Computing E-Safety

What is E-Safety?

E-Safety is the process or steps taken to stay safe online. This can include using the internet, social networks, apps, games and beyond.

What is cyberbullying?

Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behaviour.

How to stay in Control

1. Don't put any images online of yourself or friends that you would not want your family or someone else to see

2. Make sure your user settings are set to private so only your real friends can view them

3. Make sure you know who is on your friends list. Someone who you think is a friend may not be a friend at all

4. Report any abuse using the Report Abuse button

Copyright

Copyright is the right of the owner to reproduce or permit someone else to reproduce copyrighted works.

Basically, if you did not write or create the article, graphic, or data that you found, then you need permission from the owner before you can copy it!

Copyright, Designs and Patents Act 1988

When you buy software, for example, copyright law forbids you from:

- giving a copy to a friend
- making a copy and then selling it
- using the software on a *network* (unless the *licence* allows it)

Online Threats & Solutions

Hackers: People who access your computer/files without your permission. They may do this with, or without the intention of editing your files.

Virus: A program designed to copy itself and spread, usually attaching itself to applications. It can be spread by downloading files, exchanging CD/DVDs and USB sticks, copying files from servers, or by opening infected email attachments.

Worms: A worm is malicious software that spreads by itself. A worm tends to send itself to all email addresses it finds on the infected PC. The email then appears to originate from the infected user, who may be on your trusted senders' list, and catch you off guard.

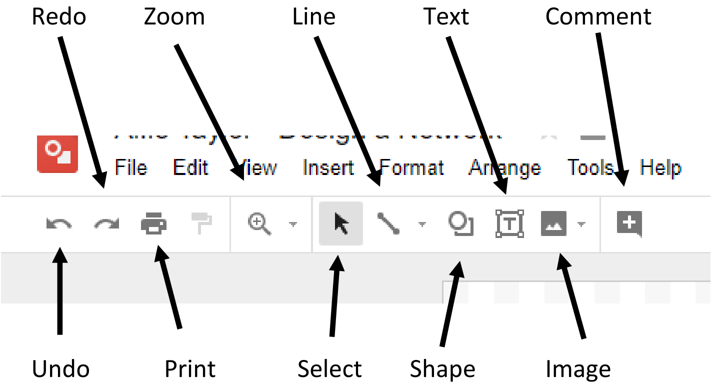
Trojan: Software that appear harmless but has malicious software hidden in it, but it leaves your PC unprotected, enabling hackers to steal sensitive information.

Adware: This malware launches advertisements, mostly in the form of pop-ups. These are customised to you as a user, based on your behaviour on the Internet, which maybe monitored by spyware.

Spam: Spam is unwanted emails. Most users are exposed to scam, which is more than 50% of all Internet emails. Though spam is not a direct threat, it can be used to send different kinds of malware.

Phishing: This is sending official-looking emails impersonating a trustworthy sender and then gathering the recipients personal details.

Antivirus: Software that scans your computer and looks for malicious software. It will either remove the infected files, heal them or quarantine them. You must update your virus definition regularly so that your computer is aware of newer viruses.



FORTI NIHIL DIFFICILE