

### What is 'cyber security'?

Methods and technologies designed to protect networks, computers and data from attack, damage and unauthorised access.

### Threats

**Weak/default passwords** These are easily guessed or found through brute force decryption.

**Misconfigured access rights** This means that systems/files that should be secure can be accessed by other users.

**Removable media** (e.g. USBs) This can bypass security measures (like firewalls), so malware can be installed more easily.

**Outdated software** Software that has not been patched is vulnerable to attackers.

In addition to this, **malicious code** and **social engineering** techniques also pose threats.

### Cyber Security Threats

Video: [http://youtu.be/mJVAofe5m7s?list=PL04uZ7242\\_M6O\\_6ITD6ncf7EonVHyBeCm](http://youtu.be/mJVAofe5m7s?list=PL04uZ7242_M6O_6ITD6ncf7EonVHyBeCm)

### Methods of Protection

Identity authentication: biometric, passwords, two-step authentication

CAPTCHA (human or robot test)

Anti-Virus software (keep up-to-date)

Updating software and installing patches

### Social Engineering

**Social engineering** The process of manipulating people into undertaking certain actions or disclosing confidential information.

**Blagging or Pretexting** Creating a fictional scenario in order to obtain a user's personal information, then using this information for malicious purposes.

**Phishing** Contacting users (usually through fraudulent emails that mimic a legitimate organisation) to cause users to disclose personal information (e.g. usernames, passwords)

**Pharming** Setting up and guiding users to a bogus website that is visually identical to a legitimate one, allowing the attacker to gain login details.

**Shoulder surfing** Spying on people, usually while they're logging in to accounts or using an ATM, to find sensitive information (e.g. passwords, PINs).

### Phishing and Pharming

Video: <http://youtu.be/pSJnZaHhvGE>

### Penetration Testing

What is **penetration testing**?

Attempting to gain access to resources without knowledge of login details and other normal means of access, in order to test defences.

What is the difference between **black-box** and **white-box** penetration testing?

**White-box** penetration is where the tester already has some knowledge of the target system. This simulates an attack by a malicious insider. **Black-box** is where they have no prior knowledge. This simulates external hacking or cyber warfare.

### Malware

**Malware** Dangerous or intrusive software.

**Virus** Malicious program that duplicates itself once inside a computer or network.

**Trojan** A malicious program disguised as a legitimate one to trick users into installing it.

**Spyware** Software enabling attackers to obtain information about another's computer activities by transmitting data from their hard drive.

**Ad ware** Software that automatically displays advertisements when a user is online, generating revenue for the attacker.

