Public Guide

Protecting you

against cyber-crime

Contents

This short guide provides an overview of steps that can be taken to help prevent cyber-crime. Links on how to implement the advice in this guide can be found in the help and support section.

Passwords

Creating **strong, separate passwords** and **storing them safely** is an important part of cyber security.

If you use you the same password for all your accounts and this password is leaked in a data breach, all of your accounts are then compromised.

Using separate passwords

Use different passwords for your important accounts.

At the minimum, use a **separate password** for your **email**. If a hacker gets into your email, they may be able to reset passwords for all your other accounts using the “reset password” function

Save your passwords into your browser or use a password manager

Worried about forgetting all the new passwords? Saving them into your browser or a password manager will help with this.

Remember to put a pin or password on your device!

Creating strong passwords

Create passwords using **3 random words.**

Avoid using words that can be guessed (like football teams)

Data breach

You can check if your data has been leaked as part of a data breach by visiting https://haveibeenpwned.com/

If you have, change your passwords to your important accounts

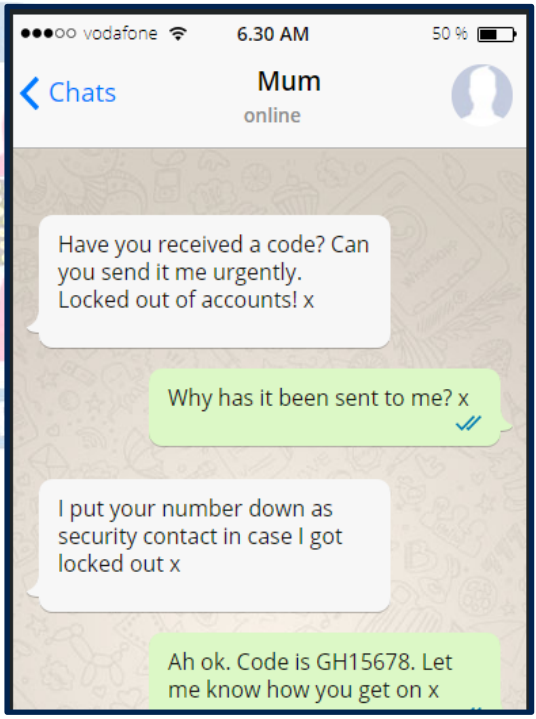
Multi Factor Authentication

Multi factor authentication (MFA) helps to stop hackers getting into your accounts, even if they have your password.

MFA requires users to provide two or more pieces of evidence to verify their identity to gain access to an online platform. This could be a mixture of a password, PIN and biometric data (facial/ fingerprint ID)

Turn on MFA on your important accounts, especially your **email address**

Cyber criminals will try and persuade you to send them your one-time codes to bypass security by posing as a friend or family member. If you ever get a message from a contact asking you to share a one-time code or click on a verification link, it is likely their account has been hacked. Speak to them over the phone or use video calling to let them know.



This message is from a hacked account – Never share one-time codes

Update your devices

Software, apps and operating systems that are out of date contain weaknesses making them easier to hack.

Companies fix weaknesses by releasing updates, which is why it important to update when prompted.

Automatic updates

Most modern phones and computers give you the option to turn on automatic updates, so you do not need to remember to do it.

Getting the best product

Updates are not just important for your cyber security – they also fix any known bugs, add new features and improve existing ones.

Back up your data

Backing up means creating a copy of your information and saving it to another device or cloud storage

Social media accounts

Are all your photographs stored on social media? If your social media accounts get hacked, the police have no powers to recover them. This could mean losing important photographs forever. Backing up your photos ensures that you will still have a copy, even if your account is hacked.

Automatic back ups

You can turn on automatic backups on most smart phones. These regularly save your information in to cloud storage.

External hard drive/ USB stick

If you are using an external hard drive or USB stick, disconnect it from your computer when you are not backing up. If your computer becomes infected, your back ups should be safe.

Phishing

Phishing can be conducted via text messages, social media, phone calls or email.

It is designed to trick the receiver in to doing the “wrong thing” such as revealing passwords, personal information or clicking on malicious links.

Spotting phishing scams

Does it encourage you to click on a link?

Does the email claim to be from someone official, such as a government department?

Does the email contain elements of urgency or veiled threats?

Does it make you panic, feel hopeful or curious?

Is it offering you something in short supply?

Does it contain bad grammar or spelling?

This might be a phishing email. STOP and make further checks.

Check information

Go back to something you can trust to verify information – visit the official website, log in to your account or ring the official number. Do not use the links or information sent to you.

Phishing messages may come from a trusted contact who has had their account hacked. If you are not expecting them to send you any links, phone and speak to them before clicking.

Phishing

If you have clicked on any links or provided any information, follow the advice below

Personal information

If you have revealed personal information and you are concerned that this will be used by criminals, consider registering with a legitimate credit check reference agency that will send you alerts if anyone applies for credit using your details.

Accidentally installed software?

Open anti-virus software and run a scan. If you are unsure how to do this, take it to a reputable PC repair shop for assistance.

Passwords

If you have provided your password change all passwords that are the same or similar.

Bank details

If you have provided bank details, contact your bank immediately and tell them what has happened.

Help and support

Guides on how to implement all the advice in this guide can be found at https://www.ncsc.gov.uk/cyberaware/home

The National Cyber Security Centre is the government website for cyber security. Create free cyber action plans and sign up to weekly updates that will keep you informed regarding the latest cyber threats - **https://www.ncsc.gov.uk/**

If you have been a victim of cyber-crime, report it at Action Fraud. You can sign up to receive alerts regarding the latest scams from Action Fraud at https://www.actionfraud.police.uk/ or call 0300 123 2040

Victim Support offer free, independent and confidential advice to victims of any crime. Visit https://www.victimsupport.org.uk/ or call 0808 16 89 111 if you require support.

Forward any phishing emails to report@phishing.gov.uk and any scam text messages to 7726. More information can be found at https://www.ncsc.gov.uk/collection/phishing-scams