Online security at home

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

Online security at home:
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 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

Online security at home

Discussion points

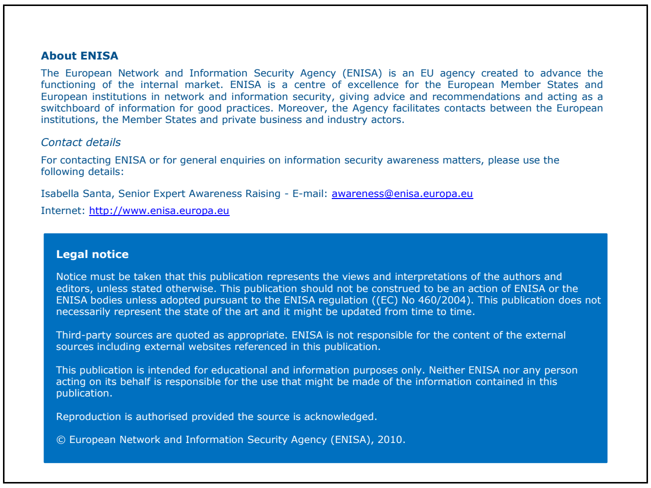
This is a good time to have the attendees introduce themselves.

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

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.

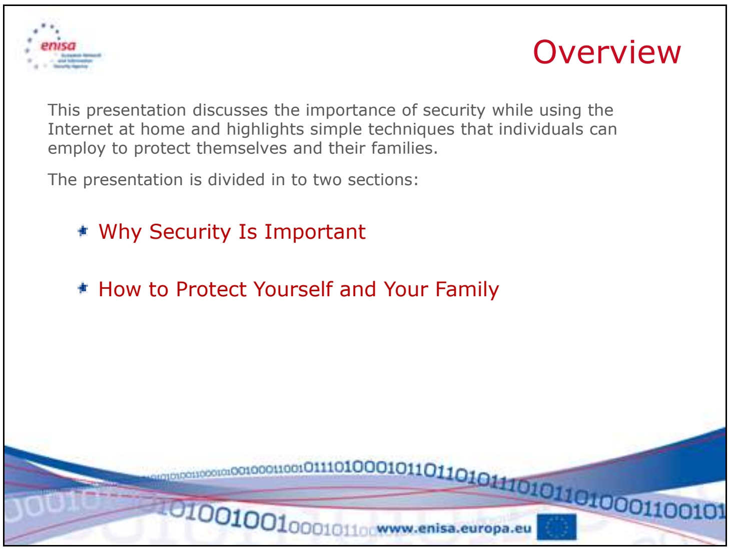
Discussion points

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 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 in to two sections:

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

www.enisa.europa.eu

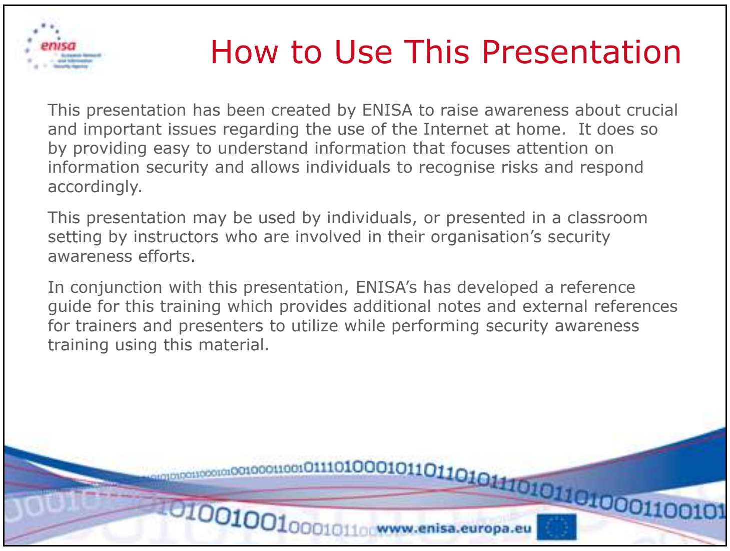
Discussion points

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

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?

