

How to stay safe online



EQUIFAX®

Welcome to The Equifax Online Safety Guide

Being able to store and transfer information online, as well as carry out financial transactions, has made life more convenient for millions of people. But with these opportunities comes the potential for dangers like fraud and invasion of privacy.

Using a smartphone, PC, tablet or even smart devices like fridges and thermostats can leave security gaps that are exploited by fraudsters. Social media is another avenue for those looking to gather data about an individual. Children can be particularly vulnerable, because even if they are familiar with new technology, they may not be aware of the best ways to avoid scams and tricks.

This shouldn't put anyone off using online services, though, as it's possible to stay safe as long as you take the right precautions. In our guide to online safety, we cover a range of topics you should know about, as well as tips on how to best avoid becoming a victim of fraud.

Contents

1. Protecting your financial information	P4
- Different types of fraud	P5
- Tips on staying safe	P6
- Password management	P7
- How to report fraud	P8
- Data security health checklist	P9
2. Social media privacy	P10
- What information to avoid sharing	P11
- How to make sure your privacy settings are appropriate - network by network	P12
- Messaging apps - which are encrypted or safe to use	P14
- What to do about phishing/trolling/having your account hacked	P15
- Social media privacy cheat sheet	P16
3. Parents - keeping kids safe online	P17
- Potential threats to watch out for	P18
- Tips on how to supervise kids without snooping	P19
- Using parental controls and restrictions, including finances	P20
- Official laws and rules on how children can access websites	P21
- Family ground rules	P22
4. Mobile device safety	P23
- Things to look out for	P24
- How to use public Wi-Fi safely	P25
- Checking GPS/location tracking settings	P26
- Managing software to stay safe	P27
- Step by step chart on how to secure devices	P28
5. Useful links	P29

Protecting your financial information



Different types of fraud

There are different ways fraudsters go about trying to get hold of personal and financial information and different crimes they commit once they have it. We look at some of the most common techniques and types of fraud.



Phishing/Email fraud

Phishing is when someone poses as a legitimate individual or organization to try and extract personal information. This could be done by email, text message or even over the phone. Victims may unknowingly give out information, such as a password, account number or PIN code, to someone posing as their bank or other service provider.



Identity theft and fraud

Identity theft is when someone uses methods like the ones on this page to steal personal information. Once a fraudster has got enough information – name, address, account details, passwords, and so on – they can commit identity fraud. This is when they use the information to take control of new or existing financial products, for example, for loans and credit cards or buying a new car on credit.



Browser hijacking and malware

Some hackers will use software to steal your information or to trick you into entering details into a fake site. This may be done by hijacking your browser and redirecting to fake versions of real websites that ask you to enter personal details. Malware can track the information you enter into various websites.



Facility takeover

Taking over an existing account could be as simple as phishing for – or resetting – a password and then using an email address to log in. It could also mean cloning a credit card and then getting hold of the PIN code. Once a facility has been taken over, it may take a while for the fraud to be discovered. If cards are stopped or credit limits are reached, this could mean that the true owner of the account then has limited access to funds until the fraud can be cleared up.

Tips on staying safe



Passwords and PIN codes

There's more information about choosing and looking after your passwords on the next page, but the key things are to pick one that's not easy to guess, not to share it with anyone and not to keep it written down.



Software updates

Keeping your devices up to date with the latest security patches and updates will help make it more difficult for hackers to exploit any gaps in security. You should also make sure you use strong anti-virus software that can spot any unsafe websites or downloads.



Secured websites

When you're online, be aware of unsecured websites that start with http rather than https, or websites that your browser flags as potential risks. Secured websites will usually have a padlock or green tick in the browser bar, meaning that your information is encrypted and secure from hackers.



Communications

Make sure you check any emails carefully, as fraudulent communications can look very convincing. Tell-tale signs include misspellings and links that don't go to the official website domain name. Be wary of requests for personal information to be shared via email, especially when they claim to be 'urgent'.



Research

Before you make a purchase or other transaction online, check if the website is reputable. You can look at reviews on third-party websites, check if the website has a security certificate or look around the website for any industry certification.



