Key Definitions

Antivirus

- Antivirus is a security software installed on systems to protect, monitor and remove any form of malware. Different antivirus softwares offer different levels of protection.

Cybercriminal

- Cybercriminals are individuals, or teams of people, who commit malicious activities on computer systems or networks. Their intention is often either stealing sensitive organisational, personal information generating profit, or destroying data.

Distributed Denial of Service Attack (DDoS Attack)

- A type of attack where devices are disabled and are no longer functional

Email Attachment

- Email attachments are computer files sent along with email messages. Multiple files can be attached to email messages and be sent along with it to the recipient.

Encryption

- Encryption is the process of converting information or data into code, mainly to prevent unauthorised access.

Malware

- Malware is a blend of malicious software. Malware is designed to disrupt or damage a computer system, or gather information unlawfully.

Phishing

- Phishing is the fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers. When targeting important individuals, the term used is “whaling”.

Ransomware

- Ransomware is a form of malware designed to block access to a computer system until a sum of money is paid by the owner to regain control.

Removable Data Storage Device

- A removable data storage device is any storage device that can be removed from a computer system while it is running. Examples include USB memory sticks and CDs.

Secure Sockets Layer (SSL)

- When a website has a padlock at the start of the web address it has a SSL. It means that the information is only viewable at either end of the link and nobody else can snoop in on the information.

Key Definitions

Shoulder Surfing

- Shoulder surfing is the practice of spying on another person’s device to obtain their personal identification number, password and any other sensitive information that they can see on screen.

Smishing

- Smishing is the use of SMS messages to conduct phishing attacks.

Social Engineering

- The term used to describe when someone is tricked into doing something. Phishing is a form of social engineering, and so are real-life cons..

Social Media

- Social media networks are websites used to share information, ideas and digital media in an online community. Notable examples of social media include Facebook, Twitter and Instagram.

Software

- Software is the general term that describes computer programs, operating systems and applications.

Tether

- To tether is to use a smartphone to connect a computer or other device to the Internet.

Trojan

- A trojan is a malware that gains access to the computer system by appearing to be useful but instead is programmed to complete an insidious task, often stealing confidential information.

Virus

- A virus is a form of malware that causes a detrimental effect to computer systems, such as corruption or destruction of data.

Watering Hole

- A watering hole is a website that has been infected with malware by a cybercriminal, which will automatically download onto your computer.