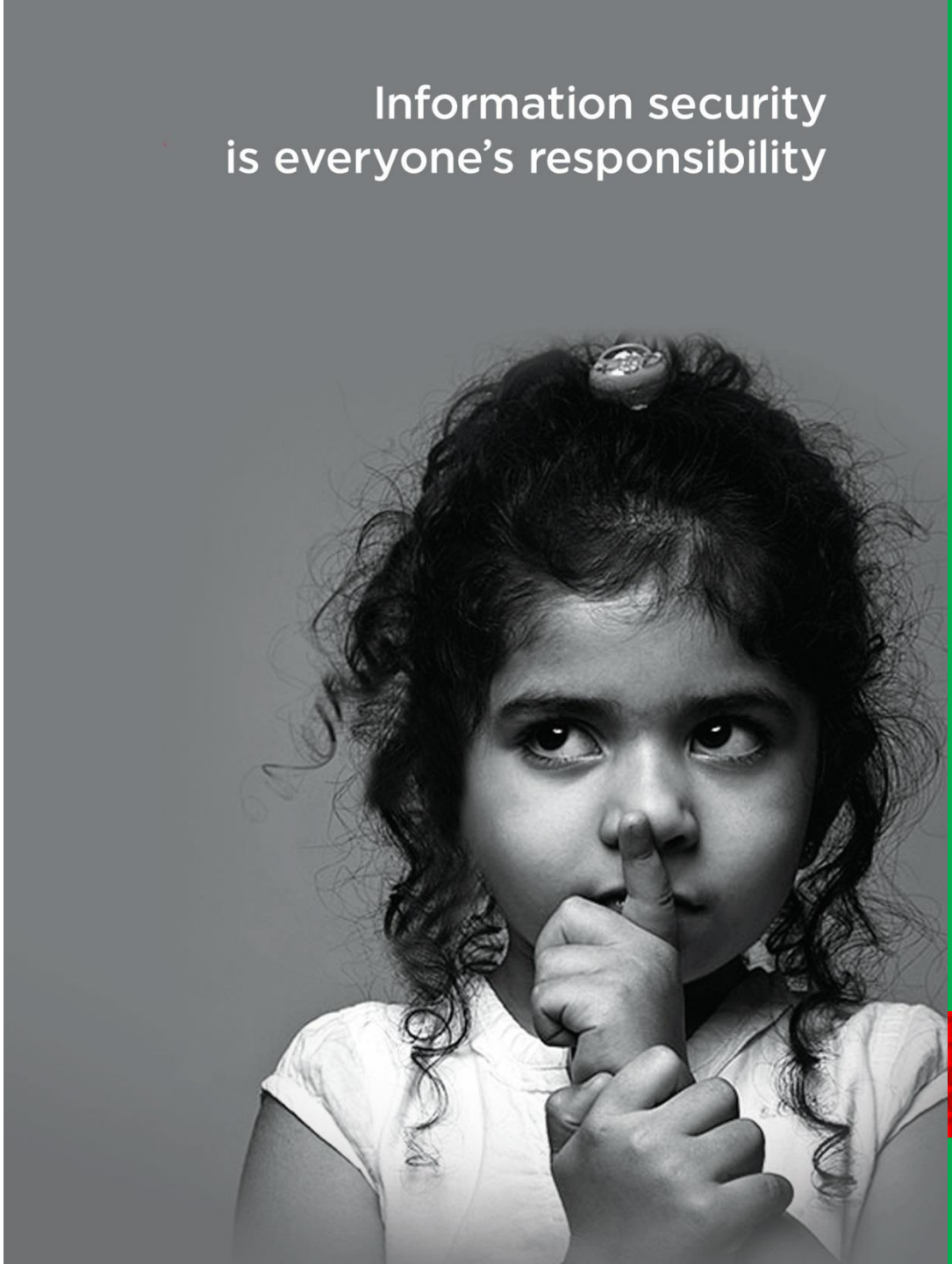
Information Security Awareness Program

Author : Firoz H. Khan



SecuritySense

SecuritySense

Objectives:

Upon successful completion of this program, you will be able to:

- ✓ Understand your roles and responsibilities as they relate to basic practices for Information security.
- ✓ Understand the importance of information security to as a whole and to you as an employee or contractor or consultants.
- ✓ Identify threats to information security.
- ✓ Learn and practice good security habits.
- ✓ Understand security is everyone's responsibilities.

