# SAFEGUARDING SPOTLIGHT

MARCH - DIGITAL SAFETY

CYBER CRIME

Cybercrime is an umbrella term used to describe two closely linked, but distinct ranges of criminal activity.

- Cyber-dependent crimes - crimes that can be committed only through the use of ICT devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity).
- Cyber-enabled crimes - traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).
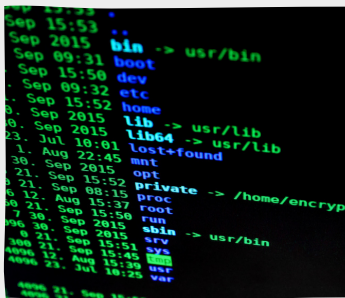
TIPS AND ADVICE

1. Do not give out any personal information.
2. Make sure your computer has up-to-date anti-virus software and a firewall installed.
3. Many frauds start with a phishing email. Remember that banks and financial institutions will not send you an email asking you to click on a link and confirm your bank details. Do not trust such emails, even if they look genuine.
4. Sign-up to Verified by Visa or MasterCard Secure Code whenever you are given the option while shopping online.

THE IMPACT

On individuals:
Financial loss or loss of income
Identity theft
Emotional trauma
Loss of reputation

On businesses:
Financial loss
Damage to reputation
Legal repercussions
Loss of intellectual property

CYBER MISUSE ACT

Computer Misuse Act makes it illegal to acquire access a computer without permission, and make changes to files on a computer without permission.

- Up to two years in prison and a £5,000 fine for gaining unauthorised access to a computer.
- Up to 10 years in prison and an unlimited fine (depending on the severity of the case) if you acquire unauthorised access to a computer to steal data or use the data to commit fraud.
- Up to 10 years in prison and an unlimited fine if you modify the content of a computer or provide the tools so that others can alter the content.
- Up to life imprisonment if the computer misuse puts national security at risk, or causes harm to welfare.

HELPFUL WEBSITES

Action Fraud

Police reporting

internet matters
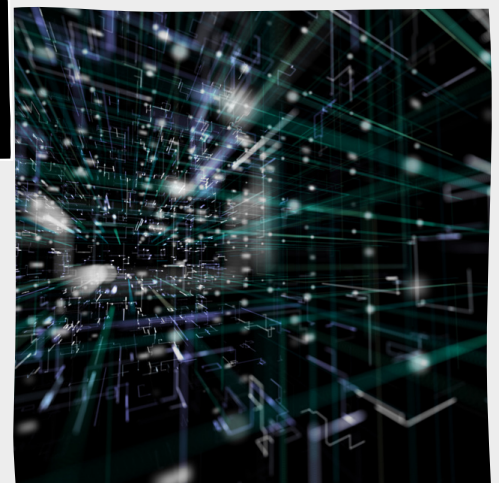
If you have any concerns for your safety, or the safety of others, Want to discuss any issues or want to Seek advice and guidance to keep yourself safe You can speak to your tutor or the safeguarding team in college. Email safeguarding@mbro.ac.uk Text SAFE to 60081 or drop into the wellbeing centre.
To report a non-emergency to police please call 101.
If you, or anyone else, is in immediate danger please call 999.