Financial statements

Sometimes fraud can happen without you even realising it, so it's important to check your bank and credit card statements regularly for any unusual transactions. It can also be useful to check your credit report for any loans or defaults that you don't recognise.

Managing your passwords

Passwords are an essential part of online life, but with so many different accounts and logins it can be hard to keep track. It's also important to make sure passwords are hard to guess, which can make them hard to remember. Here are a few tips on picking a strong password and the dos and don'ts of how to store it.



Length

There's no perfect length for a password, but the longer and more complicated it is, the harder it will be to guess. Most sites will have a minimum length, but aim for at least eight to ten characters.



Special characters

Adding characters other than letters, like numbers or symbols, makes a password more complicated and harder to crack. Adding random numbers or replacing letters with symbols are both good options.



Randomness

Avoid choosing passwords that include obvious words like the name of your street, pet or place of work. These can be researched and are easier to figure out than random words and numbers.




Variety

Don't use the same password for every account. If a company is hacked and its data is exposed, fraudsters can use that one password to access all of your accounts.



Sharing passwords

Never tell anyone your password and be wary of people asking you to share it online. Try and avoid writing your password down, as this could easily be found or spotted by someone else.



Password managers

You can use online password managers to keep track of all your passwords, using one master password to access it. Make sure to only use reputable software by researching beforehand.

What to do if you're a victim of fraud

If you believe you've been the victim of identity theft or fraud, it's important to contact any financial providers you have accounts with, as well as informing the police. Take the following steps:

1

Alert your bank

Contact the fraud team at your bank to let them know the details of what has happened. They can check your account activity and issue replacement debit or credit cards.

2

Alert your lenders

If you have a credit card or other loan facility that might have been compromised, let the lender know so they can stop any activity and verify real transactions.

3

Change passwords

If you think fraudsters may have access to your email or financial accounts, change the password and make sure you have 2-step verification enabled.

***4

4

Check statements

Check all of your recent statements for any transactions you don't recognise. Also, check your credit report for any loans or information that is not accurate.

5

Contact Action Fraud

Call Action Fraud on 0300 123 2040 or visit their website <http://www.actionfraud.police.uk> to report the details of the fraud.

Data security checklist

Use the list below to make sure you're doing everything possible to secure your data.

Personal Data

- ☐ Shred any financial documents that you don't need to keep
- ☐ Close down old accounts that you no longer use
- ☐ Check that email and postal addresses are up-to-date on all your accounts
- ☐ Switch to paperless documents where possible
- ☐ Review your credit report for unusual activity



Passwords

- ☐ Make your most important passwords longer and more complex
- ☐ Research password managers and use if appropriate
- ☐ Change any easy-to-guess passwords
- ☐ Add a password, code or fingerprint scan to your smartphone
- ☐ Delete or password-protect key documents saved on your computer
- ☐ Change default passwords and codes on smart gadgets



Software

- ☐ Turn on 2-Step verification for your main email account
- ☐ Install anti-virus software across your devices
- ☐ Adjust your privacy settings on social media
- ☐ Update your web browsers to the latest versions



Social media privacy



What to avoid sharing on social media

Social media sites like Facebook, Twitter and LinkedIn can be fantastic platforms for keeping in touch with family, friends and colleagues. However, by their very nature these networks are open and visible to people we may not even know. This might be a good way to discover new contacts, but it's also a great opportunity for fraudsters to spy on you and gather personal data.

Information shared on social media can be combined with other exposed data to commit identity fraud. Beware of sharing the following types of information.



Address

You'll often need to enter a cardholder address when making a purchase, so avoid sharing your full address on open networks. Share via direct message if absolutely necessary.



Birthday

Your date of birth is a crucial piece of information for proving your identity. Try to avoid sharing the full date e.g. day, month and year. Limit to friends and family only.



Card numbers

It seems obvious, but make sure not to share your card numbers or pictures of your credit cards on social media. Even partial information could be useful to a fraudster.



