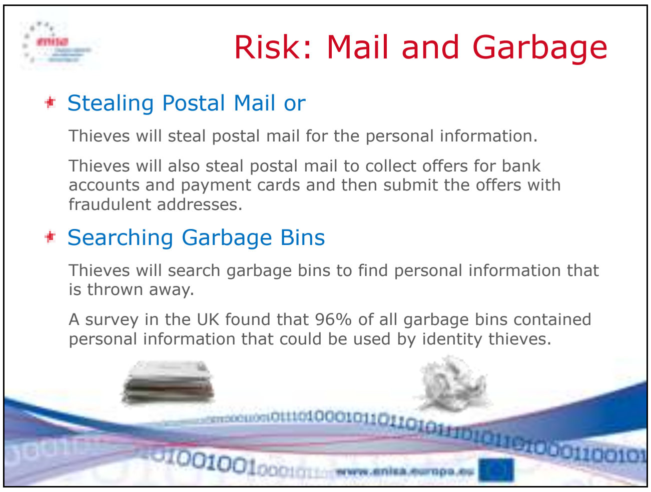
There are also technical attacks that collect information from computers and servers. These computers that are compromised can be a user’s personal computer, or can be large company systems. Several recent examples of computer incidents have resulted in significant loss of personal information.

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.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

Discussion points

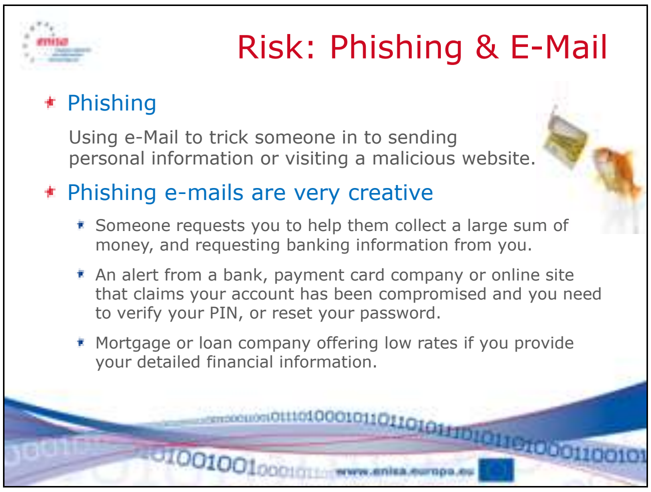
Thieves will actually lie in wait for postal mail delivery and collect the mail from postal boxes. They will search for anything that looks like it might contain personal information, or any offers for payment cards, loans or other financial services. They will fill out applications for financial services 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
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://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

Discussion points

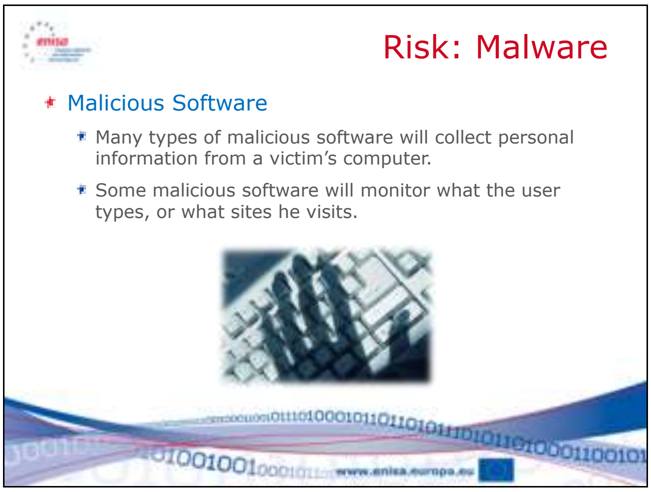
Phishing is a type of social engineering. It is a method of convincing someone to do something they wouldn’t otherwise do. By using various types of enticements they convince people to send them confidential and personal information. The enticement of a large amount of money, or the urgency of your bank 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

