THE LITTLE LEAFLET OF CYBER ADVICE

THE EASTERN CYBER RESILIENCE CENTRE

Eastern Region Special Operations Unit

ROCU

COUNTER TERRORISM POLICING

TIP 1

HAVE STRONG PASSWORDS

Your password is the key to your online life. 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 them with anyone! Always have a different password for your email.

To create a strong password simply join three random words together. You could add uppercase letters, numbers and symbols to make it more secure. You can also store passwords in your browser.

TIP 2

USE ANTIVIRUS

Antivirus is your first line of defence. Make sure you use it, and it's kept up to date.

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

Most systems have antivirus built in, so make sure you're using it. Also, consider installing extra antivirus on all of your devices (this can be free). These check everything coming into your device and will alert you if anything tries to infect your system.

TIP 3

ALWAYS UPDATE SOFTWARE

Vulnerabilities are like holes in your device's systems. Updates and patches fill the holes in.

Software is never perfect. Often it has vulnerabilities or holes that criminals can use to access your systems. When a vulnerability is found, the software developer creates and releases an update or patch to fix the problem.

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

TIP 4

ALWAYS BACK UP DATA

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

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

Regularly copy your important information to external storage like external hard drives, USBs or clouds storage. Keep these separate from the originals. You should also set your phones and tablets to automatically back up your data.

TIP 5

TURN ON TWO-FACTOR AUTHENTICATION (2FA)

Two-factor authentication (2FA) proves you are who you claim to be online.

Passwords can be stolen by cyber criminals. However, accounts that have been set up to use 2FA will require you to input an extra 'factor'. This will be something only you can access like a code sent to you by text, or generated by an app on your device. So even if a criminal knows your password, they won't be able to access your accounts.

Where available turn on 2FA on any accounts that contain important or personal information. Go to www.ncsc.gov.uk/cyberaware for instructions on how to set up 2FA across popular online services.

TIP 6

BE CAUTIOUS USING FREE WI-FI

Public or free Wi-Fi isn't secure. Someone could be monitoring 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 sent between your device and the internet. This means they could steal passwords, emails or even banking details. Also, be careful using apps that automatically login without you having to enter your password.

Be wary using free Wi-Fi for anything you don't want a stranger to see, and consider keeping Wi-Fi turned off unless you need it, or use a VPN.

TIP 7

THINK TWICE BEFORE CLICKING ON LINKS OR ATTACHMENTS

Clicking on unverified links or attachments can give criminals access to your devices.

Emails or texts you receive may contain attachments or links you are asked to click on. If you do, you're bypassing security you have in place. If the message was from a criminal, they can then infect or gain access to your device.

- **Double check before you click on links. Make sure you can verify where they came from. Call the sender to check it's genuine. If in doubt, don't click on it.**

TIP 8

CHECK WHAT YOU'RE SHARING ON SOCIAL MEDIA

Unless you're careful on social media, you could be sharing personal information with the wrong people.

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 aware that once it's online it will be there forever in one form or another.

- **Be careful who can see what you share online, ensure your privacy settings are set to a high level. Never share private information (like your address or school) on social media. Make sure your family follow the same advice.**

TIP 9

ALWAYS QUESTION REQUESTS FOR PERSONAL INFORMATION

Criminals will tell you all sorts of stories to get you to part with your money or your data.

Whether face to face, over the phone or the internet, criminals will lie to pretend to be someone they're not. They could impersonate police officers, the tax office, your bank or anyone who you might trust in order to steal your data, or your money.

- **Never give information to anyone who contacts you out of the blue. Always take time to verify their credentials through a trusted source.**

TIP 10

REPORT ALL FRAUD AND CYBER CRIME TO ACTION FRAUD

It's important all crime is reported, cyber crime is no different.

Even if you didn't lose money, you should still report every instance of fraud or cyber crime you're targeted by. Every report assists police investigations, disrupts criminals, and reduces harm. Reports are also used to identify crime trends and create awareness campaigns to help protect people against them.

- **Report online at www.actionfraud.police.uk or by telephone on 0300 123 2040.**
- **Forward suspicious emails to report@phishing.gov.uk, and suspicious texts to 7726.**

For more information please visit
www.ncsc.gov.uk/cyberaware/home
For our website, please visit
ersou.police.uk
or contact us at
cyberprotectersou@beds.police.uk

Published by the Metropolitan Police Service