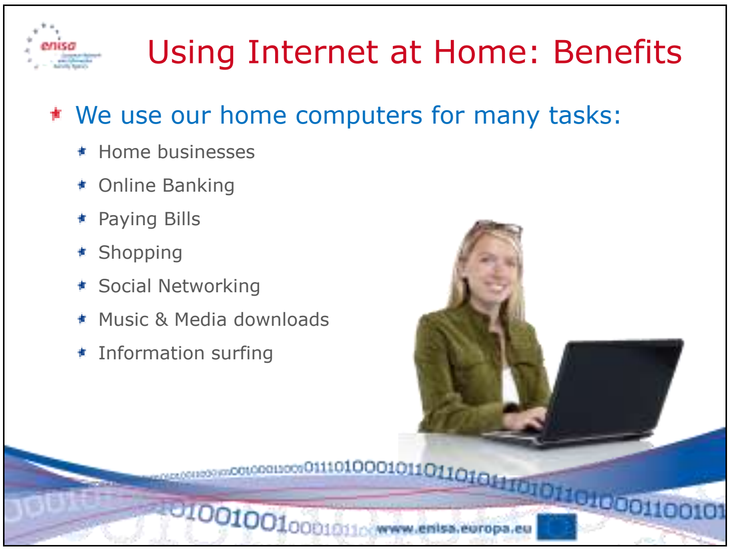
Discussion points

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

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.

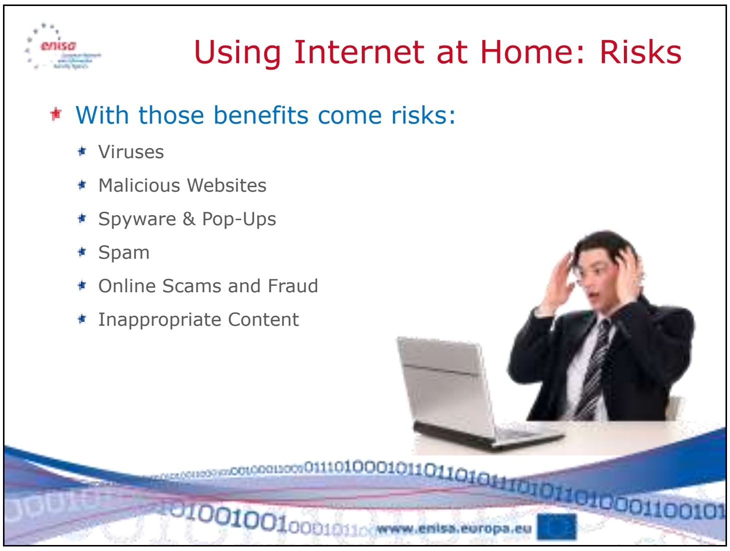
It is not difficult to recognize that the Internet is an important part of our personal lives. The statistics back this assumption. Most countries in the EU have more than 50% of their citizens as Internet users. The European region has the highest number of Internet users per 100 inhabitants than any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

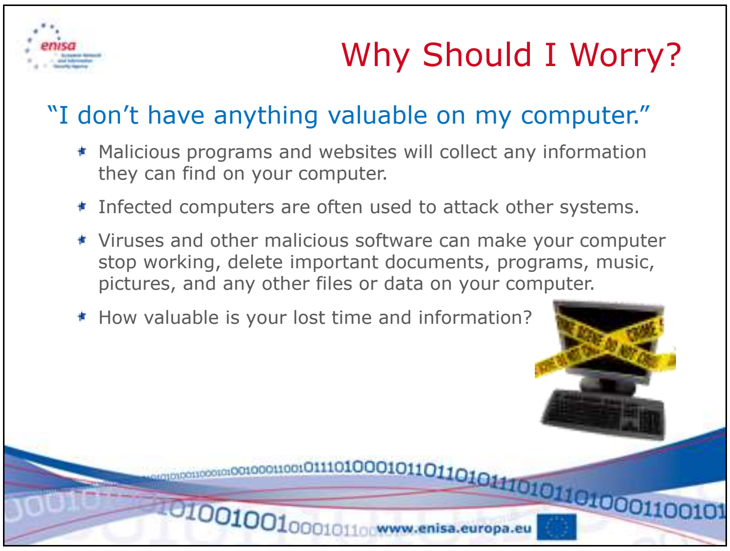
Discussion points

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.

