RISK SOLUTIONS

Staying Safe Online

Smartphones, computers and the internet have transformed how people communicate, work and access information, **but they can also expose individuals to the perils of cyber-crime.** However, by implementing a few simple cyber-security strategies, you can safeguard your devices and the online services you use from theft or damage.

Stay safe online at home and work with these six tips:

Choose strong passwords.
Criminals may use publicly available information to guess passwords. To create strong passwords, combine letters, numbers and special characters, and don't use personal information (eg date of birth.)

Recognise phishing.
Cyber-criminals may use artificial intelligence tools to craft convincing phishing scams. Remain vigilant and only click links in emails and texts after verifying that the sender is trustworthy.

Use multi-factor authentication.
Enhance security by using multiple access methods when logging into websites and applications (eg a password and facial recognition.)

Update software.
Keep software and applications updated, as providers may release patches necessary to maintain users' safety.

Secure your devices.
Lock your devices when not in use. Set up a PIN, password or fingerprint/face ID to make it harder for criminals to gain access if devices are lost or stolen.

Protect Wi-Fi.
Secure any wireless networks by changing the manufacturer's default password and username and regularly monitoring connected devices.

Report Incidents

If you suspect cyber-crime, promptly reporting your concerns can reduce potential harm. At work, report incidents to your line manager or the IT department. Contact Action Fraud UK or the police for cyber-incidents occurring in your personal life.

Contact us today for additional cyber-security resources.