***Digital security basics***

Security in information technology (IT) is the defense of digital information and

IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services.

Security is critical for enterprises and organisations of all types and sizes and in all industries. Weak security can result in compromised systems or data, either by a malicious threat actor or an unintentional internal threat.

* Never leave your portable computer unattended, especially when you at a coffee shop, the library or the airport.
* Use tracking and recovery software, such as CyberAngel and LoJach
* If your computer got stolen, get IT department to wipe it remotely.
* If you have to leave your portable computer in your car, never leave it in plain view. Lock it up in the boot or cover it up.
* Use Apple's Find My iPhone system to track missing iPhones, iPods, and iPads.
* Record your portable computer's make, model, and serial number and store them away from the computer.
* ~ If your computer got stolen, call IT to change your logins asap.
* Use STOP (Security Tracking of Office Property)
* Secure your portable computers with anti-theft devices such as security

***Computer protection and maintenance***

You can protect your computer equipment from power surges by plugging it into a surge suppressor, instead of directly into a wall outlet. For added protection during thunderstorms, shut down your computer, turn off your peripheral devices, and unplug the surge suppressor and all computer-related cables from wall outlets, including thee cable for your

* Back up your files regularly, particularly those that are most important to you.
* Test your back up procedures periodically.
* Run utilities that ensure peak performance for your hard disk drive.
* Delete your browser's history and cache files on a monthly basis in order to free up space for your temporary files.
* Apply the latest operating system, driver and security updates.
* Scan your computer for viruses and spyware once a week.
* Keep antivirus and spyware definitions updated

***Types of password assaults***

* Password attacks is a big serious problem nowadays.
* When someone gains unauthorised access to your personal data and uses it illegally, it is called identity theft.
* If a hacker doesn't have physical access to your work area, but your computer is connected to a network, your password can be discovered by hacker using a remote commuter and sottware tools that systematically guess your password, intercept it.
* The brute force attack uses passwords cracking software which choose all possible combinations of letters to decrypt a password, a brute force attack can run for days to crack some passwords.
* ﻿﻿Sniffing is a process of interception information sent out over computer networks.
* ﻿﻿Phishing is when a hacker poses as a legitimate representative of an official organization such as ISO in order to persuade you to disclose highly confidential information.
* ﻿﻿A key logger is software that secretly records a user's keystrokes and sends the information to a hacker.
* ﻿﻿Trojan is a computer program that seem to perform one function while actually doing something else.

***How to prevent attacks***

The best way to prevent password attacks is to adopt best practices for password hygiene and management.

Password best practices include:

* Requiring long, complex passwords that are unique for each website
* account ..
* Implementing multi-factor authentication when possible
* Adopting a password manager to simplify password management and ensure secure storage

***Password security, authentification***

The core function of a password manager (sometimes called a keychain) is to keep track of passwords so users don't have to memorise them. Some password managers also have the ability to fill in forms with stored address and credit card data. Password managers are available as operating system utilities, browser extensions, and standalone utilities.

Authentication protocols that use more than one means of identification are more secure than others. Computer-related security is primarily based on passwords

associated with user IDs. The level of protection depends on good password selection and management on the part of users. A user ID is a series of characters - letters, numbers or special symbols - that becomes a person's unique identifier.

***Malware and its types***

Malware is a program designed to gain access to computer systems, generally for the benefit of some third party, without the user's permission. Malware includes computer viruses, worms, Trojan horses, ransomware, spyware, and other malicious programs.

Types of malware include the following:

* A virus is the most common type of malware
* ﻿﻿A worm can self-replicate without a host program and typically spreads without any interaction from the malware authors.
* ﻿﻿A Trojan horse
* ﻿﻿Spyware collects information and data on the device and user, as well as observes the user's activity without their knowledge.
* ﻿﻿﻿﻿A rootkit obtains administrator-level access to the victim's system. Once installed, the program gives threat actors root to thesystem.
* ﻿﻿A backdoor virus or remote access Trojan (RAT) secretly creates a backdoor into an infected computer system that enables threat actors to remotely access it without alerting the user or the system's security programs.
* Keyloggers, also called system monitors

﻿﻿ One of the most common ways a computer becomes infected is when a user accepts what they see on the screen without reading or understanding the prompt.

When downloading any software (programs, utilities, games, updates, demos, etc.) via the Internet, make sure you're downloading the software from a reliable source.

As a general rule, do not open e-mail you were not expecting to receive. Viruses enter the computer when users open e-mail attachments that contain malicious code.

***How To Protect From Malware?***

The good news is that there are just as many ways to protect yourself from malware as there are different types of malware. Look at these top suggestions:

* Protect your devices.
* Update your operating system and software. Install updates as soon as they become available because cybercriminals search for vulnerabilities in out-of-date or outdated software.
* Never click on a popup's link. Simply click the "X" in the message's upper corner to close it and leave the page that generated it.
* ﻿﻿Don't install too many apps on your devices. Install only the apps you believe you will regularly use and need.
* ﻿﻿Do not click on unidentified links.
* ﻿﻿Choose the websites you visit wisely. Use a safe search plug-in and try to stick to well-known and reputable websites to avoid any that might be malicious without your knowledge.
* ﻿﻿Emails requesting personal information should be avoided. Do not click a link in an email that appears to be from your bank and asks you to do so in order to access your account or reset your password.

***Antivirus Software***

Antivirus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, These antivirus tools are critical for users to have installed and up-to-date because a computer without antivirus software protection will be infected within minutes of connecting to the internet.

* ﻿Scan specific files or directories for any malware or known malicious patterns
* ﻿Allow you to schedule scans to automatically run for you
* ﻿Show you the health of your computer

Antivirus solution protect more than just laptops, computer office fire computers, smartphones. They protect music and photo libraries, and important documents from destruction by malware.