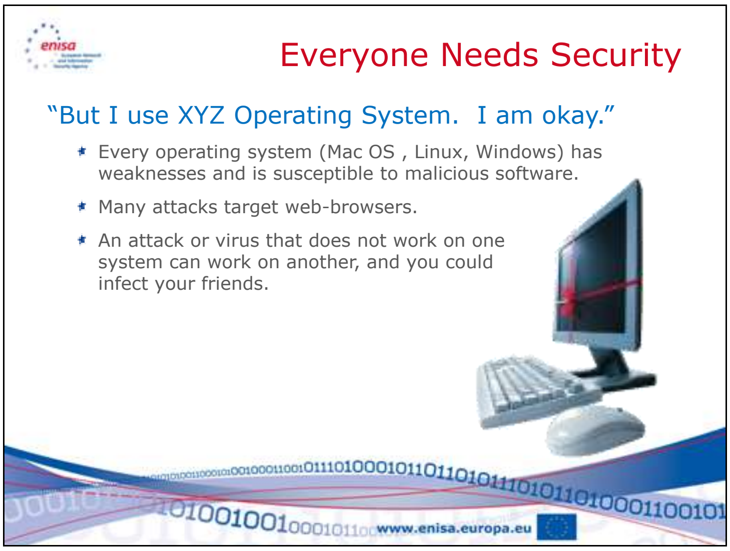
a) What do you use your computer for?
b) What if you couldn't use it to do that?
c) What things do you save on your computer (i.e. music, pictures, email addresses)?
d) What if you lost that information and all of it was destroyed?
e) How frustrated would you be if the computer became unusable?
f) How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



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

Discussion points

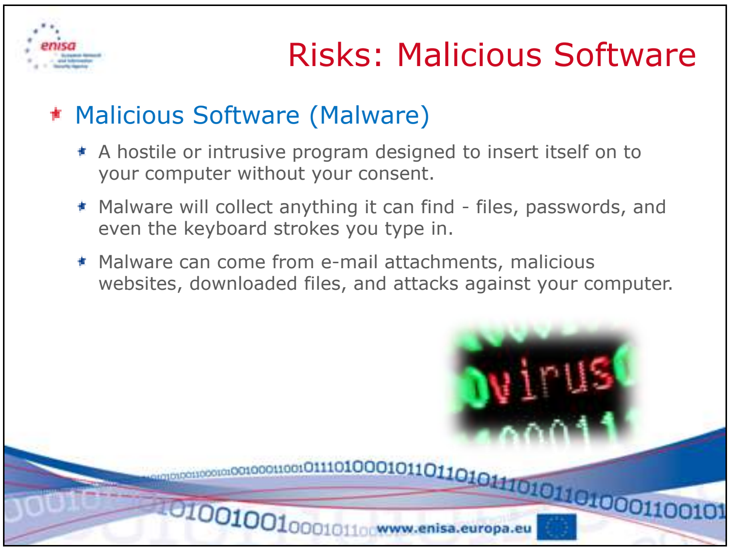
In reality, every operating system and application has vulnerabilities. Each operating system has different types of issues, but in the end, they are all susceptible to outside attackers and malicious software. Different malicious software is designed for different operating systems and applications.

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.

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: **Mal**icious and Soft**ware**.

