ENISA's ten security awareness good practices

July 09

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

ENISA's ten security awareness good practices

July 2009

Contents

Executive summary

This booklet touches upon crucial and important issues of awareness of information and communication technologies (ICT) for organisations. It does so by providing security good practices to focus employees' attention on information security and allow them to recognise IT security concerns and respond accordingly.

Good practices can be used as guidance for the main steps to undertake when promoting information security awareness. ENISA has produced this booklet to sensitise employees to information security risks and remind them of the basic golden rules. It is available for use in any information security training programme, awareness activity and company website.

The ENISA's ten security good practices are part of the set of tools developed in line with the information security awareness campaign that the Agency has launched across Europe.

ENISA's ten security awareness good practices

Recent high-profile data breaches have raised concerns, leading private and public organisations to understand that policies and technologies must be put in place to secure sensitive corporate information. These controls have to ensure the ability to secure information on the network as well as the opportunity to manage data which enter and leave the company. While policies and technology are certainly a critical part of any information security programme, these measures alone cannot deliver sufficient information security in practice.

Awareness of the related risks and available safeguards is the first line of defence for security. Employees are the real perimeter of the organisation's network and their behaviour is a vital aspect of the total security picture. Protecting organisations begins with making sure employees understand their roles and responsibilities in safeguarding sensitive data and protecting company resources and assist the organisation in keeping computers and network safe.

To this end, ENISA is engaged in positively influencing employees' behaviour towards information security, changing the mindset of the human element in order to achieve greater information security self-awareness.

Thus, the Agency has produced this booklet containing ten security good practices. These good practices are a great tool which will sensitise employees to information security risks and remind them of the basic golden rules.

This document is intended to be used by any organisations which are tasked to run initiatives which help employees learn how to protect corporate information and assets proactively.

1. Use of password

Your password is the equivalent of the lock and key to your house on the Internet. Passwords are a major defence, and developing good password practices will help keep your sensitive personal information and identity more secure.

Use a strong password

- ✓ The password of your computer is the key to access all information — both corporate and personal — you have stored on your computer and online accounts. Use a strong password to protect your data: use at least eight characters; combine letters (capital and lowercase), numbers and symbols. The greater variety of characters that you have in your password, the harder it is to guess. Don't use personal information — name, child's name, birthdates, etc. — that someone might already know or easily obtain and try to avoid common words: some hackers use programs that try every word in the dictionary.

Change your password regularly

- ✓ If you believe your system has been compromised change passwords immediately.

Keep your password secret

- ✓ Your password is unique and must not be shared with anybody.
- ✓ Whenever possible, try to commit your passwords to memory. Have a strategy to memorize them.
- ✓ If you write your passwords down, be careful where you store them. Do not leave these records of your passwords anywhere that you would not leave the information that they protect.

Use different passwords

- ✓ Use different passwords for each online account you access (or at least a variety of passwords). If you use the same passwords on multiple accounts, an attacker who gains the access to one account will be able to access to all of your accounts.

2. Protect your computer

- ✓ Lock your desktop when you leave your desk to go for a meeting, a break and/or lunch.
- ✓ Do not allow other people to plug their USB drive into your computer, especially personal non-secure drives.
- ✓ Don't install or use illegal and/or unauthorised software as you are compromising your data security and breaking the law. Unknown outside programs can open security vulnerabilities in your organisation's network.
- ✓ Don't connect any personal disk, music player and/or USB drive to your computer.
- ✓ Don't connect your personal laptop to the network of your organisation as it may contain viruses or malware.

3. Use e-mail and the Internet with care

- ✓ Don't open unknown e-mails and attachments.
- ✓ Don't click on any hyperlinks contained in a suspicious email.
- ✓ Forward e-mail whether it is appropriate. Consider deleting the history of the message before doing so.
- ✓ Share documents in PDF format to ensure that the files cannot easily be changed.
- ✓ Confidential information should be encrypted when sent by e-mail.
- ✓ Surf the Internet carefully.
- ✓ Do not share information about your organisation and duties on social networking sites.
- ✓ Avoid participating in blogs in which your views and opinions may be interpreted as those of your organisation.
- ✓ Don't download documents and material from untrusted parties.
- ✓ Do not access, download, store or send any illegal or offensive material.
- ✓ Remember that what you surf on the Internet using your workstation can be traced back.

4. Use of portable corporate devices: laptops, USB drives, mobile phones and BlackBerrys

Laptops

- ✓ Don't install or use illegal and/or unauthorised software as you are compromising your data security and breaking the law.
- ✓ Switch off wireless connections when not required.
- ✓ Connect your laptop to the network of your organisation regularly to update your security checks.
- ✓ Back up the information stored in your laptop.
- ✓ Lock your laptop when you leave your desk to go for a meeting, a break and/or lunch.
- ✓ Do not allow other people to plug their USB drive into your laptop, especially personal non-secure drives.
- ✓ Don't leave your laptop unattended.
- ✓ Don't leave your laptop on view in the car.

