R 73 Cyber Security – Detection and Prevention - Reading

The following methods show ways in which cyber security incidents are prevented.

WARNING: This sheet discusses ways in which computers and networks are misused. It is illegal to use these techniques yourself.

Biometric measures

Biometric measures are any characteristic unique to a person, such as **fingerprints**, the **iris** in the eye, **facial structure** or a person's **voice**. For example, a **facial scanner** at an airport will take a photo and then analyse points on a face to determine if it is the same as the photo in a passport.

One of the most common biometric measures is **fingerprint recognition**, which is increasingly used for mobile phone and tablet computers.

Password systems

One of the most common methods to prevent unauthorised access to a computer system is the use of a **password**. The password is stored (often **encrypted**) in a **database**. The password entered is then compared against this password to see if the user is authorised to use the system.

CAPTCHA

CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart". CAPTCHAs intend to ask questions that are very simple for humans to answer, but very hard for computers to answer. This normally involves reading some text in a distorted image. By making the image hard for computers to recognise, this system prevents computers from automatically being able to attempt to log into systems.

Email confirmation

When a computer wishes to **verify** that an **email address** is correct, it will send an email to that email address with a **hyperlink** inside it. By clicking the link you prove that the email account is active and you have access to it. This prevents fake email addresses from being used.

Automatic software updates

Software and operating systems will use automatic updates to apply the latest fixes to **security vulnerabilities**. By keeping the auto-update turned on you allow the software to download the latest security updates and apply or install them so that the software always has the most **secure** version.

Penetration testing

Organisations will pay companies to try to break into their computer systems, possibly without knowledge of usernames, passwords or other normal methods of access. This allows them to find weak points in their systems and fix them. This process is known as **penetration testing** (**pen testing**).

White-box penetration testing is where a malicious insider is simulated. They will have a username and password which gives basic credentials. In this test, an attempt is made to try and access parts of the system that this user shouldn't have access to. An attempt will also be made to try and increase any of the rights of the user.

Black-box penetration testing simulates a hacking attempt by someone external to the organisation or from a cyber warfare attack, such as a **denial of service** (**DoS**) attack. For this simulation the company doing the penetration testing will not have any username or password to access the system, but they will attempt to gain access by security flaws in software, or by searching for information in rubbish, or by social engineering.