Contents:

- What is Information?
- Example of Information.
- Why information is important?
- What is Information Security?
- What will be if no security?
- Some quotes of information security.
- What is Security policy?
- Why is a security policy needed?
- Who need these policies?
- Where are these policies?
- Local Security Policy and Procedure
- Highlight of Information Protection policy, Password policy, Email distribution policy, Information classification policy, Access control policy, Internet usage rules

Contents:

- What is Threat?
- What is Malicious Code?
- What is Virus, Worm, Trojan Horse, Spyware, Phishing, Social engineering?
- What is identity theft/Phishing?
- Password Management
- Email Management
- Laptop Management
- Security Incident
- As a Organization employee, you should
- As a Organization employee, you should not
- Questions

What is Information?

- Information is an organisational asset, which has a value and needs to be appropriately protected
- In human terms and in the broadest sense, information is anything that you are capable of perceiving. This can include written communications, spoken communications, photographs, art, music, nearly anything that is perceivable.
- Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation.

Example of Information

- Paper
  - Documents
  - Ordinary mail
- Electronic media
  - Database records
  - E-mails
  - CD ROMs, DVDs, tapes etc.
- Films (not as in movies…)
- View foils
- Conversation

Why is information important?

- Customer information
- Systems documentation and configuration
- Business and marketing plans
- Procedures for key processes
- Financial information

How would you deliver your business services if you lost this information?

What is Information security?

- Information Security is about protection of information in support of the business
- Security can be defined as " the state of being free from unacceptable risk".

- Information security is concerned with the preservation of (CIA Triad):
  - Confidentiality
    - Keeping Information safe, hidden, private
  - Integrity
    - Knowing and using information that is Sound and Unchanged by anyone who is not authorized
  - Availability
    - Making resources are present, ready for immediate use

- However we may also consider things like
  - Authorisation
  - Non-repudiation
  - Accountability

Information Security….

- Some Quotes…
- “What keeps the hackers out/ unauthorized access.”
- “Managing access to systems through the use of IDs and passwords.”
- “A barrier, preventing me from doing what I need to do.”

What will be if NO security?

Without protections information can

- Loose confidentiality
- Be modified, with or without our knowledge
- Be deleted or lost irreparably
- Be made unavailable

What is Security policy?

- A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide.
- States management commitment
- Sets out organization’s approach to managing information security
- Sets out clearly the strategic aims and control objectives that will guide the development of the information security management system.
- The main purpose of a security policy is to inform users, staff and managers of their obligatory requirements for protecting technology and information assets.

Who need these policies?

- All employees,
- Consultants,
- Temporaries
- And others not mentioned who access system, applications and networks.

Security is everyone's responsibility.

Where are these policies ?

Policy are available @portal.

All policies are not open for all. For any restricted policy required for applicable use need to contact with Network Security & Audit Personnel.

As a user it is important to know and abide by rules.

Why is a Security policy needed?

- A *security policy* is a preventative mechanism for protecting important company data and processes. It communicates a coherent security standard to users, management and technical staff.
- A policy can be used to measure the relative security of current systems.
- A policy is important for defining interfaces to external partners.
- There are mandatory ICT Act & Organization requirements as regards protection of customer and employee data.
- A policy is a prerequisite to quality control (ISO 27001).

Threats / Risk

- A *threat* is a danger which could affect the security (confidentiality, integrity, availability) of assets, leading to a potential loss or damage.

