Computer Science

Year 9 E-Safety Knowledge Organiser

E-safety

E-safety refers to staying safe online, this includes the use of the internet, social media sites and gaming.

Top tips for staying safe online:

1. Do not talk to strangers
2. Do not give out personal information
3. Make sure all social media accounts are set to private.
4. Do not meet anyone online.

Cyberbullying

Cyberbullying is ***"bullying for the 21st century, using email, text messages and the internet."*** (Richard Aedy, *ABC Radio National*)

Flaming

Flaming is the online act of posting insults, often laced with profanity or other offensive language on social networking sites.

Cyber Stalking

Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization.

Masquerading

Masquerading is an elaborate form of cyberbullying where the bully pretends to be someone who they are not. They might create fake email addresses or instant messaging names, or they might use someone else's email or mobile phone to bully someone.

Malware

Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. There are several different types of **malware**.

Viruses

A virus can be defined a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

Worms

A worm can be defined as a self-replicating program able to propagate itself across a network, typically having a detrimental effect.

Trojan Horses

A Trojan horse, or trojan, can be defined, as any malware which misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy.

Spyware

Spyware can be defined as a piece of software that is installed in a computer without the user's knowledge and transmits information about the user's computer activities over the Internet.

10 Malware Protection Tips

1. Keep your operating system up to date. Always use the latest software version available. Out-dated programs often suffer from severe security vulnerabilities, which hackers take advantage of.
2. Install a firewall to ward off threats.
3. Use a virus scanner program to detect and reject possible security threats.
4. Create passwords that are at least 12 characters long. Longer passwords are harder to crack. In fact, the length of the password is more important than the use of special characters.
5. Choose a unique password for each of your digital accounts.
6. Only open emails from trusted senders. If you open a dubious looking email, do not click any links, and delete it straight away.
7. Never pass on personal data such as account or credit card data using email.
8. Use a trusted email provider and always send sensitive data encrypted.
9. Do not use public WLAN routers (unencrypted wireless networks).
10. Only install programs from trustworthy sources.