Service providers

Mentioning what bank or credit card provider you use could be useful to someone looking to 'phish' for information, i.e. they'll know what bank to pose as when trying to obtain your secure data.



Location

Geo-tagging on social media could reveal places you visit regularly, such as your house, bank or office. It could also reveal when you're away on holiday, leaving behind an empty house.



Secure answers

Your mum's maiden name, first pet, favourite colour. These can all seem like trivial pieces of information, but they could be the answer to the security question that lets someone into your accounts.

Picking the right privacy settings

Each social network has its own privacy settings, which you'll need to customise to prevent people from seeing your updates. The information below was correct at the time this guide was published, but settings might have been changed or updated since, so be sure to check.



Facebook

You can make the changes below by going to Settings and selecting either the 'Privacy' or 'Timeline and tagging' sections.

Changing who can see your posts

You can make your posts available to anyone, just to friends or to a custom list. You can also restrict who can see your list of friends.

Changing who can add you as a friend

You can always reject friend requests, but to stop strangers from trying to add you, you can restrict friend requests to 'Friends of friends' in the 'Who can contact me' section.

Changing who can see your timeline

Even if only your friends can see your posts, if someone else posts on your timeline it might be visible to everyone. You change this in the 'Who can see things on my timeline' section.



Twitter

You can make these changes by going to the 'Privacy and safety' or 'Blocked accounts' section of your settings page.

Changing who can see your tweets

Ticking the 'Protect my tweets' box will stop people from following you and seeing your tweets unless you have accepted their request.

Blocking specific users

You can block specific users from seeing your tweets from the drop-down arrow on one of their tweets or from their profile page. You can review blocked accounts in the 'Blocked accounts' section of your settings page.

Picking the right privacy settings (continued)



LinkedIn

You can make the changes below by going to settings and selecting the 'Privacy' section.

Changing who can see your full name

You can stop people who aren't already connections from seeing your surname in the 'Who can see your last name' section. They will then only be shown your first name and first initial of your surname.

Changing who can view your list of connections

In the 'Who can see your connections' section you can restrict other LinkedIn members from seeing your full connections list.

Changing who can see your updates

In the 'Blocking and hiding' section you can choose to hide your public updates from everyone on LinkedIn. This means only your connections will see them.

Changing what someone sees when you view their profile

When you view someone else's profile on LinkedIn, they get a notification with your details. In 'Profile viewing options' you can show all your details or your company name, or remain anonymous.



Instagram

Changing who can see your pictures.

In the Instagram app, look for the 'Options' menu on your profile. In here you'll find an option to make your account private. This means that only approved followers can see your photos and videos.

Blocking specific users

If you don't want to make your entire account private, you can block specific users by going to their profile, tapping the drop-down menu and hitting 'block'. You can review blocked users in the main 'Options' menu.



Messaging apps – are they secure?

Most messaging apps, like Skype, Slack and Google Hangouts will be secured with 'encryption'. This means no-one should be able to read your messages unless they have access to your password or device.

Some apps go even further and offer 'end-to-end encryption', making it impossible for anyone, even government agencies, to read your messages.

What is end-to-end encryption?

It's when messages are [secured with a kind of 'digital lock'](#) that can only be opened by the sender and recipient of the message. Even the owners of the app cannot read the messages being sent, making them incredibly secure.

How do I enable end-to-end encryption?

A number of apps automatically encrypt your messages in this way, including [WhatsApp](#), [Viber](#) and [Signal](#). Apple's iMessage and FaceTime apps also use [end-to-end encryption](#). On Facebook Messenger you can activate what they call 'Secret conversations' in your account settings.

Are my messages stored in the cloud?

Message histories on your smartphone might be backed up remotely in the cloud. You should check individual apps to see if this is set up. Data exposure incidents in the past have led to cloud-stored [data being leaked](#).

How do I protect my messages?

Make sure you use secure apps, like the ones mentioned above, with encryption enabled. Use secure passwords, fingerprints and 2-step verification on your smartphone and other devices. If you have shared sensitive information, you can delete specific messages from your phone, though of course they will still be on the device of anyone you've sent them to.

What information should I avoid sharing?

