

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.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2010



Security when working remotely: *Train the trainer reference guide*

February 2010

Contents

ABOUT ENISA	2
CONTENTS	4
EXECUTIVE SUMMARY	5
HOW TO USE THIS MANUAL	6
STRUCTURE OF THE MANUAL.....	6
STRUCTURE OF THE PRESENTATION PAGES.....	6
THE PRESENTATIONS SLIDES	7
SLIDE 1	7
SLIDE 2	8
SLIDE 3	9
SLIDE 4	10
SLIDE 5	11
SLIDE 6	12
SLIDE 7	13
SLIDE 8	14
SLIDE 9	15
SLIDE 10.....	16
SLIDE 11.....	18
SLIDE 12.....	19
SLIDE 13.....	20
SLIDE 14.....	22
SLIDE 15.....	24
SLIDE 16.....	25
SLIDE 17.....	26
SLIDE 18.....	27

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 how to be secure when working remotely.

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 utilise 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 Security while working remotely 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 how to be secure when working remotely 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



Discussion points

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

When everyone is introducing themselves, ask them to also say how they use e-mail, and what do they expect to get from the course. The answers will tell you what scenarios you can use as examples for this course, and what their expectations are for this course. This information is very useful so that you can adjust your discussions accordingly.

References

N/A

Slide 2

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the Agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on information security awareness matters, please use the following details:

Isabella Santa, Senior Expert Awareness Raising - E-mail: awareness@enisa.europa.eu

Internet: <http://www.enisa.europa.eu>

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA regulation ((EC) No 460/2004). This publication does not necessarily represent the state of the art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2010.

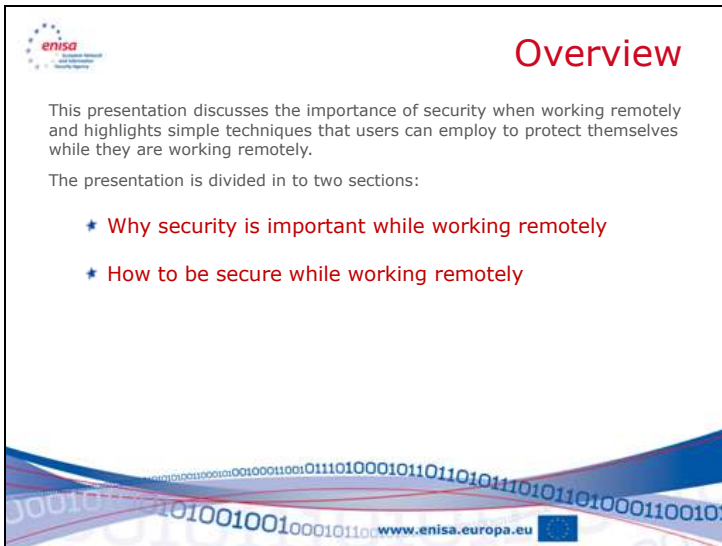
Discussion points

Introduce ENISA and their activities. Suggest that attendees should examine 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

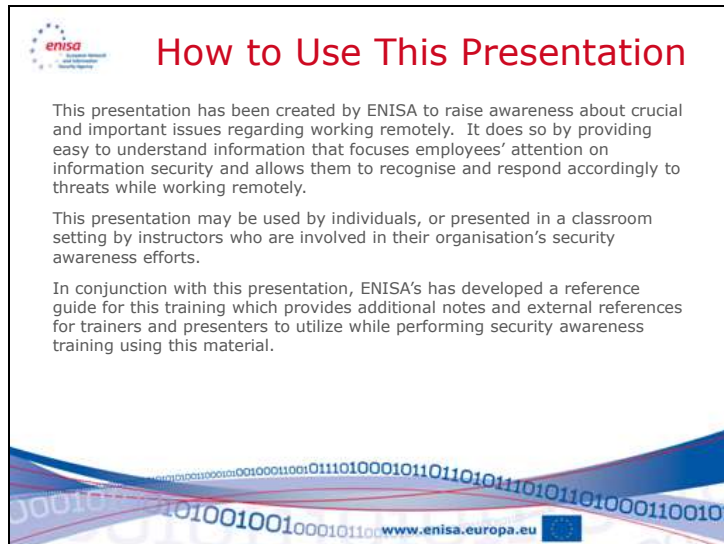


Discussion points

Point out that this presentation is intended to make users aware of the most common and pervasive risks when working remotely, 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 work safely and securely while they are remote.