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

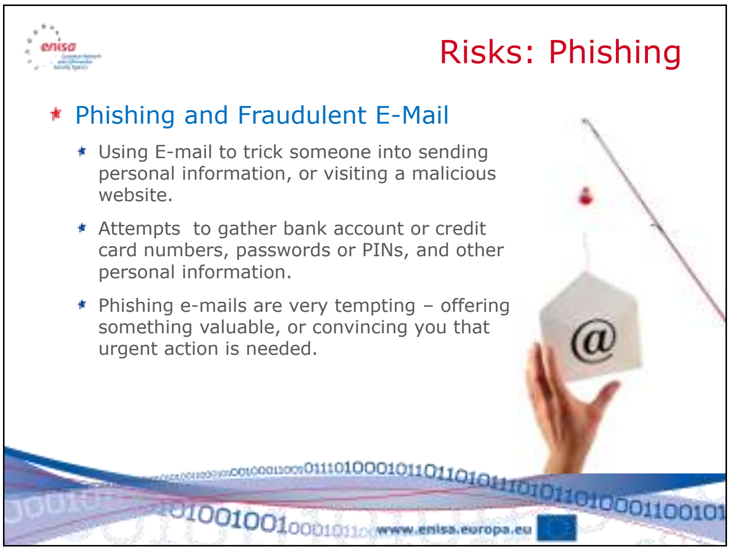
References

http://technet.microsoft.com/en-us/library/dd632948.aspx
http://en.wikipedia.org/wiki/Malware

http://malware.wikia.com/wiki/Main_Page
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

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.

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.

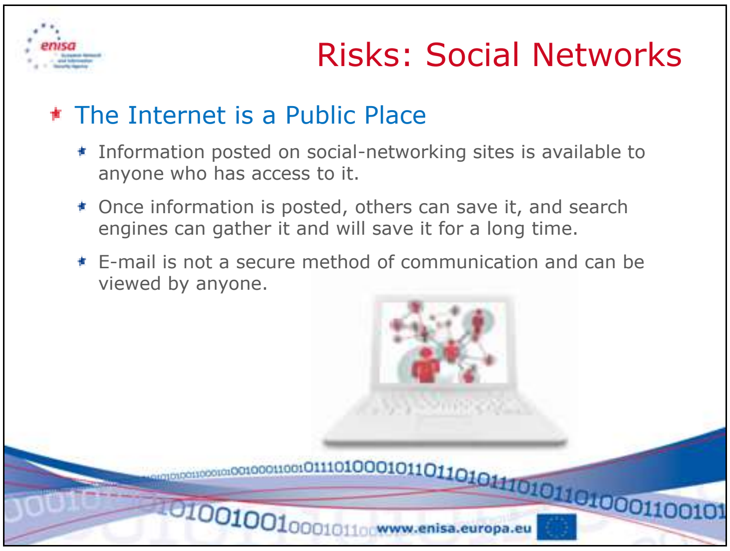
SPAM is a very large problem. SPAM is any e-mail which comes from sources we did not ask to send us e-mails or that we did not give our consent. It accounts for over 80% of all e-mail traffic. Companies spend a large amount of time and money to combat SPAM and filtering it is considered a standard part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

Discussion points

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

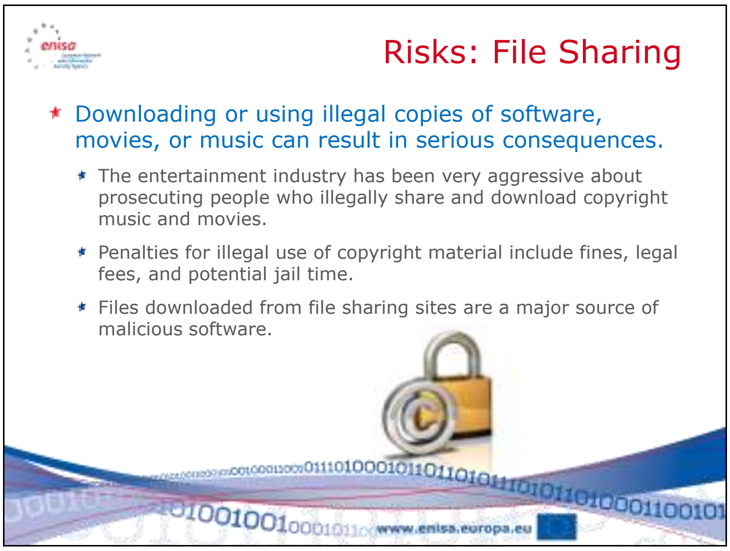
The information that is placed there is virtually impossible to remove. It also is collected by search engines, and can be viewed by almost anyone. Once it enters in to the world of the search engines, it is virtually impossible to remove.

