System security

Malware

“Software written to cause loss of data, encryption of data, fraud and identity theft: virus, worm, trojan, ransomware and spyware.”

System security

Phishing

“Sending emails purporting to be from reputable companies to induce people to reveal personal information.”

Social Engineering

“Most vulnerabilities are caused by humans. Not locking computers. Using insecure passwords. Not following/poor company network policies. Not installing protection software. Not being vigilant with email/files received. Not encrypting sensitive data.”

Brute Force Attacks

“A trial and error method of attempting passwords. Automated software is used to generate a large number of guesses.”

Denial of Service Attacks

“Flooding a server with so much traffic it is unable to process legitimate requests.”

Data Interception

“Stealing computer-based information.”

System security

SQL Injection

“A hacking technique used to view or change data in a database by inserting SQL code instead of data into a text box on a form.”

Network Policies

“Rules put in place on a Local Area Network by a systems administrator. They control aspects such as what certain types of users are allowed to / what they are allowed to access etc.”

Penetration Testing

“Testing designed to check the security and vulnerabilities of a system.”

Network Forensics

“Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection.”

Anti-Malware Software

“Antimalware software protects against infections caused by many types of malware, including viruses, worms, Trojan horses, rootkits, spyware, key loggers, ransomware and adware.”

System security

Firewalls

“A computer application used in a network to prevent external users gaining unauthorised access to a computer system.”

System security

User Access Level

“The amount of access a given user is allowed to a computer. On a network most users will have restricted access. Whereas a systems administer or network technician would be allowed much greater access with fewer restrictions.”

System security

Password

“A secret word or phrase that must be used to gain access to a computer / program / interface / system.”