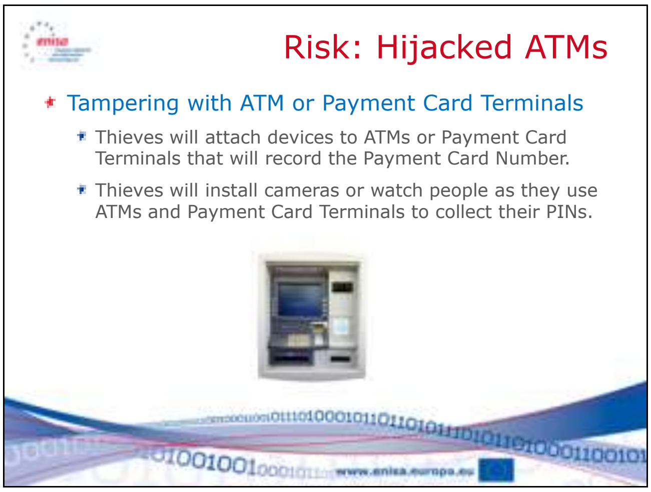
Discussion points

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.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

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.krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/

Slide 14

How To Protect Yourself

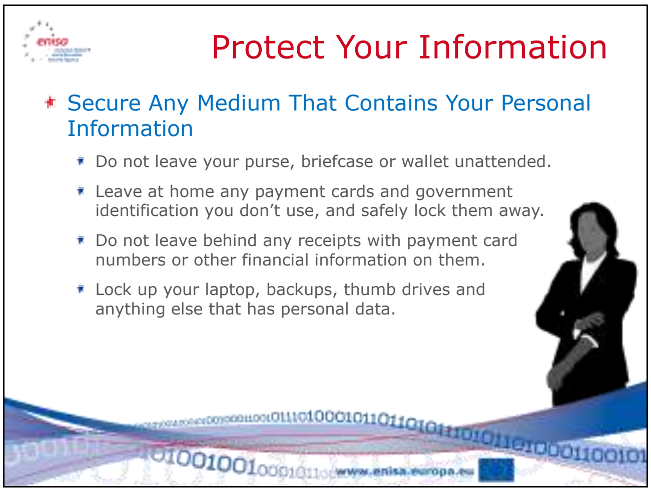
Discussion points

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

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.

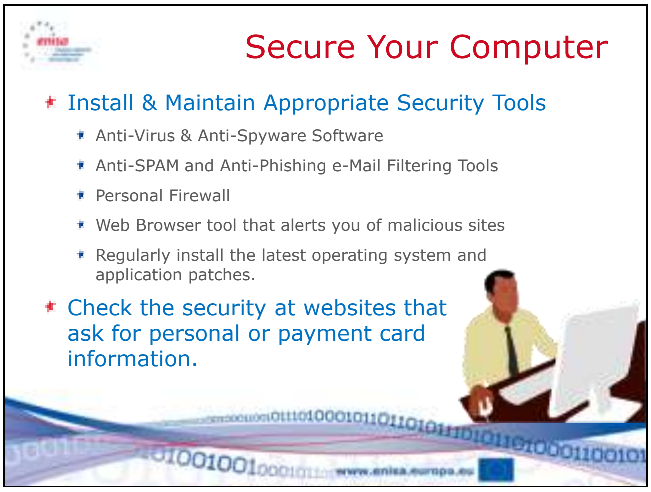
Paper receipts often have payment card numbers printed on them. This information is highly sensitive and should be carefully protected. Never leave a receipt behind at a store, restaurant or termina. A thief can use this information to perform identity theft, or even make charges using your number.

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

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.