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.

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?

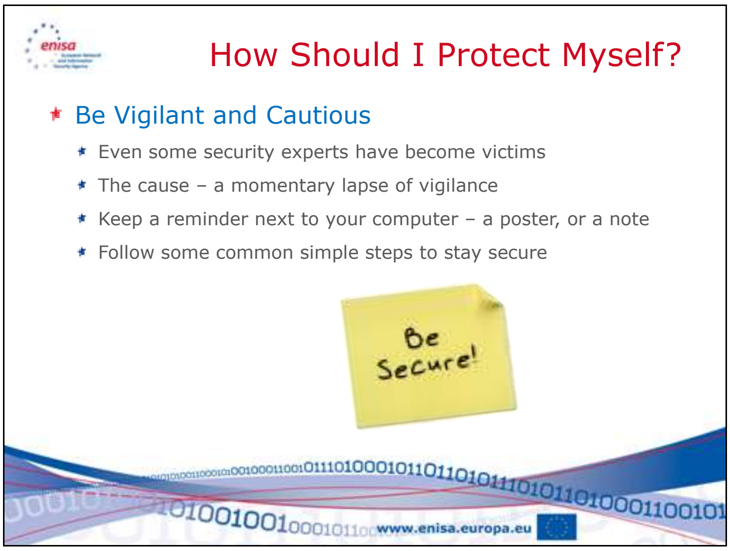
Discussion points

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

Discussion points

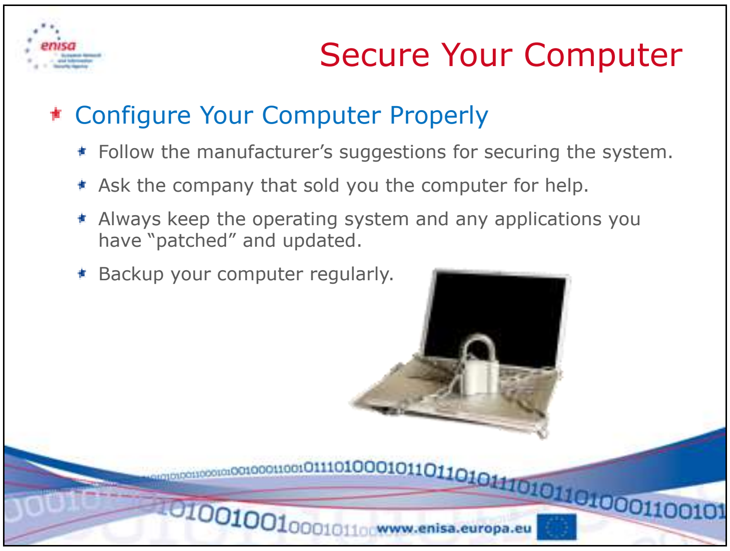
Being aware of security risks and being vigilant are the most important steps. Many people, even experts have relaxed, and the result has been damaging and time consuming.

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

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.