- **Threats:**
- **Phishing**
- **Identity Theft**
- **Malicious code**

  - Spyware

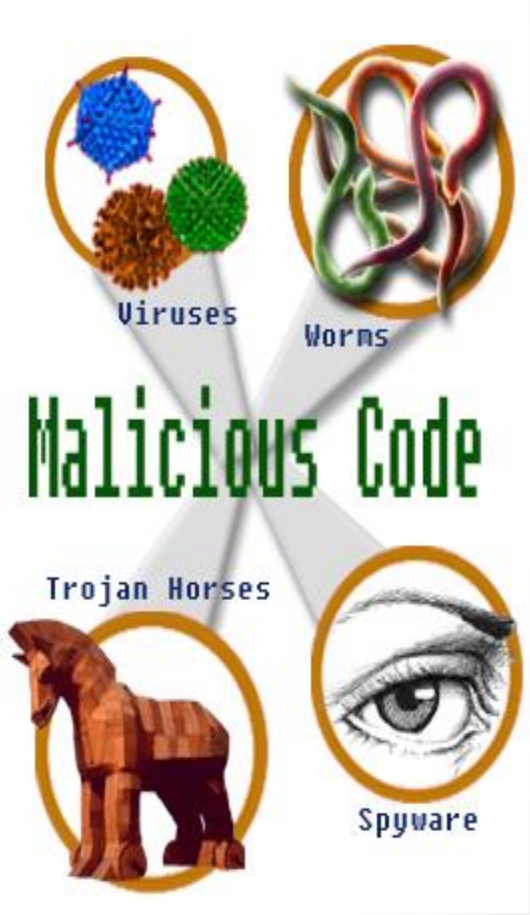
  - Viruses
- **Other threats**

What is Malicious Code?

Malicious code, also known as malware (malicious software), is designed to deny, destroy, modify, or impede a system's configuration, programs, data files, or routines.

Malicious code comes in several forms. Following are some terms you may see in references to malicious code:

- Viruses.
- Worms.
- Trojan Horses.
- Spyware.

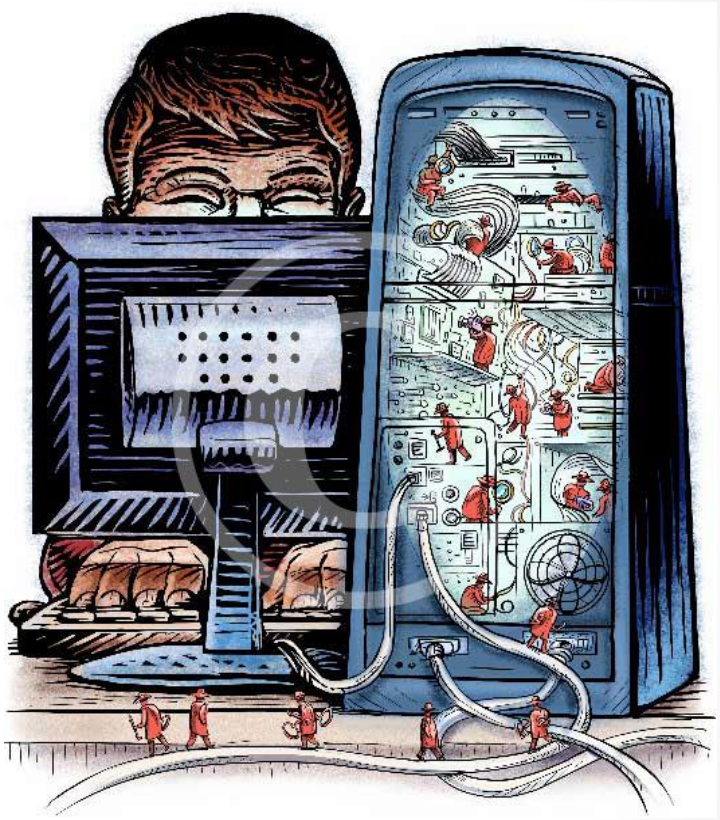


What is Spyware?

Spyware

Software that performs activities on your computer without properly obtaining your consent.

- behaviors such as advertising,
- collecting personal information,
- changing the configuration of your computer, generally without appropriately obtaining your consent first
- It sounds like science fiction, but criminals can secretly install on your computer to steal your identity and do other mischief.