Even with tight security, it's still not a good idea to share things like passwords, PIN codes, account numbers and other valuable data on messaging apps. Even if your own device is secure, you can't always rely on the person you are messaging to be as thorough.

What to do if you're harassed on social media

People may try to take advantage of your presence on social media in different ways, either for financial or personal gain. These include phishing, account takeovers, impersonation and 'trolling' – meaning abusive behaviour or harassment.

If you encounter any of these on social media, take the following steps:

1.

Block and report

Block the individual involved from following your account or being able to contact you. Report them to the social network, who can investigate further and take stronger steps.

2.

Review privacy settings

Review your privacy settings using the steps on pages 11 and 12. Hackers or trolls may use new accounts to continue their efforts and evade being blocked. Limit access to your information, even if just in the short term.

3.

Contact the authorities

In the case of phishing – Let both the social network and Action Fraud know about what has happened. If you handed over information to the fraudsters, follow the steps on page 8 about what to do if you're a victim of fraud.

In the case of harassment – If the abuse is severe and persistent or you are a victim of hate speech, you should report it to the police - <https://www.gov.uk/report-stalker>

In the case of impersonation – If someone sets up an account in your name, either to phish your friends and relatives or just to harass you, get in touch with the social network to report it.

In the case of account takeover – If someone else gains access to your account, you should attempt to change your password. If this doesn't work, contact the social network to let them know about the problem. If you've used the same password for other accounts, you should also change those.

Social media privacy cheat sheet

	Type	Information that might be open	Security tip
 Facebook	Network	Name, birthday, workplace, pictures, interests	Limit profile to friends, or friends of friends
 Twitter	Open	Birthday, location	Make your feed private if you want to share personal info
 LinkedIn	Network	Name, birthday, workplace, professional connections	Hide your updates from non-connected members
 Instagram	Open	Pictures, location	Avoid location-tagging all of your photos
 WhatsApp	Messaging	None	Add a PIN code to make registration more secure
 Snapchat	Messaging	Pictures	Turn on 'Secret Conversations' for extra protection

Keeping kids safe online



Potential threats to kids online

Kids in the UK are spending more and more time online. A 2016 survey showed that even 3 to 4 years olds spend, on average, over an hour a day online. Many of the threats children face are similar to the ones adults face, but kids might be even less prepared for how to deal with those dangers. Here are some to keep an eye on.



Bullying

Cyberbullying can involve verbal abuse, threats or the sharing of private or embarrassing information on social media.

Predators

The anonymity of the internet can increase the chances of online grooming, which can lead to violent or abusive encounters offline.

Inappropriate content

The openness of the internet makes it much harder to restrict which content is seen by youngsters, whether it's video, images or difficult concepts.

Privacy

Sharing names, pictures, addresses and other personal information may seem more innocent to children, making them easier targets for phishing.

Unauthorised spending

Apps and software that have a credit card or other payment account attached can allow spending without the approval of the account holder.

Supervising kids online

It can be hard to find a balance between monitoring what your kids are up to online and giving them the freedom to use it when they want to, especially as they get older. Here are some tips on how to encourage them to share without having to snoop.

1

Use devices in shared areas

Encourage kids to do their homework and use their devices in communal spaces like the kitchen or living room.

2

Research new websites and social networks

Learn about new apps and social networks so you have a better understanding of what your kids might be seeing or sharing.

3

Set up a Wi-Fi password

Give yourself control over access to the internet at home by setting a password on your Wi-Fi router (this is an important security tip, kids or not).

4

Use shared accounts

Use shared accounts for sites like Netflix or YouTube to see recently viewed shows (this will also mean that your kids can see what you watch).

6

Set up payment alerts

Get app alerts when your PayPal, credit card or bank account is used, to spot any unauthorised spending quickly.

5

Talk to other parents

Share information with other parents or friends in case there are any signs your kids or their friends might be having trouble online.

Using parental controls and restrictions

Using the right settings on your kids' devices can make life a lot easier. Here's a list of different technologies that give you control over what can be accessed.