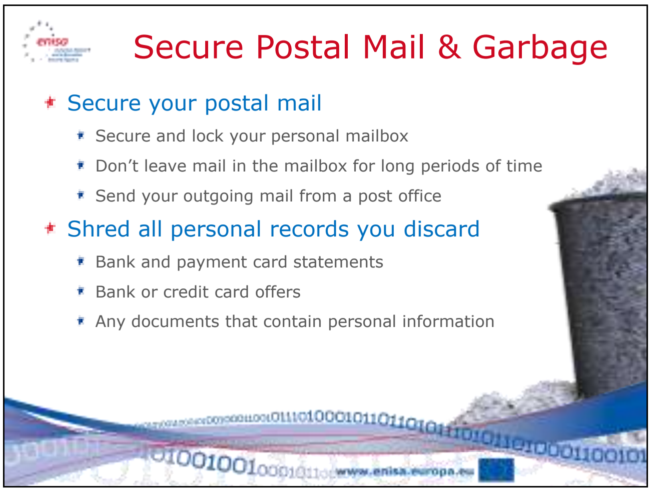
Discussion points

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

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

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.

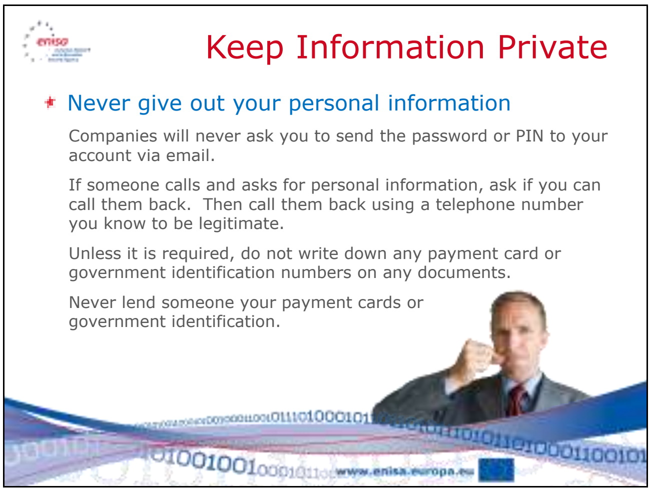
Talk to your post office to determine what are good ways to secure your mailbox. If it can't be locked, consider using a postal box at the post office.

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.

Discussion points

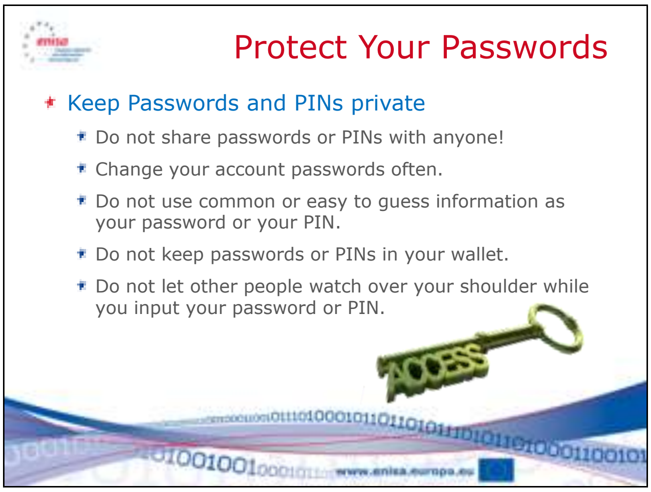
While it might seem simple enough not to give out our personal information, you would be surprised how often we actually do it. Remember the statistic that 43% of all identity theft is perpetrated by someone we know? How often do you give someone your password, or lend them your payment card? How often 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.

ACCESS
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.