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 working remotely. 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 threats while working remotely.

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



Discussion points

This is the start of Section 1, "Why Security is Important While Working Remotely?"

References

N/A

Slide 6

Why Be Secure

- ★ Working Remote Presents Many Risks
 - ★ You are responsible for your own security
 - ★ Public places can have criminals and competitors
 - ★ Lack of preparation can make you an easy target
- ★ Good preparation can limit the risks!

www.enisa.europa.eu

Discussion points


When you work remotely, you are responsible for ensuring the security of yourself, your belongings, and your information. When you work remotely, you do not have the benefit of the security you have in your office. You typically do not often have control over your environment or the people you are around. This makes working remotely more of a risk than your environment at work or at home. Lack of preparation for working remotely can make you an easy target for thieves, pick-pockets, unscrupulous competitors, and other criminals.

Good preparation however can significantly reduce your risks and make your experience far more relaxing and productive.

References

<http://www.itpro.co.uk/126695/remote-working-is-major-network-security-concern>
<http://www.itpro.co.uk/187986/remote-working-is-the-chink-in-the-network-armour>

Slide 7



Risks of Working Remotely

- ★ A lack of security can result in significant losses
 - ★ Theft of property and valuables
 - ★ Loss of confidential information
- ★ Simple techniques can make you secure
 - ★ Personal security to protect yourself
 - ★ Protection of your valuables and information

Discussion points

If you do not have good security habits, you can suffer a significant loss. You can have your property or valuables stolen. This might include your wallet, money, jewellery, and identification documents. You may also lose confidential information you're carrying. The theft of wallets, check books, and the identification cards, payment cards, and bank account information they contain is the main methods of identity theft. The loss of these items can also hamper any plans or travel.

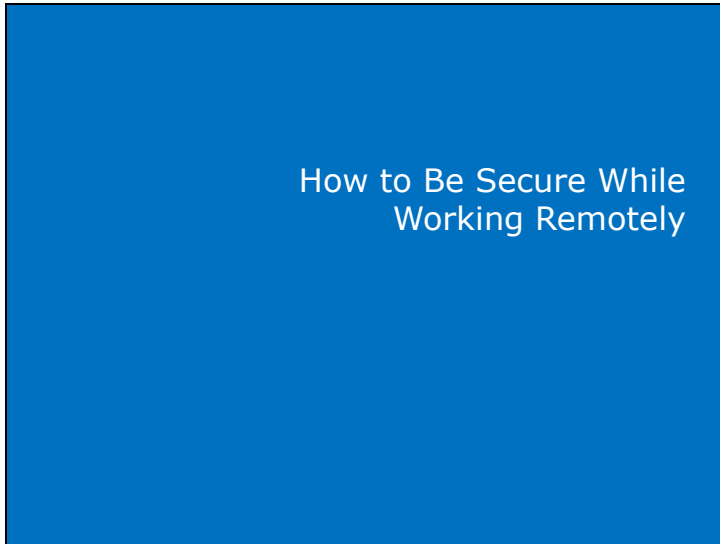
The theft may include a briefcase or a laptop. The information that they contain can include confidential company product plans, customer names, proprietary knowledge, and other items that can be very valuable to a competitor. Even the personal information that is stored there is valuable to a thief. The inconvenience that results can spoil your work and your travel.

What can seem like a simple incident can actually result in a significant problem.

Simple techniques can, however, protect you against many of these security risks. These simple techniques should focus on your personal security to protect yourself, how to protect your valuables and confidential information, knowing where to find assistance when you need it, and having contingency plans in case of emergencies.