Technology	Examples	What you can do
Computer	PC or Laptop	Microsoft allows you to set controls on your online account. On a Mac you can do this through system preferences. You can also restrict what software is installed.
Web browser	Chrome, Firefox, Safari	Browser settings let you filter certain content. You can also install add-ons, which give you greater control over restrictions.
Smartphone/tablets	Samsung Galaxy, iPhone, iPad	Samsung has a ' kids mode ' app for younger children. Apple allows you to restrict adult content in its general settings. You can also download free or paid apps that can filter content.
Video streaming	Netflix, iPlayer, YouTube	Set a PIN code which is required when trying to watch age-restricted content. YouTube allows you to turn on ' restricted mode ' and there is also a YouTube Kids app.
App stores	Google Play, iTunes	In the Google and Apple app stores, you can set a PIN code which is required to access age-restricted games, films and music with explicit content. It can also restrict purchases.
Internet Service Providers (ISPs)	Virgin Media, BT, Sky, TalkTalk, Plusnet	Many ISPs have services that automatically filter adult content or allow you to whitelist safe websites.
Search engines	Google, Bing, Yahoo	Google, Bing and Yahoo all have a SafeSearch filter , which can be turned on in their preferences.
Game consoles	Xbox, PlayStation, Nintendo Switch	The most popular consoles all have parental control settings that restrict what content can be seen and purchased. They also allow you to limit how long the console is used each day.

What age restrictions exist online?

Most online activity is governed by the same rules that apply to offline life, such as age restrictions for buying alcohol, weapons or cigarettes. It can be very difficult to verify how old someone is online, which is why children may be able to access things that are inappropriate for their age. Below is some guidance on what restrictions exist for different types of digital content.



Social media networks

The vast majority of social media networks require you to be at least [13 years](#) old before you can join. This includes Facebook, Twitter, Snapchat and Instagram. This is because these sites are complying with the American Children's Online Privacy Protection Act (COPPA), and also apply it in the UK. Age limits vary on other sites, for example, [LinkedIn requires](#) you to be 16 and YouTube is only open to under-18s with parental consent.

18

PEGI and BBFC

The Pan European Game Information (PEGI) system is a European age rating system for computer games. It includes 3, 7, 12, 16 and 18 age categories. The British Board of Film Classification (BBFC) classifies films as 12, 15 and 18 when on sale in digital formats. However, whereas a retailer could be prosecuted for selling a physical copy of a film or game to someone underage, this is very unlikely with digital copies.



Access to services

Some websites stipulate that users be over the age of 18 before their services can be used, [including eBay](#) and the property [rental site Airbnb](#), among others. Dating websites also require users to be 18 or sometimes older. This information may not be obvious at first, so it's important to check terms and conditions for any specific age requirements.



Alcohol websites

Many alcohol-related websites will ask you to enter your age before you can browse the site. This is [done voluntarily](#) and there is no actual law stating you have to be 18 to browse their website. You will need to be 18 to buy any products.

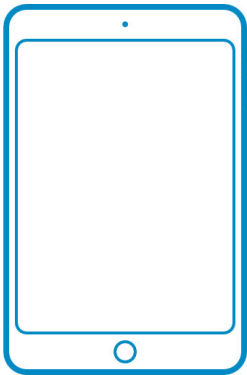
Platform by platform protection



Set a stronger router password for the home wifi



Install parental controls in browsers



Limit purchases in app stores with PIN code or fingerprint



Set social media accounts to private to limit who can follow

Mobile device safety



Mobile device dangers

There are some unique threats that can be attached to using a mobile device, some of which can make it easier for fraudsters to gather information that is useful for identity theft. Here are some dangers to keep an eye out for.



GPS tracking

Many apps use location tracking via GPS to give you useful information about where you are. They might also share your location on social media. This can be handy, but if it's turned on without your knowledge, it could also allow people to track places like your home, school or place of work.



Data privacy

Some services may automatically back up your data to the cloud or track your online activity. It's important to be aware of app or phone settings that allow this to happen. It's also possible, in extreme circumstances, for hackers to remotely activate your microphone and camera.