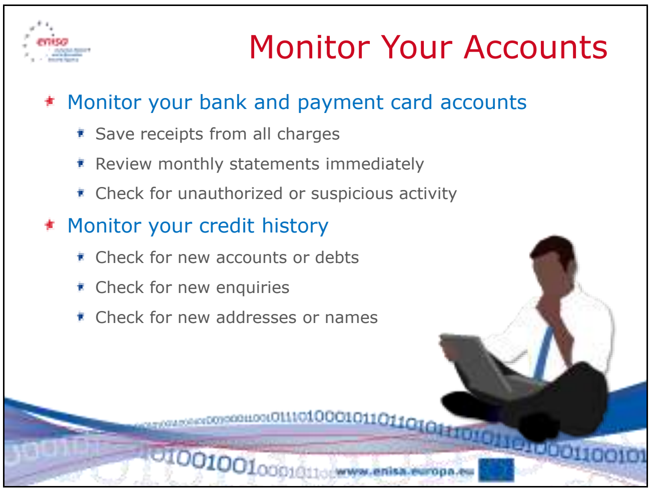
Do not keep this information somewhere that someone could access it. Since wallets and purses are a desirable target for thieves, they are a very bad place to store passwords or PINs. Keeping them in the same place as the payment card is an invitation for an identity thief to instantly get access to 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.

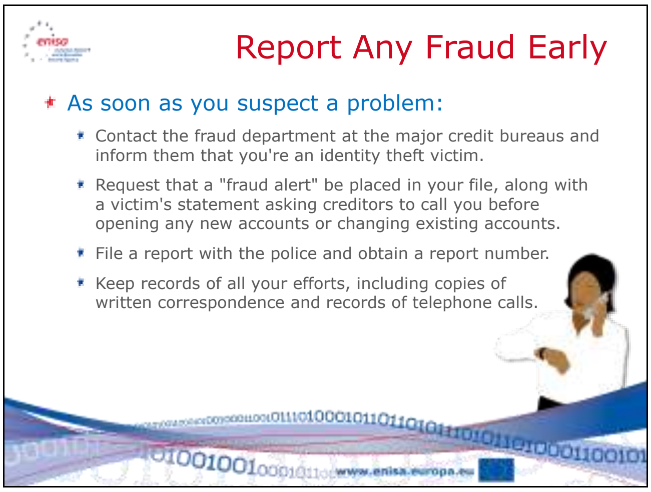
The best way to protect yourself against these situations is to regularly monitor all your accounts and credit history. Your credit history will inform you of accounts, enquiries, and other activity that may indicate identity theft.

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

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.

Discussion points

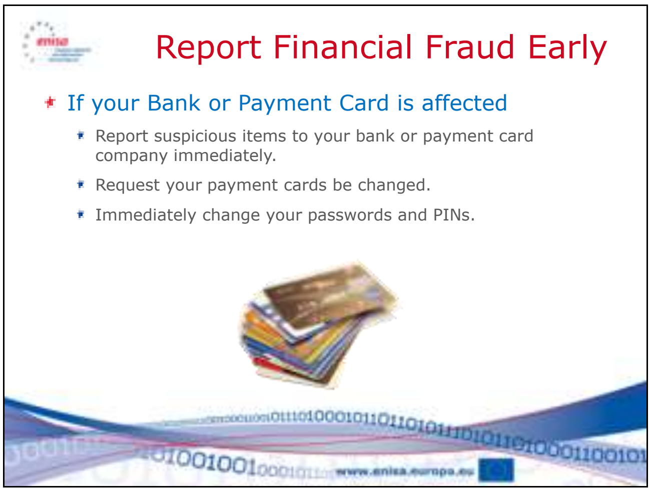
Report fraud as soon as you identify it. The earlier you identify it, the earlier it can be stopped, and the damage can be minimized.

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

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

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

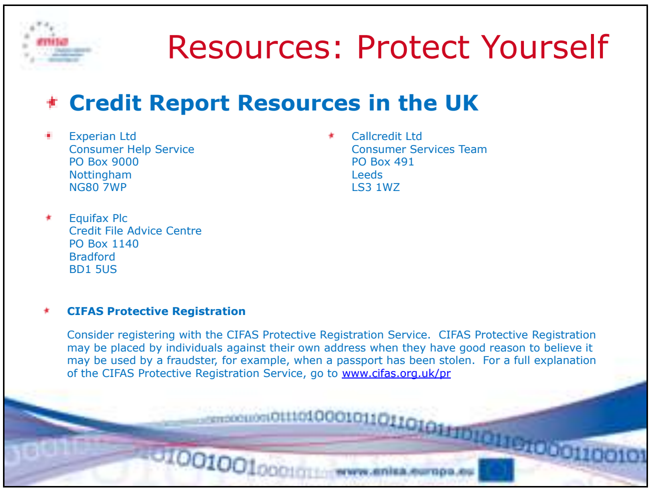
Discussion points

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
- Callcredit Ltd
  Consumer Services Team
  PO Box 491
  Leeds
  LS3 1WZ
- 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