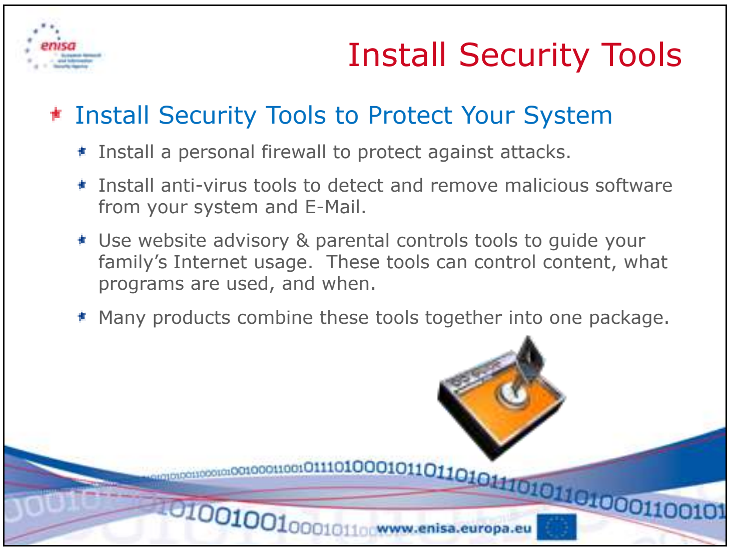
By configuring your browser to block pop-up windows you reduce the possibility of a site displaying a pop-up with malware embedded in it, or with links that will install malicious software. This, like patches is only a partial fix to the problem. Blocking pop-ups only address one possible way that malware 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.mspx
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

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.

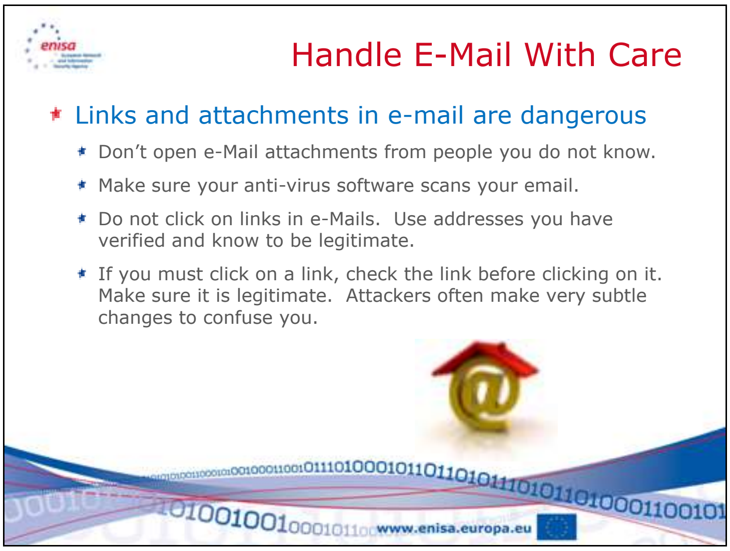
Personal computer security and anti-virus products are not full-proof. They cannot detect all malware. Some malware is disguised as Trojans – programs that look normal but which really contain malicious software inside. It is still important for you to be aware and avoid common user mistakes that result 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.mspx
http://www.cert.org/homeusers/HomeComputerSecurity/
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.

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?

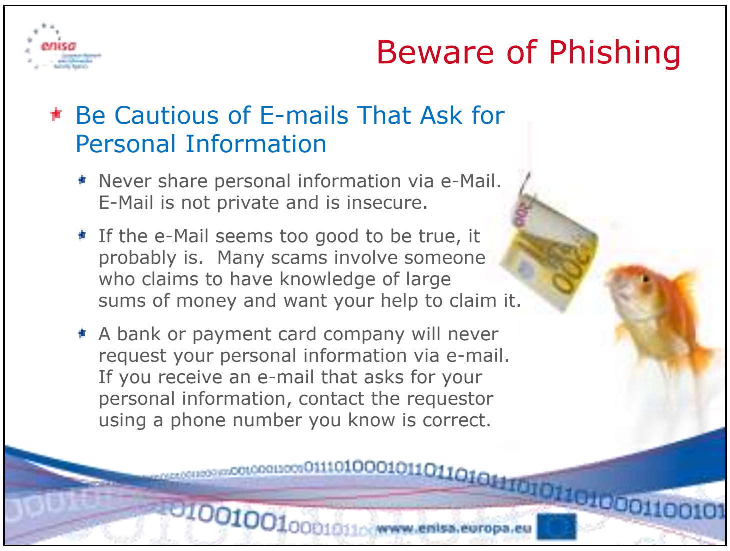
These items can help you identify a fraudulent e-mail. If you find these discrepancies, delete the e-mail. If you are still not sure if the e-mail is fraudulent or not, contact the sender through the phone, or through a method you know is legitimate. Do *not* click on the link or respond directly to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

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.

