Stay safe online - Top tips

What causes cyber attacks?

Online criminals
Stealing and selling sensitive data or holding information to ransom.

Hackers
Individuals acting in an untargeted way, to test their own skills or cause disruption.

Honest mistakes
Sometimes people just make a mistake, for example by emailing something sensitive to the wrong email address.

Secure your devices

Smartphones, tablets, laptops or desktop computers can be exploited. You can protect them from most attacks.

Software updates help keep your device secure. If you're prompted to install any, make sure you do.

Always lock your device when you're not using it. Use a PIN, password or fingerprint/face ID. This will make it harder for an attacker if your device is lost or stolen.

Only use app stores like Google Play or the Apple app store. Don't download apps from unknown sources.

Defend against phishing attacks

Phishing messages appear real but are fake. They try and trick you into revealing sensitive information, contain links to malicious websites or infected files.

- Phishers use publicly available information to make their messages look beleiveable. Review your privacy settings and think about what you post.
- Know the techniques that phishers use in messages. This can include urgency or authority cues that pressue you to act.
- Phishers may pretend to be people who would contact you. Make sure you know how to spot unusual activity.
- If you think you've received a phishing email tell Action Fraud immediately. You'll be helping reduce the harm caused.

If in doubt, call it out

Reporting incidents quickly can reduce the harm caused by cyber attacks.

Cyber attacks can be difficult to spot, so don't wait to ask for help when something feels wrong.

Report attacks as soon as possible. Don't assume that someone else will do it. Even if you've done something (such as clicked on a bad link), always report what's happened.

If you think you've been the victim of cyber attack, call Action Fraud (0300 123 2040).

Use strong passwords

Attackers will try common passwords, or use publicly available information to try and access your accounts. If successful, they can try the same password to access your other accounts.

- Create strong and memorable passwords for important accounts, such as using three random words. Avoid using predictable passwords, such as dates and names.
- If you write your passwords down, store them securely away from your device. Never reveal your password to anyone.
- Use two factor authentication for important websites like banking and email, if you're given the option. This provides a way of double checking that you really are who you say you are when loggin on.