THE LITTLE LEAFLET OF

CYBER ADVICE

Eastern Region Special Operations Unit

Regional Organised Crime Unit

TIP 1: HAVE A STRONG PASSWORD

Your password is the lock on your door. Make sure it's strong.

Simple passwords can easily be guessed by criminals. Don't use words personal to you (sports teams, pets, family names etc.) and never share it with anyone! Make sure you have a separate password for your email.

sam[illegible]vdog ✗ englan[illegible]1966 ✗ passw[illegible]123 ✗ qw[illegible]ty ✗

fishboattulip ✓

To create a strong password simply join three random words together. Then add numbers, symbols and uppercase letters. For example: 19fisHboaTtuliP95!!

TIP 2: HAVE ANTIVIRUS

Antivirus is your building's security guard. Make sure you have some, and that it's up to date.

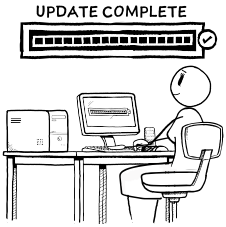
Viruses and malicious software (malware) can infect any device (computers, phones, etc.) Once it's there, it can lock you out, steal your information or even watch you in your home!

Most systems have anti-malware already built in, so make sure you're using it. Also, consider installing extra antivirus on all of your devices (which can be free). These act as a security guard, checking everything that tries to come in. They will alert you if anything tries to infect your system.

TIP 3: ALWAYS UPDATE SOFTWARE

Vulnerabilities are holes in your walls. Updates and patches fill the holes in.

Software is never perfect. It often has vulnerabilities or holes that criminals can use to get inside. When one is found, the software is updated or patched to remove the problem.



Always update or patch your software as soon as you're prompted to ensure that it remains safe and secure.

TIP 4: BACK UP DATA

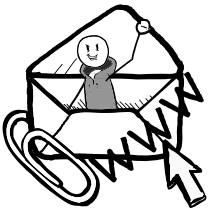
Make copies of things that are important to you. Keep them safe.

Your files, contacts and memories are some of the most important things on your computer. If your computer was to break, or become infected, having a safe backup means you don't lose them.

Regularly copy your important information to multiple external locations (hard drives/thumb drives/cloud etc.)

TIP 5: DON'T CLICK ON LINKS AND ATTACHMENTS

You wouldn't let a stranger into your home. Why let them onto your computer?



Emails you receive may contain attachments or links you are asked to click on. If you do, you're effectively opening your door, bypassing your security guard and inviting them into your home.

Don't click on links unless you can verify where they came from. Call the sender to check it's genuine. If in doubt, keep them out.

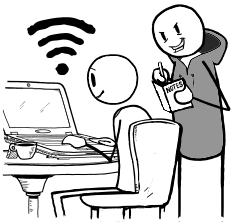
TIP 6: DON'T SHARE EVERYTHING ON SOCIAL MEDIA

You wouldn't take an advert out to say you're going on holiday and your house is empty. Why tell the world via social media?

Social Media is great to keep in touch with friends and family, but unless you've checked your privacy settings, you might be telling more people about your life than you intend.

Be careful who can see what you share online. Ensure your privacy settings on social media are set to a high level.

TIP 7: DON'T USE FREE WI-FI FOR EVERYTHING



Public or free Wi-Fi isn't secure. It's like someone is looking over your shoulder watching everything you do.

If a Wi-Fi network is free or available to the public, then anyone can be on it and watch the traffic between your device and the internet. This means they could steal passwords, banking details or even photos of loved ones.

Never use free Wi-Fi for anything you don't want a stranger to see.

Always report fraud and cyber crime to Action Fraud, either online at **www.actionfraud.police.uk** or by telephone on **0300 123 2040.**

For practical advice on how to protect yourself and your business online visit **www.ncsc.gov.uk**

To contact the ERSOU Cyber Protect team, email **cyberprotect@ersou.pnn.police.uk**