SecuritySense

How can you get rid of spyware?

- Only download from sites you trust.
- Install anti-spyware software.
- Read privacy statements and license agreements.
- Only close windows with the red “x” in the corner.

What can Spyware do?

- Bombard you with ads.
- Change your home page.
- Slow down or crash your computer.
- Transmit information about you online.

What Is A Virus?

.

A computer virus is a small software program that spreads from one computer to another computer and that interferes with computer operation.

What can it do?

A computer virus may corrupt or delete data on a computer,

use an e-mail program to spread the virus to other computers, or even delete everything on the hard disk.

Symptoms of a computer virus

- The computer runs slower than usual.
- The computer stops responding, or it locks up frequently.
- The computer crashes, and then it restarts every few minutes.
- The computer restarts on its own. Additionally, the computer does not run as usual.
- Applications on the computer do not work correctly.
- Disks or disk drives are inaccessible.
- You cannot print items correctly.
- You see unusual error messages.
- You see distorted menus and dialog boxes.
- There is a double extension on an attachment that you recently opened, such as a .jpg, .vbs, .gif, or .exe. extension.

Symptoms of a computer virus (contd.)

- An antivirus program is disabled for no reason. Additionally, the antivirus program cannot be restarted.
- An antivirus program cannot be installed on the computer, or the antivirus program will not run.
- New icons appear on the desktop that you did not put there, or the icons are not associated with any recently installed programs.
- Strange sounds or music plays from the speakers unexpectedly.
- A program disappears from the computer even though you did not intentionally remove the program.

How to protect your computer against viruses

To protect your computer against viruses, follow these steps:

- On the computer, turn on the firewall.
- Keep the computer operating system up-to-date.
- Use updated antivirus software on the computer.
- Use updated antispyware software on the computer.

What is Phishing ?

- This short video illustrates how you may become a victim of Internet fraud via email, websites or instant messenger by being duped into sharing your personal information (e.g., credit card or account information, passwords, social security cards).

*** (Video is available on request.)

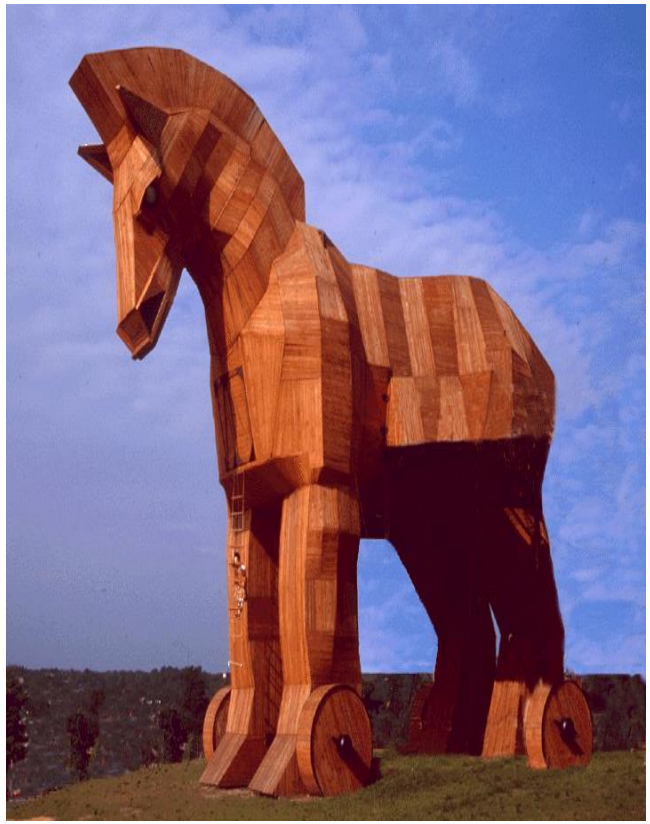
What is a Worm?

- A worm (a type of virus) resides in the active memory of a computer. It duplicates itself and sends copies through e-mail.

