Keep yourself safe online

A Digital Eagles guide to help you use digital devices and sites safely online

BARCLAYS

1. Always use strong passwords

We use passwords to access our devices, accounts and apps every day, accessing personal and financial information that needs to be kept safe and secure. There are a number of different things to consider when creating a strong password:

- **Length** – the longer your password the harder it'll be to guess
- **Random words** – try using three random words that are easy for you to remember but hard for others to guess, avoid using words that people would associate with you, like the name of your pet
- **Special characters** – adding special characters to a password adds a further level of complexity that makes them more secure
- **Case sensitive** – try mixing up lower and upper case letters in your password.

It's advisable to have a different password for each different account you're accessing, but this can sometimes be tricky depending on how many you have, if you find yourself in this position a password manager could help.

2. Setup two factor authentication (2FA)

Two-factor authentication (sometimes referred to as 2FA) provides your accounts with an extra layer of security and can stop cyber criminals accessing your account – even if they have your password.

You'll be asked to verify a second piece of information after entering your password, this could be digits from a code sent via a text message (SMS), a notification in your app or providing fingerprint or facial recognition.

This type of security means that your account can't be accessed directly from just entering your password, adding another barrier between your personal details and cyber criminals.

3. Don't give away too much online

Don't share information that fraudsters could use to impersonate you or access your accounts. This includes anything that might give away:

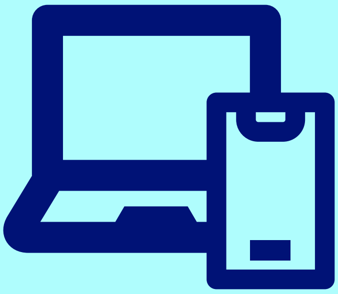
- **Your address** – don't share your address or any photos that could give it away by showing your house number, street name or other unique features
- **Where you are, or where you're going to be** – posting holiday photos, checking in at locations or sharing walking routes can all tell fraudsters when you're not home. This gives them the chance to steal from you or impersonate you – like pretending you're stranded on holiday to trick people into sending them money
- **Information that could be used to reset your passwords** – criminals post games and quizzes designed to get information about you. Never share or enter any details commonly used in security questions or password resets, like your pet's name or the model of your first car.

4. Ensure all devices are secure

All of the devices (smartphones, laptops, tablets, computers) you use to access the internet up and activated. These include PIN entry, fingerprint or facial recognition and passwords to access your device.

This forms the first barrier to anyone other than yourself trying to access your device.

5. Keep your software up to date



The software installed on our devices is constantly being developed and upgraded to work more efficiently, provide a better user experience and improved security features to combat the latest techniques used by illegal hackers.

Software weaknesses can be exploited by illegal hackers so it's important to keep all software, including any internet security software you have installed on your device, up to date with the latest updates (also known as patches).

6. Ensure privacy settings are on

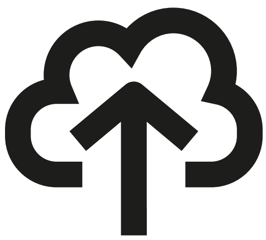
The web browsers you use to access the internet have privacy settings that you can change to keep your browsing activity private, this can also be said about many of the websites you may visit, e.g. social media sites.

7. Take care with downloads

There's an incredible amount of content available to view and download on the internet but it's important to take care over what you download, and where you download it from. It's advisable to only download content from reputable and trusted websites to reduce the risk of you downloading content embedded with malicious software.

Make sure anything you download is scanned by an up to date anti-malware scanner because don't forget, the primary objective of some cybercriminals is to get you to download and install malware so they can cause harm to your device or try and steal your personal information.

8. Back up your personal data



It's a good idea to back up your personal and valuable data you have stored on your devices to an external source such as an external hard drive or cloud storage service. This creates a copy that can be accessed easily if you become the victim of a malicious attack.

How can you protect yourself against fraud and scams

If you receive a request to provide personal or financial information whether that's over the phone, in an email, online or through social media always remember:

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment. Stop and think. It could protect you and your money.

Stop: Taking a moment to stop and think before parting with your money or information could keep you safe.

Challenge: Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

Protect: Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud. On **0300 123 2040** or via **actionfraud.police.uk**.

Always remember

1. Only provide organisations that you trust and have given consent to with your personal or financial details.
2. Question uninvited approaches and contact companies directly using a known email or phone number to verify requests.
3. Just because someone knows your basic details doesn't mean they're genuine.
4. Never disclose your PIN or let anyone persuade you to hand over your bank card,financial information or withdraw cash.
5. One-Time Passcodes (OTPs) should be treated in the same way as your PIN in that they should never be shared with anyone. (We may send you an OTP or ask for 2 random digits from your telephone banking passcode when you contact us, but Barclays will never call you and ask for these details). Before entering your passcode make sure it accurately describes the transaction/purchase you're about to make.
6. Be suspicious of any "too good to be true" offers or prices – if it's at a rock bottom price ask yourself why.
7. Avoid clicking on any links or attachments in social media posts, emails or texts.
8. Request copies of your personal credit report from a credit reference agency on a regular basis to check for any entries you don't recognise.
9. Cancel any lost or stolen credit or debit cards immediately.
10. Keep your personal information secure when using your card over the phone, on the internet, or in shops by ensuring that others can't overhear you or see your information.