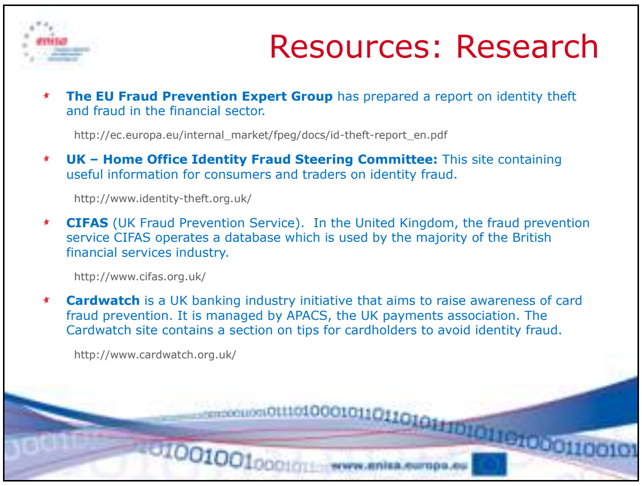
Discussion points

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

- **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

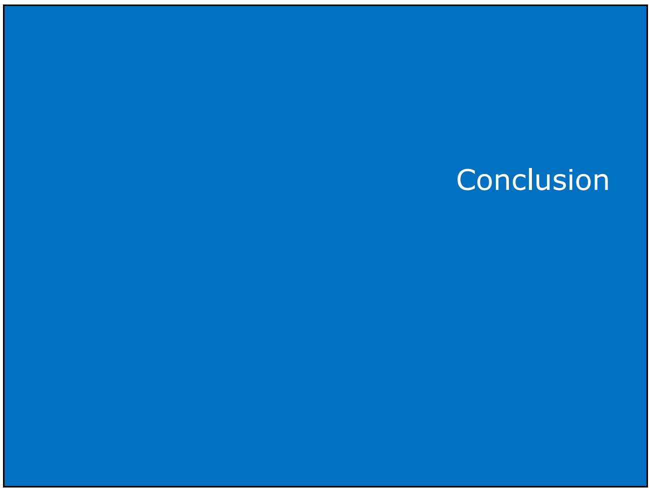
Discussion points

N/A

References

N/A

Slide 26



Conclusion

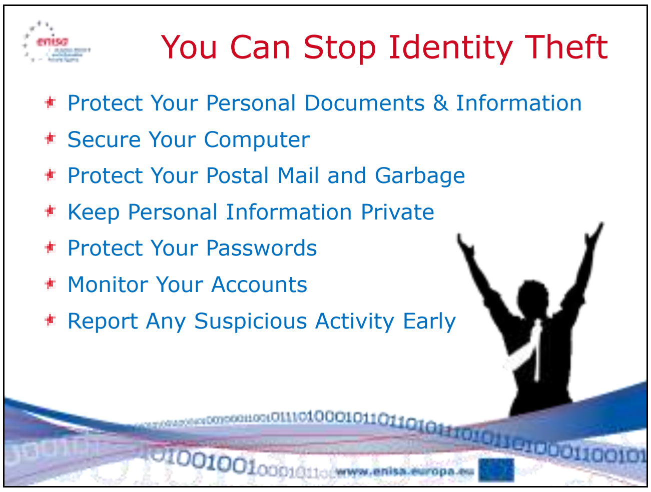
Discussion points

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

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

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

Discussion points

N/A

References

N/A

Preventing identity theft: Train the trainer reference guide enisa

European Network
and Information
Security Agency

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