What is a Trojan Horse?

- Like the original, software Trojans are dangerous. They typically appear to be one type of software, but have hidden functionality that allows the unauthorized collection, exploitation, falsification, or destruction of data.

  Some Trojan Horses even allow remote and unauthorized access to a computer!



What is Social Engineering ?

- Online criminals can use sophisticated technology to try to gain access to your computer, or they can use something simpler and more insidious: social engineering.
- Social engineering is a way for criminals to gain access to your computer.
- The purpose of social engineering is usually to secretly install spyware or other malicious software or to trick you into handing over your passwords or other sensitive financial or personal information.
- Some online criminals find it easier to exploit human nature than to exploit holes in your software.

Types of Social Engineering:

- Phishing
- Spear phishing
- E-mail hoaxes

SecuritySense

Highlight of Password Policy

- Minimum password length is 8 characters.
- Passwords contain combination of minimum three out of these four: One numbers, one capital character. One small letter, One Special character **(e.g.,!, ?, #, %, *).**
- User can not use the same password after next two times. (system will remember last two password.)
- Limit the number of unsuccessful log-on attempts allowed to 5 (Five) attempts
- In network environment, users need to change password after 45 days interval.

Password Management

- Choose a secure password.
- Add complexity by mixing uppercase and lowercase letters, numbers and special characters.
- Avoid sequences or repeated characters. "12345678," "222222," "abcdefg,“
- Use words and phrases that are easy for you to remember, but difficult for others to guess.
- Avoid dictionary words in any language.
- Don’t share your password with anyone.
- Don’t write it down.
- Watch for signs of misuse.
- Change your password regularly.
- Never provide your password over e-mail or based on an e-mail request.

Software Usage

- ***Organization committed to copy right- intellectual property laws.***
- **Don't use unauthorized / Unapproved Software.**
- **Install Unlicensed/ unauthorized Software is violation of policy**
- **Unlicensed/ unauthorized Software/ freeware:**
  - May be tempting to use useful-looking software that you can get free on the Internet, but these tools may carry a hidden cost.
  - Installing them may often cause other programs to stop working and it can take a long time for your IT teams to track down the problem.
  - More seriously, they can display unwanted ads, slow your PC down or make it less secure by letting the PC download more ads from the Internet.
  - Most seriously, they can be infected by viruses or spyware that are intended to damage your PC or steal confidential information.
- **License software list is available in enterprise portal**
- **Software accusation policy available in enterprise portal**
- **Approval Template is available**
- **Protecting Computers and information assets requires everyone's help.**

Admin Privilege on PC

Allowed User actions with the Administrative Privilege:

- ✓ Reinstall Licenses/ approved Software application for troubleshooting purposes.
- ✓ Execute Licensed/ approved Software application that doesn't run without Admin Privilege.

User actions not allowed with the Administrative Privilege:

- ✘ Install Unlicensed/ unauthorized Software i.e. install software other than Organization IT or user division provided/approved.
- ✘ Reset the local Administrator account password.
- ✘ Uninstall existing Organization IT installed software e.g. MS Office, Unicenter agent etc.
- ✘ Uninstall/disable Antivirus software.
- ✘ Disjoin PC from Windows domain.
- ✘ Disable Windows Firewall.
- ✘ Create/modify local user accounts.

How can you get it ?

- ITS
- Admin privilege Form
- Approval

Highlight of Email distribution Policy

- Do not send or forward email containing libelous, defamatory, offensive or obscene expressions.

- Do not forward or copy any emails or attachment marked INTERNAL or CONFIDENTIAL to any external party without acquiring permission from departments heads.
- Do not send unsolicited email message or chain mails.

Hints and Tips: Use e-mail responsibly and securely...

E-mail is exposed to many vulnerabilities that could turn today's secret into

tomorrow's front-page story. Use e-mail responsibly and securely by following basic security

***measures*:**

Use appropriate content.

- Organization's e-mail is official business correspondence. Choose content and language accordingly.
- Be sure the recipient is authorized to see the content you are sending.
- Never send e-mail that is harassing, pornographic or contains foul language.

