Cyber Security

Keyword	Definition
Pharming	A cyber attack that redirects users to a fake website
Malware	Malicious software used to cause an act of harm
Social engineering	The ability to obtain confidential information by manipulating people for it
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart

Strong Passwords

Minimum length of characters

Include at least one lowercase letter

Include at least one uppercase letter

Include at least one symbol

Change password every month

DON'T USE

Names of family members, friends or pets

Words in a dictionary or place names

Holiday destinations

Computers are vulnerable to:

Malware including viruses

Social engineering

Pharming

Weak and default passwords

Misconfigured access rights

Removable media

Unpatched and/or outdated software

Social engineering techniques

Blagging (pretexting) – using an invented scenario to target someone

Phishing – using email or SMS (text) message to obtain information

Shouldering – observing information as its entered

Confidence tricks

Psychological technique	Example
Fear	An IT manager gets a phone call from their computer support team saying there is a bug in the software that means they could lose all data if it isn't patched
Worry	An email from a family friend says that they are in trouble abroad and need money
Request for help	A receptionist gets a phone call from a company asking for the contact details of their IT manager
Urgency	A webpage says it has blocked a virus and you need to give your details to recover the files

Viruses

Replicate their code in other programs

Infect other computers

Harm the computer by deleting, corrupting or modifying files

Trojan horses

Have a program, game or cracked file which is something the user wants

Have negative program code which causes damage, takes control, or provides access to the computer

Types of Malware

Viruses

Trojan horses

Spyware

Cyber Security

Common Biometric authentication

Fingerprints

Facial recognition

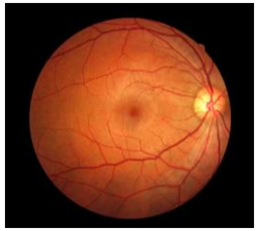
Retinal scans

Less common methods

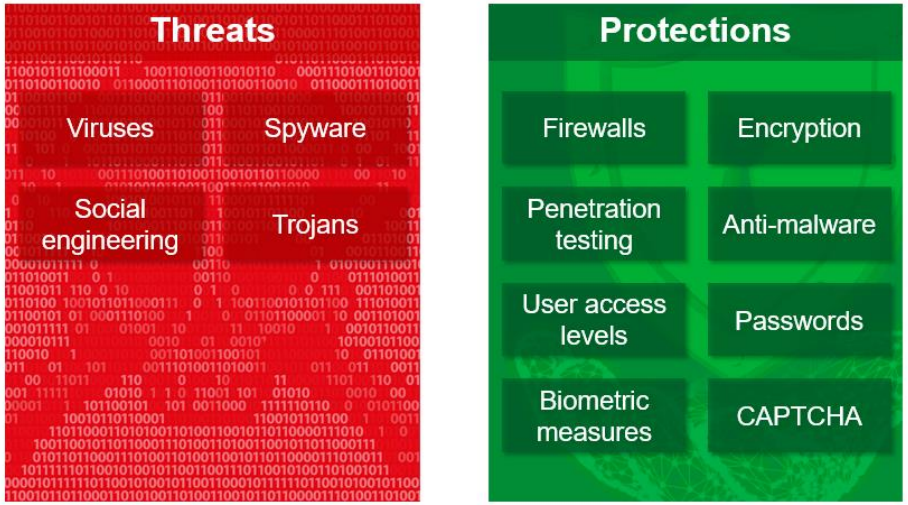
Palm vein recognition

Ear recognition

Voice recognition



Threats and Protection



Threats

- Viruses
- Spyware
- Social engineering
- Trojans

Protections

- Firewalls
- Encryption
- Penetration testing
- Anti-malware
- User access levels
- Passwords
- Biometric measures
- CAPTCHA

Preventing vulnerabilities

Penetration testing

Anti-malware software – including anti-virus software

Biometric measures (especially for mobile devices)

Password systems

CAPTCHA

Email confirmation to confirm identity

Automatic software updates

Network security such as authentication, encryption, firewalls and MAC address filtering

Spyware

Spyware is installed without the users knowledge

It aims to spies on user activities often by:

- Tracking them as they visit websites
- Installing a keylogger that can read passwords and personal information

Personal data is then sent back to the hacker, often through the use of cookies

Penetration Testing

The goal:

Identify the targets of potential attacks

Identify possible entry points

Attempt to break in

Report back the findings

White box:

Simulates a malicious insider with knowledge of the system

Black box:

Simulates an external hacking or cyber warfare attack