Cybersecurity

Cybersecurity is concerned with the protection of computer systems, computer networks and data. Its purpose is to:

- to protect computers and networks from cyberattacks
- to prevent unauthorised access to computers
- to protect computers against damage caused by malicious software
- to prevent data from being stolen
- to protect against the disruption of services running on the computer

Cyber Security Threats

Malware is software that has been purposely developed to damage, disrupt or take control of computer systems.

Social engineering techniques manipulate people into giving away confidential and personal information.

Weak passwords are easy to guess. Passwords that use words are easy to crack using an algorithm that systematically goes through all the words in a dictionary until the word matches the password.

Default passwords Upon registration for an online account, users may be given a default password that they do not change. Often these passwords are sent out unencrypted via email so pose a major security vulnerability.

Removable media such as a USB pen drive can be a vector for transmitting malware.

Unpatched/outdated software Software needs regular updates to fix security vulnerabilities in computer systems. Software that remains unpatched is vulnerable to attack.

Misconfigured access rights Users should only have access to files and data that they need, but sometimes they have access that they should not.

Penetration Testing

Penetration testing is legitimate testing of an organisation's computer system to identify whether there are any vulnerabilities that an attacker could exploit. By identifying vulnerabilities, these can be patched before the system gets attacked.

White box testing testers are given some information about the network, such as network architecture, source code, and IP addresses. This is designed to simulate an attack by a malicious insider.

Black box testing testers are given very little information about the network before the test. This is designed to simulate an outside attack or cyber warfare attack.

Cyber Security Threats - Malware

Computer viruses replicate themselves and can transfer from one computer to another. They are activated by a user often as email attachments and attachment to other files and programs.

Trojan gains access to a computer by pretending to be legitimate software. The trojan allows unauthorised backdoor access to a computer without the user being aware.

Spyware records the activity on your computer such as your keystrokes, thereby logging your passwords for instance and then send the data back over the network to a hacker. Spyware can also be used to control your webcam and microphone.

Adware includes banners and popups that are automatically installed onto a computer. Whilst this does not cause any, adware is undesirable and can slow down the performance of a computer.

Worms spread like viruses but do not require human intervention. They attach themselves to network tools to spread automatically around a network very quickly.

Methods to detect and prevent cyber security threats

Biometric measures such as fingerprints, facial recognition and iris scans are increasingly being used to verify a user's identity for mobile devices. These are more secure than passwords that can be guessed and forgotten. Biometric measures require a user to be present when signing into a system.

Automatic software updates to firewalls, operating systems, antivirus and other security software are needed so that software can be kept up-to-date against new malware and to fix recently discovered vulnerabilities.

CAPTCHA is a test that can distinguish between humans and bots. It uses images that machines cannot interpret but humans can.

Password systems Virtually all accounts require passwords to access. Some secure sites such as online banking require 2 passwords. Banks may also contact you by phone to confirm a large transaction. This is called two-factor authentication. Password systems can force users to have strong passwords that regularly need to be changed.

Using email to confirm a person's identity Often when you register for an online service you need to provide your email address. You are then requested to activate a link sent to you in an email. This is to confirm that the email account is actually active. Helps to ensure that the users are human and not bots.

Anti-virus software scans the computer intermittently to identify whether there is any malware on the computer. The software compares each file against a database of known virus codes. If viruses are found (ie contains code that is in the database) the file is quarantined. That is the file cannot be run without explicit authorisation from the user. New malware are regularly being created and so anti-virus software needs to be updated to identify the new viruses. That is why anti-virus software is regularly updated.

Cyber Security Threats – Social Engineering

Blagging (Pretexting) Fraudsters make up a scenario to con victims into revealing something they would not ordinarily do. They may have found out some personal information about you from social media sites, to pretend they already know you.

How to prevent

- Use biometric measures because these cannot be divulged.
- Ensure you have your privacy settings on any social media to maximum so that fraudsters cannot find information about you such as your date of birth, where you live etc.

Phishing Normally an email or text messaging scam where victims are conned into believing that they are being contacted by their bank for instance and can give sensitive personal details such as bank account passwords.

How to prevent

- Awareness and vigilance. Be particularly aware of unsolicited texts, emails and phone calls. Do not give personal confidential information away. Official organisations such as banks will never ask for this information.
- Apply email filtering to prevent dubious emails getting through.

Pharming Users are redirected to a fraudulent website that they believe to be genuine because it looks like the real site. For instance, you could be directed site that pretends to be an online store that asks you for your credit card information.

How to prevent

- Check the URL in the web address. For secure websites such as banking or e-commerce sites the HTTPS protocol should be used.
- Website filter

Shoulder surfing Fraudsters look over the shoulder of users to see what passwords or pin numbers that are being typed into the device. This can easily occur at computer terminals and at ATMs that are out in the street.

How to prevent

- Be aware of who is around you when typing in your pin into an ATM or into a chip and pin device. Make sure you cover your hands and they are shielded from prying eyes.
- Place computers in locations that makes shoulder surfing difficult