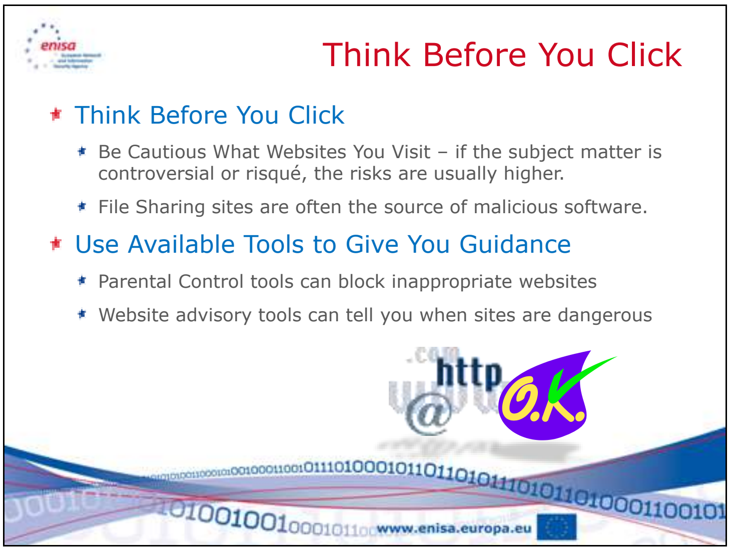
Keep in mind: no bank or payment card company will ever ask you to send personal information, passwords or PINs via email. These types of companies are typical targets for criminals using phishing. Many banks and payment card companies will post news of the newest phishing attacks. If you are unsure 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 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

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.

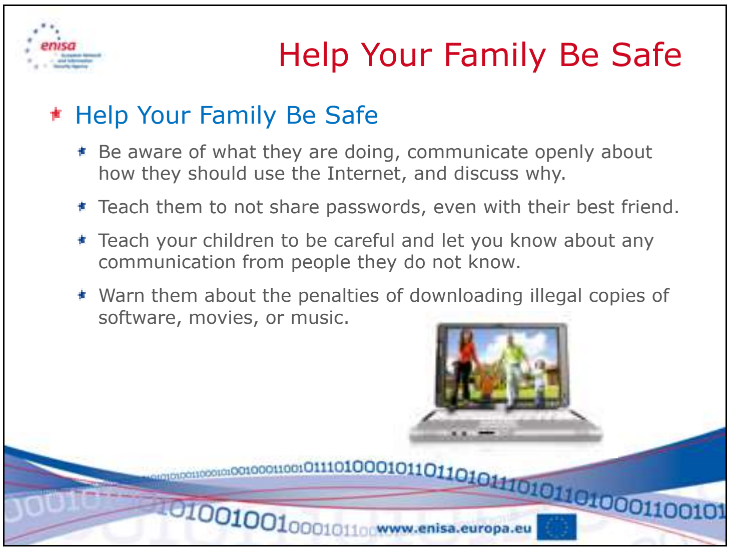
File sharing sites also contain a large percentage of infected files. While it can be enticing to be able to download the latest music, pictures or programs, the high probability and risk of infecting your system with malware should be considered.

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://www.us-cert.gov/cas/tips/ST05-007.html
http://www.wired.com/techbiz/media/news/2004/01/61852

Slide 21



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.