USB drives

- ✓ Use an encrypted USB drive.
- ✓ Limit the number of corporate data which you store on your USB drive, especially on personal non-secure drives.
- ✓ Attach USB drives to key chains/lanyards to avoid loss of media: the reduced size of USB flash drives makes these devices easier to lose or be stolen. Furthermore, the higher storage capacity increases the potential amount of data at risk for unauthorised access. USB flash drives are usually put in bags, backpacks, laptop cases, jackets, trouser pockets or are left on unattended workstations. The number of incidents has increased recently as USB drives get lost, misplaced, borrowed without permission or stolen.
- ✓ Invite users to put the USB flash drive in read-only mode using the physical switch to avoid virus transmission: some USB flash drives include a physical switch to put the drive in a read-only mode to avoid the host computer from writing or modifying the data on the drive.
- ✓ Scan USB flash drive after copying files from an untrusted and/or unauthorised machine to avoid virus transmission.
- ✓ Before plugging your USB drive into someone else's computer, delete all files which are not relevant for the purpose of that action.
- ✓ Backup information: be able to recover data residing on USB flash drives.

Mobile phones and BlackBerrys

- ✓ Switch off wireless connections (i.e. Bluetooth and WLAN) when not in use. Bluetooth technology enables electronic devices to communicate with each other by using a short-range radio link. Some Bluetooth mobile handsets suffer from software bugs which lead to the practice of Bluejacking and Bluesnarfing.
  Bluejacking is when someone sends an anonymous text by creating a message and then sending it to another Bluetooth activated mobile. Bluejacking can be used to send unwanted messages.
  Bluesnarfing is used to copy personal information such as the contacts list from a handset to another.
- ✓ Don't leave your mobile and BlackBerrys unattended. Otherwise, it could lead

to data loss.

5. Handle information with care

- ✓ Mark any document with the appropriate classification code.
- ✓ Protect sensitive content with a password to help prevent someone from changing or deleting it.
- ✓ Clean desk policy: don't leave sensitive data lying around. Carefully dispose documents.
- ✓ Don't leave sensitive information in shared conference facilities or meeting rooms in order to prevent their exposition to anyone using the room after you.
- ✓ Secure printing: print, copy and scan information only if necessary. Remember to collect the document from the printer's output-tray.
- ✓ Always shred documents containing sensitive information and/or marked confidential.
- ✓ Don't store any information on your local drive.
- ✓ Ensure that any third party working with you has signed a non-disclosure agreement before providing any sensitive information.

6. Visitors

- ✓ All visitors should be registered and signed –in when they arrive and out when they depart.
- ✓ All visitors should be provided with a visitor identity badge that needs to be worn at all times while they are visiting the corporate building.
- ✓ Escort visitors around the corporate building at all times. Letting visitors roam around the office is not secure.

7. Report loss and/or damage to portable corporate devices and incidents

- ✓ Report loss and/or damage to portable corporate devices (i.e. mobile, PDA or USB drive) to the IT department of your organisation.
- ✓ Report any found portable corporate device to the IT department of your organisation.
- ✓ Report any security breaches and/or incidents, even if you are unsure.
- ✓ Report any suspicious activities on your workstation and unexpected unavailability of an application if not warned in advance by your IT department.

8. Protect information outside your organisation

- ✓ When you are outside your organisation, ensure you keep sensitive information and equipment secure at all times to prevent theft or loss. In particular when you are in public places handle information with care.
- ✓ Be aware that someone can overhear your conversation. Don't make your organisation's confidential information available to everyone.
- ✓ When travelling or working from a remote place protect yourself against shoulder surfing.

9. Comply with the corporate security policies and procedures

- ✓ Comply with implemented corporate security policies and procedures.
- ✓ Ensure the confidentiality, integrity and availability of data.
- ✓ Respect legal requirements such as copyright restrictions, intellectual property, privacy and software licences.
- ✓ If you see colleagues acting in breach of corporate security policies and procedures, report it immediately.

10. Provide feedback to further fine-tune enforced solutions and security policies

- ✓ Provide feedback to further fine-tune enforced solutions and security policies.
- ✓ Suggest the purchase of any additional software if necessary to carry out your tasks.
- ✓ Ask questions or make suggestions for improving solutions and security policies.

Conclusions

Information must be protected from unauthorised access and employees should understand their roles and responsibilities in safeguarding sensitive data and protecting company assets.

Employees should know what they can and can't take home (company laptops, etc.), what they can and can't do with company resources, and what, if any, role they have in making backups and using security technology.

To this end, ENISA is engaged in positively influencing employees' behaviour towards information security, changing the mindset of the human element in order to achieve greater information security self-awareness.

By keeping these security awareness good practices in mind, employees will focus their attention on information security and allow them to recognise the most common IT security risks and respond accordingly.

References

ENISA, *Secure USB flash drives*, June 2008, available at http://www.enisa.europa.eu/doc/pdf/publications/Secure%20USB%20drives_180608.pdf

ENISA, *Secure printing*, April 2008, available at http://www.enisa.europa.eu/doc/pdf/ENISA_secure_printing.pdf

ENISA’s ten security awareness good practices

ISBN-13: 978-92-9204-025-3

Doi: 10.2824/12769

Catalogue number: TP-80-09-758-EN-C

TP-80-09-758-EN-C

enisa
European Network and Information Security Agency

ISBN-13 978-92-9204-025-3

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