


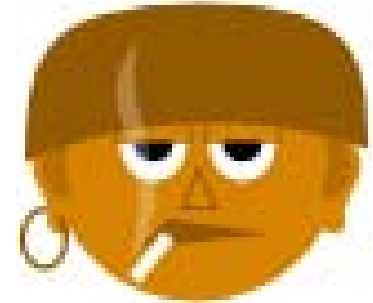










... controlled access

What to know and why ...

-  To understand why ICT security is important in eBusiness
-  To understand what threats are to ICT security
-  To understand how to behave securely



Outline

-  Value of ICT assets
-  Value of ICT security issues
-  Threats to ICT security
-  Possible channels of intrusion
-  Common tools to ensure ICT security
-  How to behave securely

Value of ICT assets

A mission-critical system

- The failure endangers human lives.
- The failure causes great economic damage.
- The inability of the information system to function would be socially irresponsible

It is possible to recognise the value of system if we ask following questions:

- What happens if the system doesn't work correctly for a 1 minute / 1 hour / 1 day / 1 week (the question is how fast the system has to be corrected so that nothing serious happens)?
- What happens if system data is lost?
- What happens if system data becomes publicly accessible?

Task

1. Take 5 minutes to think about the information security in your company and prepare to discuss which ICT assets are most vulnerable

Value of ICT security issues

Confidentiality is essential, i.e. that not everyone can read everything e.g. eInvoices, terms of sales, prices etc.

Integrity is usually the most important issue in eBusiness security. It is needed to create trust. Integrity, in terms of security, means that information is complete and there is not any data disappearance or change. Data with integrity has not been altered or destroyed without such authorisation.

Availability means that good and adequate data is always ready for use.

Threats to ICT security

Cyber crime consists of specific crimes dealing with computers and networks and the facilitation of traditional crime through the use of computers.

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

Hacking is unauthorised use, or attempts to circumvent or bypass the security mechanisms of an information system or network.

Key logger is a hardware device or small program that monitors each keystroke a user types on a specific computer's keyboard.

Threats from communication tools: MSN, Skype, etc – main recommendation is not to execute strange files.

Threats from web-browser: spy ware, cookies etc – main recommendation is to set the web-browser so that cookies are not allowed.



Possible channels of intrusion

Wi-Fi – it is a wireless technology brand intended to improve the interoperability of wireless local area network products

VPN - virtual private network (VPN) is a communications network tunnelled through another network, and dedicated for a specific network

WLAN - wireless LAN is a wireless local area network, which is the linking of two or more computers without using wires

Bluetooth – it is an industrial specification for wireless personal area networks (PANs)

Others (i.e. employees)

Common tools to ensure ICT security

Use

Antivirus software

Firewall

Spam-filter

Electronic identification/certificates




Encrypted authentication

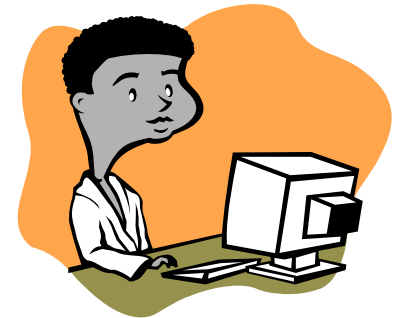
Electronic signature and ID identification

Avoid spy ware while surfing in the internet

How to behave securely

Hardware and software





-  Controlled access to equipment and applications (Identification and authentication)
-  Controlled access to network infrastructure (lines, routers, switches)
-  Controlled installation of software and services into company ICT systems (to avoid malicious software)

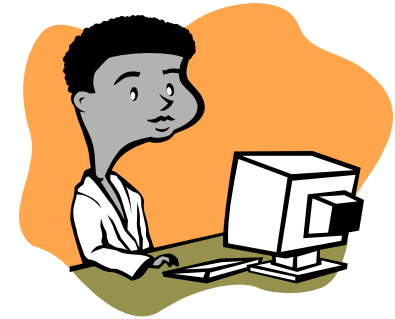




How to behave securely... cont.





Data communication

-  Controlled access to network infrastructure software
-  Controlled use of internet
-  Controlled exchange of data, internally and externally (encryption and authentication)
-  Separate web-server from company ICT system (outsource or isolated instance)



How to behave securely... cont.

Physical security

-  Controlled access to ICT locations, rooms, buildings, service stations
-  Systematically document and manage incidents
-  Systematic theft prevention
-  Controlled maintenance and service








How to behave securely... cont.

Security of documents and data sources

-  Data processing
-  Data storage
-  Data delivery
-  Data removal
-  Data destruction

How to behave securely... cont.

Security rules (examples)

-  Backup your data
-  Manage an incident contingency plan
-  Train employees in security awareness and management
-  Use e-mail safely
-  Manage passwords securely
-  Always log-out applications and computer after a task completed
-  Delete data securely

Task

1. What ICT assets do you have in your company? Please describe and make the list.
2. Which of them are mission-critical?
3. How do you protect your ICT assets?