***What is a cyberattack?***

A cyberattack is an attempt to steal, alter, destroy, disrupt, or disable information resources and systems found in computer networks and systems. Cyberattacks can fit into two categories: insider threats or outsider threats.

Cyberattackers use harmful software such as viruses, ransomware, and worms known as malware to access your system's data. When you click on a malicious attachment or link, the malware can install itself and become active on your device. Cyber attackers will sometimes imitate people or companies to trick you into giving up personal information

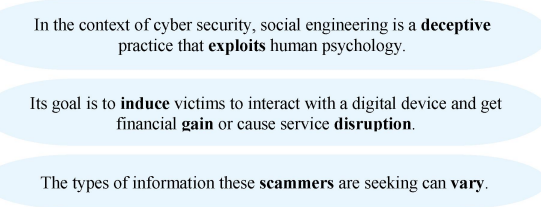
Phishing attacks rely on communication methods like email to convince you to open the message and follow the instructions inside.

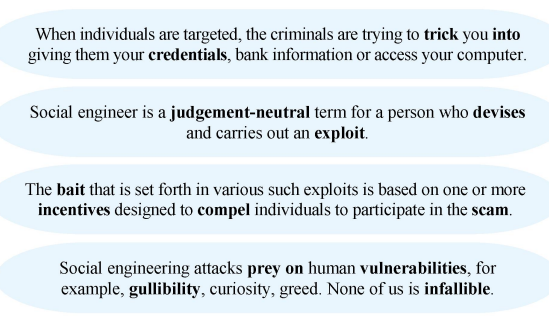
Ransomware is malicious software that cyberattackers can install on your device, allowing them to block your access until you pay the attackers a ransom.

Password attacks can be as simple as someone correctly guessing your password or other methods such as keylogging, where attackers can monitor the information you type and then identify passwords.

Communication channels between connected IoT components can be susceptible to cyberattacks and the applications and software found on IoT devices. Since IoT devices are in connection with one another through the

***Social engineering, state of the issue.***





***Methods of social engineering.***

1. Shouldering (shoulder surfing): g) It occurs when someone surreptitiously watches over your shoulder to nab valuable information.

2. Pharming: f) It redirects website traffic to fraudulent websites that distribute malware, collect personal data, sell counterfeit products, and perpetrate other scams.

3. Phishing: a) This tactic includes deceptive emails to steal information.

4. Baiting: c) It’s an online and physical social engineering attack that promises the victim some gain.

5. Spear Phishing: b) A spoofed email is used to carry out targeted attacks against individuals or businesses.

6. Vishing: h) It is voice solicitation over the phone (voice+phishing).

7. Tailgating: e) It relies on human trust to give the criminal physical access to a secure building or area.

8. Rogue Antivirus: d) Victims are tricked into believing that malware is installed on their computer and that if they pay, the malware will be removed.

***Protection techniques against phishing, vishing, smishing.***

**Protection against phishing:** a) Be cautious about all communications you receive. d) Don’t enter personal information in a pop-up screen. e) Do not click on any links listed in the email message. f) Install a special spam filter on your email application and your web browser.

**Protection against vishing:** b) Don’t pick up the phone, simply let it go to voicemail. Caller IDs can be faked, which means you might not know who’s calling. c) Don’t press buttons or respond to prompts. Scammers often use these tricks to identify potential targets for more robocalls. g) Hang up. h) Verify the caller’s identity. If the person provides a call-back number, it may be part of the scam, so don’t use it.

**Protection against smishing:** a) Be cautious of unsolicited text messages: Just like with email phishing. Scammers often use this method to reach out to potential victims. b) Don’t click on links in text messages: If a text message includes a link, it’s best not to click on it unless you are sure it’s legitimate. c) Verify the sender: If you receive a text message from a number you don’t recognize, don’t respond. d) Install security software on your phone: Just as you protect your computer with antivirus software, consider doing the same for your phone. There are many security apps available that can help protect against smishing. E) Don’t share personal information via text.

***Encryption, its types, usage, importance.***

Encryption helps protect your online privacy by turning personal information into "for your eyes only" messages intended only for the parties that need them and no one else. You should make sure that your emails are being sent over an encrypted connection, or that you are encrypting each message.

Cybercrime is a global business, often run by multinational outfits. Encryption is designed to protect your data, but it can also be used against you. Targeted ransomware is a cybercrime that can impact organisations of all sizes, including government offices. Ransomware can also target individual computer users. Attackers deploy ransomware to encrypt the various devices, including computers and servers, of victims. The attackers often demand a ransom before they will provide a key to decrypt the encrypted data.

Install and use trusted security software on all your devices, including your mobile phone. Keep your security software up to date. It can help protect your devices from cyberattacks. Update your operating system and other software. This can patch security vulnerabilities. Be wary of any email attachment that advises you to enable macros to view its content.

Back up your data to an external hard drive. If you're the victim of a ransomware attack, you'll likely be able to restore your files once the malware has been cleaned up. Consider using cloud services. Don't pay the ransom. You could pay a ransom in hopes of getting your files back, but you might not get them back.

When transmitting electronic data, the most common use of cryptography is to encrypt and decrypt email and other 1) **plain text** messages. The simplest method uses the 2) **symmetric** or **public key** system. Here, data is 3) **encrypted** using a secret key, and then both the encoded message and secret key are sent to the 4) **receiver** for decryption. But, if the message is intercepted, a third party has everything they need to decrypt and read the message. To address this issue, cryptologists devised the 5) **asymmetric** or 6) **public key** system. In this case, every user has two keys: one public and one private. Senders 7) **use** the public key of their intended recipient, encrypt the message and send it along. When the message arrives, only the recipient’s 8) **private key** will decode it.