References

N/A

Slide 8***Discussion points***

This is the start of Section 2, "How to Be Secure While Working Remotely"

References

N/A

Slide 9



Prepare Yourself

- ★ Prepare yourself and your materials for any remote work
 - ★ Only take documents that you absolutely need
 - ★ Travel with as few valuables as possible.
 - ★ Lock away any other confidential documents, identification, payment cards, or other personal information you don't need.

www.enisa.europa.eu

Discussion points

It is important to prepare for any remote work – whether just working from home, or while on the road.

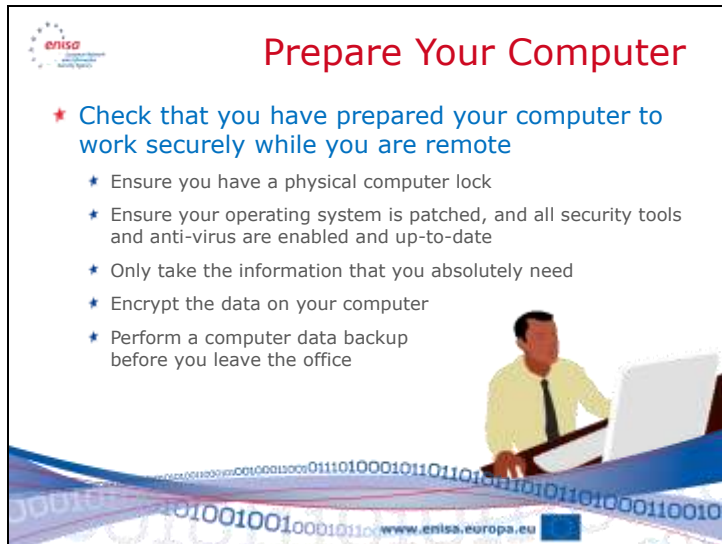
When you are preparing, only pack what you need. Avoid taking any data, documents, information, or valuables that you do not absolutely need while you are away from the office. This will reduce the risk and amount of data that is lost if something does happen to your computer while you are working remotely. It will also reduce the number of things you must worry about and secure.

Know what information is the most sensitive and avoid taking that type of information if at all possible. Information such as your personal identification, customer confidential or personal data, protected information (by law, or regulation), sensitive business plans, and proprietary data should be left at the office. There are numerous examples of employees losing valuable data after taking it home or while working remotely.

By locking away any payment cards, identification or other personal information, you ensure it is safe while you are gone.

References

http://www.cio.com.au/article/184746/fragility_road-warrior_security
<http://www.securityfocus.com/infocus/1186>
<http://fcw.com/Articles/2008/03/03/Stolen-VA-laptop-caught-in-safety-net.aspx>
<http://www.dodbuzz.com/2009/12/22/top-secret-brit-laptop-stolen/>
<http://www.securityfocus.com/news/11393>

Slide 10

Prepare Your Computer

- ★ Check that you have prepared your computer to work securely while you are remote
 - ★ Ensure you have a physical computer lock
 - ★ Ensure your operating system is patched, and all security tools and anti-virus are enabled and up-to-date
 - ★ Only take the information that you absolutely need
 - ★ Encrypt the data on your computer
 - ★ Perform a computer data backup before you leave the office

Discussion points

If you are taking your computer, it is important to ensure that it is secure. Not only is the computer itself valuable to a thief, but the data contained on it is also valuable to thieves and competitors. Many people have been the victim of computer theft which has resulted in the loss of sensitive company secrets, millions of personal records and information, and government secrets. Proper preparation might have prevented these losses.

A good computer lock will allow you to secure your computer while you are working on it, and will prevent most snatch-and-grab thefts.

Patching your computer and making sure it is up-to-date gives you the most recent security tools before you go on the road. It will minimize the exposure to malware, and attacks when your ability to make updates may be limited.

If you must take confidential or sensitive information and data on your laptop, encrypt it. Your company should be able to provide you with a solution, as many newer operating systems include disk encryption technology, and many third party tools are available as well.