Hints and Tips: Use e-mail responsibly and securely...(contd.)

- If you receive e-mail with inappropriate or offensive content, inform help desk**, call :**
- Be aware that company e-mail is typically company property and there is no expectation that its content will remain private only to you and the recipient.

- **Be sure your e-mail is addressed to the right person.**
- Many employee / people have similar names and e-mail addresses, so double-check the address before you click Send.
- When replying, double-check that you are replying only to the person(s) you intended.

Highlight of Access Control Policy

- Purpose:

The purpose of this policy is to establish guidelines, procedures, and requirements to ensure the appropriate protection of Organization's information systems.

1.3 Policy

There must have a procedures which will guide and control user registration, de-registration and periodic follow-up.

2.2 Policy

Unattended Workstations (equipment) is always to be safeguarded appropriately - especially when left unattended.

4.3 Policy

Inactive sessions should be shut down after a defined period of inactivity.

Hints and Tips – In The Office

- ✓ Ensure entrance/exit doors are not left open
- ✓ Practice Clean Desk Policy
- ✓ Do not send fax transmissions containing *confidential* information.
- ✓ Immediately remove all copies of information from the fax machine, printers, meeting rooms, whiteboards, etc.
- ✓ Be careful what you communicate verbally, over e-mail, fax and mobile phones

Hints and Tips – Computers and Laptops

- ✓ Use good password protection
- ✓ Sign off or lock your screen when you leave your desk
- ✓ Only use Organization email for business purposes
- ✓ Backup data and update virus scanners regularly

- × No abusive, unethical or “inappropriate” use of the Internet
- × No software without Unit/Section/Division Head approval
- × Do not leave the computer or laptop unattended or unsecured.

Hints and Tips: Take special precautions when traveling with a laptop.

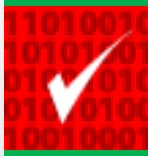
- Keep your laptop in your possession at all times.
- Be especially cautious in certain locations where theft might likely occur.
- Carry your laptop in a nondescript carrying case, one that does not advertise it contains a laptop.
- Don’t leave your laptop in your hotel room or in a Car.
- Keep your eye on your laptop at security checkpoint conveyor belts!
- Never put your laptop in overhead storage bins on planes, buses or trains.
- Never store your laptop in an airport, bus, or train station locker.
- Back up your data files before traveling.
- Prepare your laptop for security checkpoints.
- Be aware of restrictions when you travel abroad.

Security Incident

- A computer security incident is

  - an occurrence having actual or potentially adverse effects that threaten the security of an Organization resources. Organization resources include personnel, computer facilities, workstations, laptops, PDAs/ Smart phone, and other computer hardware and software.

  - the unauthorized use of a computer, or the use of a computer in a violation of laws or pertinent policies.



Security Incident (Continued)

- Examples of security incidents:
  - use of unauthorized accounts,
  - attempts to steal or crack passwords,
  - placement of virus or Trojan horse programs.

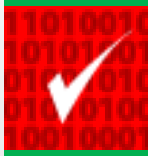
- An incident may originate either from within Organization, or from outside Organization and may involve the activities of members of the Organization community, or outside parties.

Notify:

it is responsibility

As an Employee, You SHOULD

- ✓ Use all ’s information assets appropriately.
- ✓ Participate in Organization’s information security awareness programs.
- ✓ Comply with relevant security policies, standards, and procedures.
- ✓ Report any known or suspected security violations to appropriate management.
- ✓ Take the same care in protecting information even when you are traveling.
- ✓ Learn and practice good security habits



As An Employee, You SHOULD NOT

- × Disable or circumvent any security controls on ’s information systems.
- × Use ’s information assets to illegally gain access to any systems.
- × Access any information that you do not have a need to know.
- × Use or copy software unless it is legal to do so.
- × Share passwords with anyone.


STOP
Think about what you're doing.
Security requires careful actions.
Follow Information security framework.
-Network Security & Audit, Compliance, Technology