Discussion points

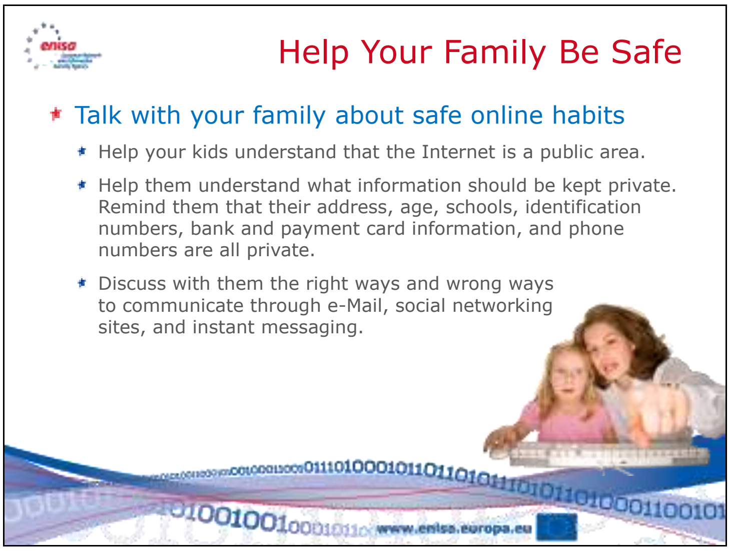
There are many good resources for talking to your children about their use of the Internet. The most important step is to talk to them openly about what is acceptable and what is not.

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.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.

Discussion points

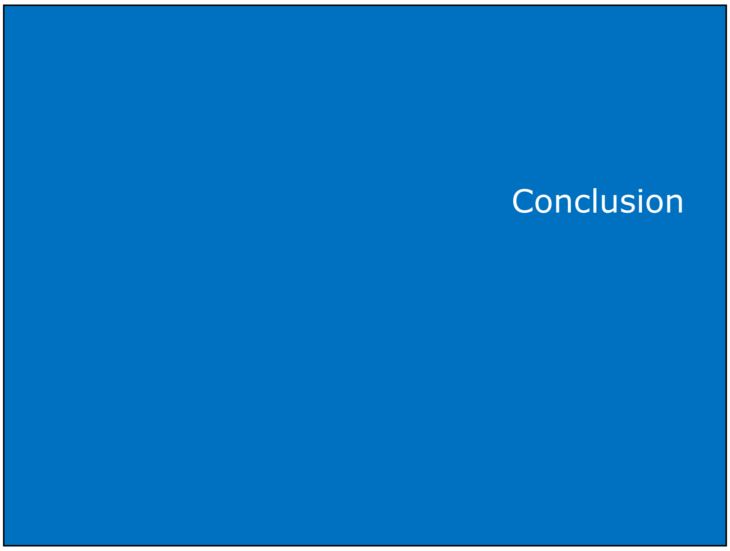
Children often do not recognize risks as we do since they are typically very trusting. The awareness you instil in them should consider the risks, and also good habits. These habits should not only include caution, but also good etiquette when using e-mail, social networks, and other communications.

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



Conclusion

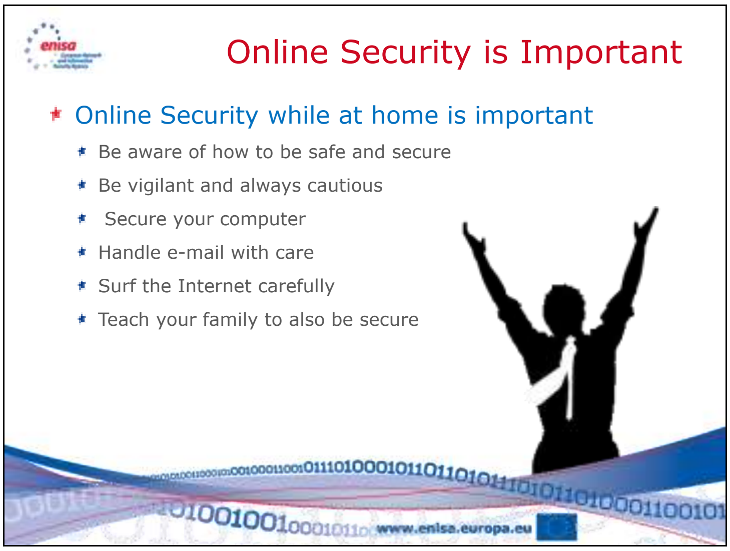
Discussion points

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

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

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

Discussion points

N/A

References

N/A

Online security at home: 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