Performing a data backup allows you to restore information if your system is stolen, damaged or has an accident while you are remote. Knowing that any damage to your computer can be mitigated by having a backup of your data can make you breathe a little bit easier.

References

<http://www.securityfocus.com/infocus/1187>
<http://technet.microsoft.com/en-us/windows/aa905065.aspx>
<http://docs.info.apple.com/article.html?path=Mac/10.4/en/mh1877.html>

<http://www.truecrypt.org/>

<http://www.pgp.com/products/wholediskencryption/>

Slide 11

Communicate

- ★ **Communicate frequently**
 - ★ Communicate your plans and itinerary with office associates and family members
 - ★ Inform them of any changes or status
 - ★ Observe and read any notices from your company or other news sources regarding risks in your area

www.enisa.europa.eu

Discussion points

Frequent communication with family members and office associates can ensure that if anything happens to you, there is someone with knowledge of your plans and your itinerary.

Also observe any notices from your company about new policies, procedures, security issues, and other information about how to work remotely. The communication between you, your office, and your co-workers is one of the most important parts about working remotely. Without this communication it is easy to lose touch with important changes, and not hear about necessary information.

References

http://homebusiness.about.com/od/workingathome/a/telework_gas.htm

<http://www.bizjournals.com/stlouis/stories/2009/10/26/smallb1.html?q=telecommuting%20communication>

Slide 12



Physical Surroundings

- ★ Be aware of your physical surroundings
 - ★ Make sure doors to locked areas close behind you
 - ★ Lock your room or office when you step away
 - ★ Do not leave valuables, your computer or important documents unattended in public places, in hotel rooms, or in your car.
 - ★ Be aware of people or activities occurring around you

The slide features a blue and white illustration at the bottom showing silhouettes of business professionals in an office setting. The background of the illustration includes binary code (0s and 1s) and the ENISA logo.

Discussion points

Your physical surroundings can have a very big impact on the security of yourself, your computer, and your belongings. Ensure physical security is in place when you are working. Having locked doors and safe places to work can reduce your stress and allow you to focus on your task at hand.

If you step away, even for a moment, make sure the room or area where you are working is secure. Do not leave doors to rooms open or unlocked.

Never leave valuables such as computers, your mobile phone, thumb drives and other storage devices unattended in a public place. Even when you think an area is secure, still protect these items by keeping them locked up and out of sight. Never leave these items in hotel rooms as staff and outsiders can gain access to your room and remove these items while you are away.

Be aware of your surroundings and the activities occurring around you – they can be good indications if an unsafe situation may be occurring, or of any impending security threats. It is not necessary to be paranoid, but awareness is part of a good defence.

References

<http://www.securityfocus.com/infocus/1186>

Slide 13

Protect Information

- ★ **Protect your confidential information**
 - ★ Do not work on confidential information in public places
 - ★ Keep information you are not using locked away and out of sight from others around you
 - ★ Do not use public computers for viewing any confidential or personal information
 - ★ Do not let others use your computer

www.enisa.europa.eu

Discussion points

If you are carrying confidential or personal information, it is important to protect at all times – when you are using it, or when you are just carrying or storing it.

Public places can be full of people interested in the information you may be working on. Some could be thieves, and others could be your competitor. Some information you may be carrying may be protected by laws and regulations and must be kept confidential. Working on this data in public places exposes it to disclosure. You or your company could be held liable for disclosing that information.

Public computers are not well protected. Previous users may not have used safe habits to surf the Internet, or may have intentionally installed malicious software that collects any sites you visit, any screens you view, or anything you type – including usernames, passwords, bank account numbers, or any other confidential information. Avoid public computers for any work that involves personal or confidential information.

