Cybercrime Help Sheet

Malware

Used to describe malicious software including Spyware, Ransomware, viruses and worms. Malware breaches a network through a vulnerability, usually when a user clicks a link in an e-mail which then installs the software.

Ransomware

Blocks access to key areas of the network and usually there is a demand for payment to obtain the key to unlock access.

Worms

Can modify and delete files on a system and also install further malicious software. Worms can also replicate themselves into different systems or servers and disrupt multiple systems.

Man-in-the-Middle Attack

Also known as eavesdropping attacks, are when a hacker inserts themselves into a two-party transaction and remove data which is shared between the two parties. i.e. using an instant messenger service to listen in to a conversation where bank account details are shared or customer data is discussed.

SQL Injection

A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

Spyware

Covertly obtains information by transmitting data from the hard drive.

Viruses

Disrupts the system and can render it inoperable.

Phishing

Sending fraudulent communications that appear to come from a reputable source usually through an e-mail. The goal is to obtain card information, bank log in details, a funds transfer from the vulnerable victim or install malicious software on to the victim's computer.

Hackers will often have obtained access to your systems and will monitor internal e-mails to ensure the phishing e-mail looks legitimate. It will often be written in the same way as a company official would usually write with similar e-mail signatures. Only when looking closer at the e-mail address can you tell it's not a legitimate company profile.

Denial-of-Service Attacks

This is a flood of network traffic which exhausts the system resources and bandwidth. As a result, the system would be underpowered and not be able to handle any legitimate requests. Ultimately bringing the business to a standstill.

Trojan or Trojan Horse

A trojan is a program which hides in another useful program. Once the program is run the Trojan opens up a back door into the victim's system and allows the hacker uninterrupted access to the system to perform further attacks or data theft.