THE MONEY HUB

Protecting yourself against fraud

There are a lot of ways that you can protect yourself from becoming an easy target for these criminals. Here are the main ways to ensure your online and your offline self is as safe as possible.

POST AND IMPORTANT DOCUMENTS

- When you move house, remember to change your address or cancel any mail that you no longer want to receive
- Dispose of your important documents with things like account numbers and access codes on by shredding them.

SOCIAL MEDIA

- Review your social media privacy settings. This is where you can see who can access your data and posts. Remove addresses, phone numbers and other personal details from Facebook that don't need to be on there
- Don't share private information publicly on social media such as your address and date of birth
- Be wary of the personal information that you share online such as pet's names or favourite places as these are commonly used for passwords and people can easily work these out.

STRONG PASSWORDS

- Remember that three random words can make the strongest password. GreenPhoneLeopard or CactusPizzaStamp are random combinations that we've created from simply looking around our desks. Think out of the box - the more random, the better!
- Don't keep all of your passwords the same, if you're worried about forgetting them all, use a Password Manager such as LastPass.
- Set up two factor authentication for your email if this is available with your provider. This means that you will need two factors to get logged in which will be something that you have such as a mobile where your email provider will send a code and you may also need something you know such as a PIN or a password.
- Remember to have a passcode on tablets, laptops and phones and don't leave them unattended if they are unlocked. This has to be as random as your other passwords so don't leave it as 1234 or your date of birth if this is something that people are likely to know.

CHECK WEBSITE SAFETY

To check whether a website is safe to visit and there will be no risk to your details or identity you can check the site's security information.

Some internet search engines like Google Chrome will let you know if a page is secure by showing you a padlock for a secure site, an i within a circle for something that is 'Not secure' and an exclamation mark in a red triangle if it is 'Not secure' or 'Dangerous'.

A security certificate can be seen when a website's server uses a certificate provider to prove its identity to the browser. HTTPS is a secure connection.

Other things that you can do to ensure a site is safe for you to use are double checking the web address as fraudsters can use similar names to common sites in order to scam people. For example, our website is https://www.bbc.co.uk but it could be easy to read https://www.bbbc.co.uk correctly if you are skimming or reading quickly. Also make sure that you watch out for other tell-tale signs of a fake website like pixelated images or spelling mistakes.

PROTECT YOUR DEVICES

Protecting your devices such as smartphones, laptops and tablets is just as important as making sure that you don't leave important documents lying around. Here are five ways that you can protect your data, information and identity through your phone or device.

1. Make sure that it's locked at all times that you're not using it. Most phones auto-lock if you have left them for a certain amount of time but try to get into the habit of physically locking it yourself when you are finished. When your phone is locked, people cannot access data or apps that are stored on it
2. Keep it up to date. It might be annoying updating apps and your phone's operating system every few weeks but they often make these changes to update security settings so you'll be doing yourself a favour to update these things
3. Avoid insecure brands. Brands such as Apple iPhones and Google Pixel phones continue to receive updates when they are a few years old which make them fairly secure.
4. Encryption is key to protecting your phone if you lose it or it is stolen.
5. Be wary of viruses and malware when it comes to downloading things onto your laptop. Be careful to not download something that is not from a mainstream vendor such as the iTunes store or the Google Play Store. Plus, scan your laptop periodically for viruses.

WIFI HOTSPOTS

Logging onto the internet from almost anywhere has to be one of the most convenient things that we are able to do in this day and age. But, it can be a hotbed for insecurity and therefore you could be opening yourself up to become a target for online criminals. Public WiFi hotspots are not as secure as your home network because you don't know who has set them up or who else is also connected to the same hotspot as you. Here are some good tips for using public WiFi hotspots in the most secure way.

1. Stick to well-known networks such as The Cloud or your favourite chain of coffee shop or department store. No public WiFi spot is completely secure but using a well-known brand's connection rather than a random free connection that you've never heard of before is safer
2. Don't use the public WiFi for sensitive information and things like online banking
3. Use HTTPS. This means that other people using the same network as you won't be able to see what you're browsing or doing on the internet
4. Don't sign up to public WiFI hotspots if they are asking for too much information such as your name, age and address. If you have to give someone your email address to log into their WiFi, make sure it's a shop, cafe or restaurant that you trust
5. Switch off AirDrop and Bluetooth. This is cutting off what is called 'frictionless file sharing' and it means that no-one nearby can grab any of your files or send you something that you don't want to receive
6. Check terms and conditions of WiFi, even if it's from a brand that you know. Chances are they will be asking for your email address to send you some marketing, but it's best to check the terms and conditions
7. Use a VPN. This is a Virtual Private Network and by installing one of these onto your device the data travelling to and from your laptop or tablet will automatically be encrypted. Using a VPN, you'll be linked to a secure server and it'll be harder for people to get access to your details. Make sure your VPN is a legitimate one, paying for one could be your best bet as the free ones may be financed by marketing companies for data collection.

If you have a large data allowance on your mobile phone contract it could be best to use this for your out-of-home surfing.

FREE SERVICES

There's a saying that nothing in life is free and this is sometimes true in the world of web applications and digital services. When signing up for 'free' services such as Dropbox to store files and photographs it is always worth taking the time to understand the true cost of the 'free' service. Check what rights you have, or are giving up over any data you share or upload to the platform.

CHECK IT'S REALLY US

If you receive a call that you're unsure about and they say they're calling from the Nottingham Building Society, call 0344 481 4444 and speak to someone from our customer service team who will be more than happy to identify if it was us calling you or not.

The Nottingham

thenottingham.com

At The Nottingham we have a number of measures in place to keep your money safe.
You can also help us to protect you – visit https://www.thenottingham.com/the-hub/scams-and-security/ to find out more.

LIT3442/0820