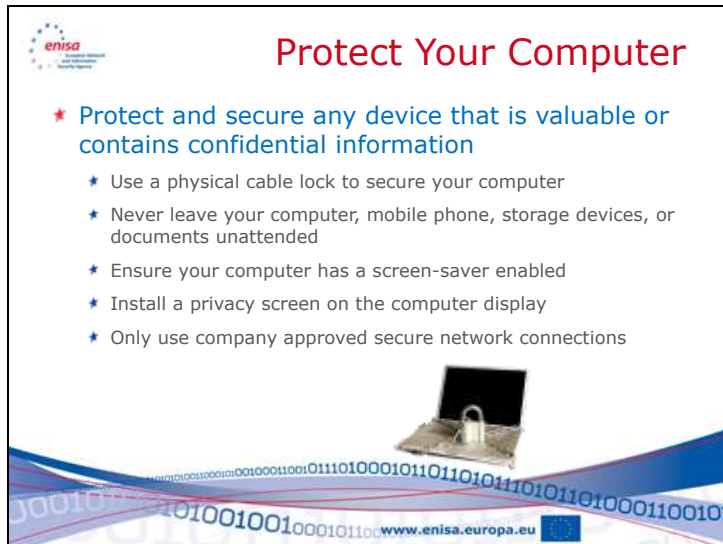
If you are travelling with your office computer, it is important to not let others use that computer. They can view confidential information that you have stored on it. They can visit malicious websites and install software (intentionally or by accident) that compromise the computer. They may also simply steal the computer from you. Never allow anyone, even family members to use your office computer. It is your responsibility to protect the company's confidential information, and if there is information that is protected by law or regulation, you can be liable for its safety.

References

<http://www.microsoft.com/atwork/security/laptopsecurity.aspx>
http://www.cio.com.au/article/184746/fragility_road-warrior_security

http://holton.it-online.co.za/index.php?option=com_content&view=article&id=23%3Akeeping-systems-and-data-safe-and-secure-while-working-remotely&Itemid=1
http://www.cisco.com/web/CA/pdf/Understanding_Remote_Worker_Security_A_survery_of_User_Awareness_vs_Behaviour.pdf

Slide 14



Protect Your Computer

- ★ Protect and secure any device that is valuable or contains confidential information
 - ★ Use a physical cable lock to secure your computer
 - ★ Never leave your computer, mobile phone, storage devices, or documents unattended
 - ★ Ensure your computer has a screen-saver enabled
 - ★ Install a privacy screen on the computer display
 - ★ Only use company approved secure network connections

www.enisa.europa.eu

Discussion points

Never leave your computer unsecured or unattended. This invites a thief to steal the computer, to attempt to access it, and to not only benefit from the value of the computer, but also the information it contains. Leaving documents or a computer in your car, your hotel room, or any other public place is an invitation for a thief. A single laptop in the United States was stolen from a government employee's home and resulted in the loss of over 1 million personal records and information.

By ensuring your security tools are up-to-date you can minimize the risk while travelling by knowing you have the most recent updates available.

Configuring screensavers and installing privacy screens on your computer display can provide some limited protection when working in public areas where others might be able to see your screen. It will not protect your computer if you leave it unattended. A thief or attacker may still sneak up to your computer before the screensaver engages and steal or view information.

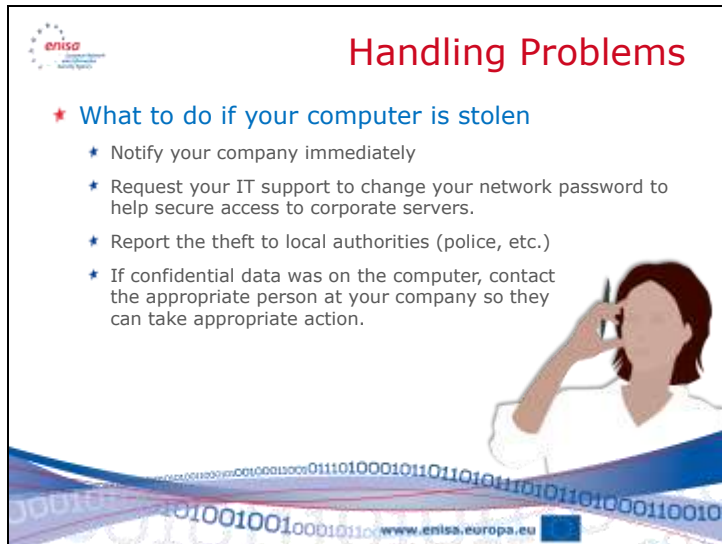
Avoid connecting to wireless networks – while some may seem secure, there are many locations where wireless networks are actually spoofed sites and malicious sites which monitor everything you do over the network. They will monitor your Internet usage, any messages or information you send, and attempt to intercept connections to secure websites.

