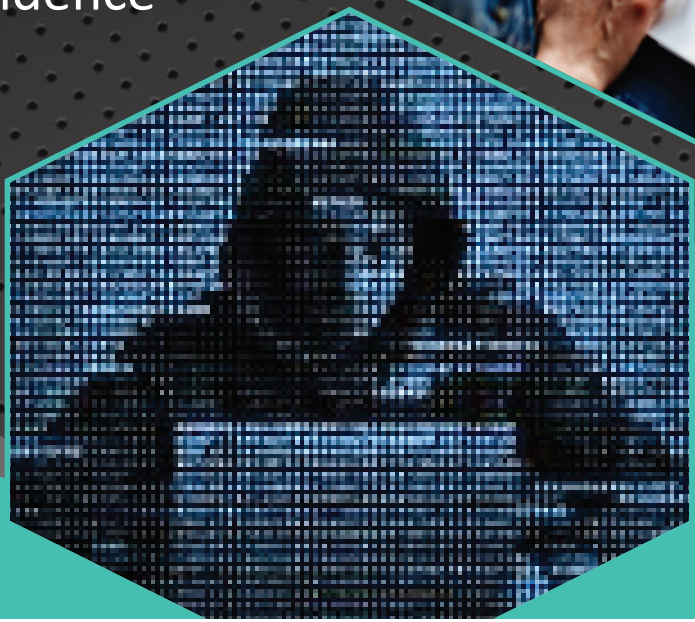
Altogether Better Policing

DURHAM

CYBER SAFETY

A guide to securing your accounts, keeping safe and capturing online evidence



TOP TIPS

PASSWORDS

Use three random words to create a strong memorable password, numbers and symbols can still be used if needed. DON'T use obvious ones like your child's name, fav sports team or pet!

Use a strong, separate password for all your accounts. If you will struggle to remember all these different passwords, use a password manager or when asked to save a password, click save!

2FA

Where available, use two-factor authentication (2FA) to secure your important accounts, such as your email.

DIGITAL FOOTPRINT

Don't over share personal information on social media platforms. Ensure you have your accounts set to private. There are step by step guides on how to secure your social media accounts on **https://www.internetmatters.org/parental-controls/social-media/**

UPDATE

Always install the latest software and app updates. These updates don't have to get in the way of what you're doing. You can choose to install them at night when your device is plugged in or set automatically updates when the device is connected to the internet.

BACK UP

Always back up your most important data! Things to consider:

- Identify what data you need to back up
- Keep your backup separate from your computer
- Consider the cloud

PUBLIC WIFI

Don't use public WIFI to transfer sensitive information such as card details. Where possible use your mobile 4G network, which will have built-in security. You can also use a Virtual private network (VPN) this encrypts your data before it's sent across the internet.

USE STRONG PASSWORDS

To create a strong password simply choose three random words. Numbers and symbols can still be used if needed.

However, using three random words is the key to creating a strong password.

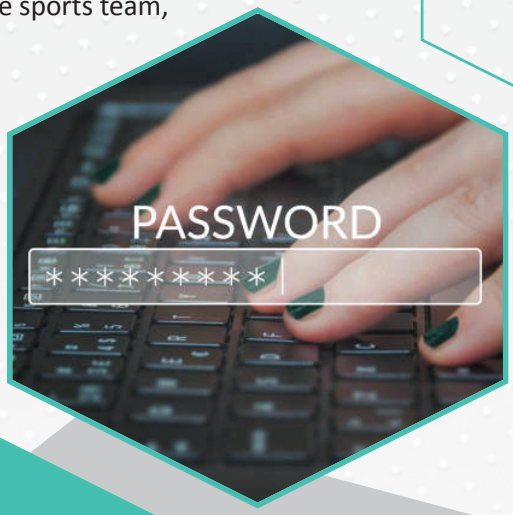
Your most important accounts are your email, social media and online banking. It's important to have strong and separate passwords for each account. With access to your email, individuals can take control of all your online accounts.
Never use any word which is related to you and may be easy to guess.

Examples of these are:

- Current partners name
- Child's name
- Other family members names
- Something related to your favorite sports team, artist or show.
- Pet's name
- Place of birth
- Favorite holiday

and...

NEVER SHARE YOUR PASSWORD WITH ANYONE!



PASSWORD MANAGEMENT

Have a look online for reviews of the best ones, and ensure you purchase a product safely through the apple, google or play stores.

For further advice you may also wish to visit the following websites:

https://www.cyberaware.gov.uk/passwords
https://www.getsafeonline.org/protecting-yourself/passwords/

Saving your password in your browser, is becoming an option with almost all providers. However, we don't advise you using this feature if the device is shared. But whenever you're using your personal device, click YES when the browser asks if you want to save your password.
The password is saved within your browser (e.g., Chrome, edge, safari) not within the website itself.

