Online security at home

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:

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.

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

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.

Why is Security Important?

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

Using Internet at Home: Risks

- With those benefits come risks:
  - Viruses
  - Malicious Websites
  - Spyware & Pop-Ups
  - Spam
  - Online Scams and Fraud
  - Inappropriate Content

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?

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.

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.

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.

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.

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.

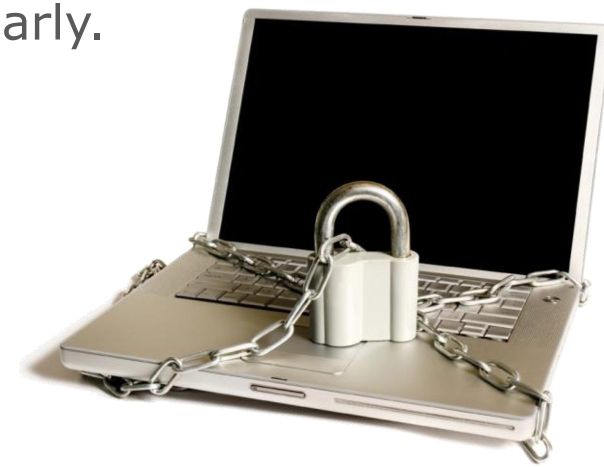
How Should I Protect Myself?

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

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.



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.

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.

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.

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

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.

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.

Conclusion

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

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