Instructor: Take note of the remote access tools that are available. Identify how a user would request remote access, and what policies and procedures the user must follow.

To help protect your security while working remotely, only use the company provide secure network connection – which is often referred to as the "VPN" (Virtual Private Network). If configured correctly, this network will allow you to transmit data securely to and from your company. It does not provide any additional security for your computer, but it will limit the ability of anyone else on the public network (including thieves and attackers) to view your confidential data as it is sent to and from your computer.

References

<http://www.onguardonline.gov/topics/laptop-security.aspx>
<http://www.microsoft.com/atwork/security/laptopsecurity.aspx>
<http://technet.microsoft.com/en-us/library/cc722662.aspx>
<http://blogs.techrepublic.com.com/10things/?p=335>
<http://www.securityfocus.com/brief/910>

Slide 15

Handling Problems

- ★ **What to do if your computer is stolen**
 - ★ Notify your company immediately
 - ★ Request your IT support to change your network password to help secure access to corporate servers.
 - ★ Report the theft to local authorities (police, etc.)
 - ★ If confidential data was on the computer, contact the appropriate person at your company so they can take appropriate action.

www.enisa.europa.eu

Discussion points

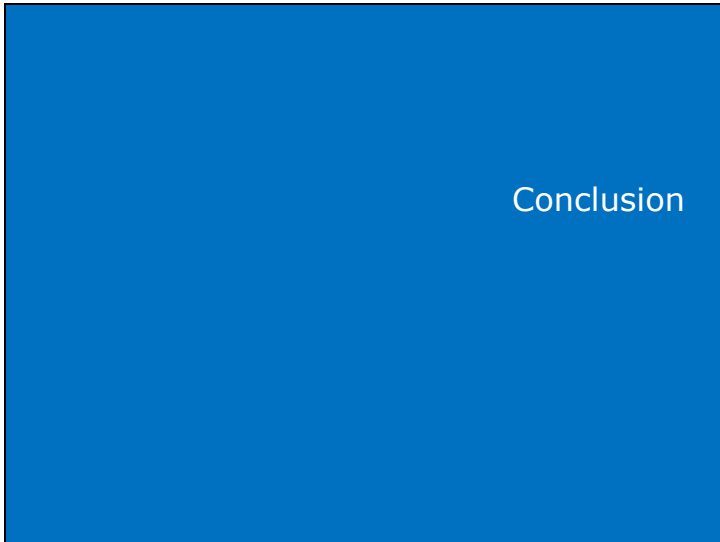
Instructor: Identify the incident response procedures for the organisation and what steps a user should take if their laptop is stolen.

If your computer is stolen it is important to report it immediately. Any delay in reporting the laptop theft can create liability for you and the company. Reporting it immediately allows your company and the authorities to respond to the theft quickly and appropriately. Let your company know what information you had on it, when it was stolen and any other facts they need for their investigation.

References

N/A

Slide 16



Discussion points

This is the conclusion of the presentation.

References

N/A

Slide 17

Security is Important

- ★ Security while working remotely is important
 - ★ Preparation is important so you can protect
 - Yourself
 - Your valuables
 - Your information
 - ★ Be aware of how to be safe and 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.

As we talked about in the beginning, E-mail is important to both companies and individuals.

We also discussed the many security risks to E-mail including loss of confidentiality, authenticity, and risk of fraud.

We talked about key ways to protect yourself:

Don't send confidential or personal information via E-mail

Recognise fraudulent E-mails including phishing, SPAM, and E-mails with malicious content.

Lastly, take advantage of the tools that are out there to protect your computer from fraudulent E-mails, malicious software, and SPAM.

References

N/A

Slide 18



Discussion points

N/A

References

N/A



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