SET UP 2 FACTOR AUTHENTICATION

Two factor authentication (2FA) is an extra layer of security on your accounts that not only requires your username and password but also something that you have on your person, such as a mobile phone or fingerprint. If someone were to try and gain access to your account, even if they had your usernames and password, they would not be able to get further without having access to your phone and the text code.

- **Something you know:**
This could be a personal identification number (PIN), a password, answers to "secret questions" or a specific keystroke pattern

- **Something you have:**
Typically, a user would have something in their possession, like a credit card, a smartphone, or a small hardware token

- **Something you are:**
This category is a little more advanced, and might include biometric pattern of a fingerprint, an iris scan, or a voice print

YOUR DIGITAL FOOTPRINT

A digital footprint is the data that's left behind whenever you use a digital service. From accessing the internet on your mobile phone, tablet or laptop. Every time you go online or use a digital service, you're leaving a trail of information behind you.

It's not only you who can influence your digital trail. Your friends, family, colleagues, associates and the club and societies you're a member of can also add to it every time they mention you online.

7 things that could be part of your digital footprint.

1. Photos and posts on social media
2. Data collected on fitness trackers and smart watches
3. Games you've played online
4. Things you've bought
5. Information you allow apps to collect or access
6. Voice searches on Alexa or other devices
7. Comments or arguments you've been in

YOUR DIGITAL FOOTPRINT

TIPS TO PROTECT YOUR PRIVACY ONLINE

Change your privacy settings
Lots of social media sites will set your account to public by default. Changing your privacy settings lets you control who can see your posts and whether they'll appear on search engines.

Think before you post
You never know who'll see photos, videos or comments you put online so think about how others might react before you post anything. Even apps like Snapchat can be screenshotted and shared. Never share your address, phone number or the name of your school online.

Delete content you don't want online
Posted something you regret? There are lots of ways to delete things about you online. It can help to close or delete old social media accounts you don't use anymore as well.

Search your name
Typing your name or your username into a search engine can help you find what's easily available about you online. Remember, if you can find it then so can other people.

Check what data your device is collecting
Devices like phones, fitness trackers or wearables can collect data about you without you realising. Every device is different so search online to find out if your data is being used.

Set permissions for apps and websites
Lots of apps will ask for permission to use your data when you install them, including things like your contacts, photos and messages. Be careful about what you agree to and pick apps and browsers that protect your privacy. When you visit sites and you're asked whether you accept cookies, make sure you check what the website says about how they'll use them before you agree.

Share positive parts of your life
Try sharing things you'd be happy with anyone else seeing, things you are proud of. When you post comments to other people, try being supportive and positive.

UPDATE YOUR DEVICES

When a provider releases an update, this is essentially telling the world that there was a vulnerability in the software or app you're using.

Using the latest versions of software, apps and operating systems immediately improves your security.

UPDATE regular or set your phone or tablet to automatically update. Cyber criminals exploit these weaknesses in software and apps to access your personal data. But with automatic updates activated for both software and apps, your provider is keeping you protected.

DON'T Jailbreak or root your Smart phones! Switching off software restrictions leaves your phone vulnerable to malicious software or applications (malware), which can infect your phone and damage or delete date including your valuable photos and videos.

BACK UP YOUR DATA

Backing up your data acts as an insurance policy if you find yourself the victim of a cyber-crime.

If your phone, tablet or laptop is hacked, your sensitive data could be lost, damaged or stolen. Keep a copy of all your important information by backing it up. You can either back up everything or only the information that is important to you.

- The most common time you'll use your back up is if your phone is lost or stolen, or you upgrade to a newer model. However, if your device becomes infected with malware, you could lose access to all your information.
- Important information could be treasured photos, bank statements, mortgage documents or your holiday packing list.

Backing up means that you will always be able to access the information that you care about.

- Identify what data you need to back up
- Keep your back up separate from your computer. Use a USB, a separate drive or a separate computer.
- Consider the cloud.

PUBLIC WIFI

DON'T USE PUBLIC WIFI TO TRANSFER SENSTIVE INFORMATION

Where possible use your mobile 4G mobile network, which will already have built-in security.

Cyber criminals can set up fake WIFI hotspots, enabling them to intercept sensitive information you are transferring online.

You can also use a Virtual private Network (VPN) a technique that encrypts your data before it is sent across the internet.

ANTI-VIRUS

Download Anti-virus software, this is a program that is used to detect, prevent and remove viruses on your computer or mobile devices or that are sent to you in an email, chat message or on a web page.

SOCIAL MEDIA

@Durhamcyber Facebook | Twitter | Instagram

CONTACT US

Cyber.protect@durham.police.uk

ACTION FRAUD CONTACT DETAILS

www.actionfraud.police.uk
24/7 helpline
Telephone: 00 123 2040
Email: report@phishing.gov.uk
Text: 7726

Altogether Better Policing

DURHAM

CYBER SAFETY

D03-22