E-mail security

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

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

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 easy to understand information that focuses employees' attention on information security and allows them to recognise and respond accordingly to e-mail threats.

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 utilise while performing security awareness training using this material.

Why is E-mail Security Important?

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

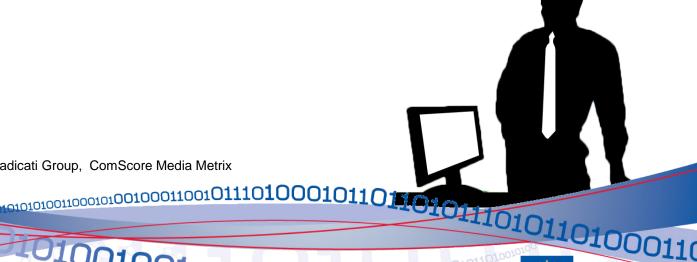★ 247 billion messages are sent per day

Sources: Radicati Group, ComScore Media Metrix

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

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

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

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

How to Use E-mail Securely

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.

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

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.

E-Mail Security Tip #4

★ ## Use Tools to Help You

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

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

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

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

Remember to Check for Updates Today!

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.

Conclusion

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

- ★ Recognise and avoid fraudulent E-mails

- ★ Implement security tools to protect your E-mail

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