Loss and theft

Phones and other mobile devices can easily be lost or stolen. Along with losing the value of the phone itself, there is a wealth of information – photos, files, emails, messages – that could end up in the hands of fraudsters, if a device isn't properly secured.



Outdated software

The technology behind mobile devices evolves quickly, so if you have an older device it may not support the latest software updates. This can make you vulnerable to malware or security exploits protected by the latest versions of your favourite apps.



Bluetooth

Bluetooth is a way of wirelessly connecting two devices that are near each other. There are ways for hackers to use this connection to gain access to information on someone else's phone. **This is sometimes called 'Bluesnarfing'.**



Unsecured Wi-Fi

Using Wi-Fi in public places is a convenient way of getting fast internet speeds, while not using up your mobile data. However, public Wi-Fi may be less secure than the connections you use at home or at work, making it easier for fraudsters to intercept information.

How to use public Wi-Fi safely

Wi-Fi hotspots can be very useful, but it's also harder to know how secure they are. Here are five steps on how to make sure you're using hotspots safely.

1

Make sure it's the real network

One way fraudsters work is to set up a Wi-Fi hotspot of their own and disguise it as genuine public Wi-Fi by using a similar name. Double check the exact name of the Wi-Fi you're trying to use by asking a member of staff.

2

Check for encryption

Encryption makes any network connection more secure. If the site address begins with "https" it's using SSL. This means that anyone who intercepts the information you share will be unable to read it.

3

Using a Virtual Private Network (VPN)

A VPN routes all your interactions with the web through a server in encrypted form, making it impossible for third parties to read. There are many desktop and mobile VPNs available, and they are fairly simple to use.

4

Update your apps

Regularly updating your apps means that you'll have the latest security upgrades and bug fixes. Download these updates as soon as your device lets you know they're available, to avoid letting fraudsters exploit out-of-date apps.

5

5. Turn off your Wi-Fi

If you're not using your Wi-Fi, turn it off. This will prevent it accessing hotspots automatically and potentially connecting to unsecure or fraudulent connections.

Turning off location trackers on your phone

Using GPS on your phone can be incredibly useful, helping with directions or finding nearby destinations. It also makes it easier to share the places you visit on social media, letting you tag photos or updates. Apps can't do this without your permission, but it can be easy for someone to agree to it when installing an app, without realising the full implications of how the data will be used. Here are some examples of apps that might use your GPS to track your movements.

Social Media – Apps like Facebook, Instagram and Snapchat can tag your posts, photos or Snaps with a location.

Google – Google's 'Location History' feature keeps a complete record of all the places you have visited.

Fitness Apps – If you're a runner, you might use an app that tracks how far and fast you run. To do this they will use GPS to track the location of your run.

Shopping Apps – Some apps will use your location to send you offers for products based on nearby shops.

The information below was correct at the time this guide was published.

Disabling location permission on Android



1. Go to Settings menu.
2. Open 'Apps' section.
3. In the drop-down menu select 'App permissions'.
4. Open 'Location' section.
5. Use the switches to decide which apps can access your location.

Disabling location permission on iPhone



1. Go to Settings menu.
2. Open Privacy section.
3. Open 'Location Services'.
4. Decide which apps can access your location, and whether that's 'always', 'never', or while you're using the app.

Managing software to stay safe

You can set your device to automatically install updates to apps, which will include security changes or new features. If you don't do this automatically or want to check which apps need updating, you'll need to review your apps regularly. Here are some key types.



Browsers

Just like on a PC or laptop, your web browser allows you to access a whole range of websites. Whether you use Safari, Android Browser, Chrome, Firefox or another app to browse the web, make sure it's updated to avoid leaving any gaps in your security.



Financial apps

Banking apps or services like PayPal offer direct access to your money and your account information. Making sure they are up-to-date and tightly secured are among the most important things you can do with your device.



Anti-Virus

Many PCs will come with anti-virus software pre-installed, but this isn't always the case on mobile phones. Installing an additional security app can give you extra protection from malware and apps that aren't trustworthy.



Permissions

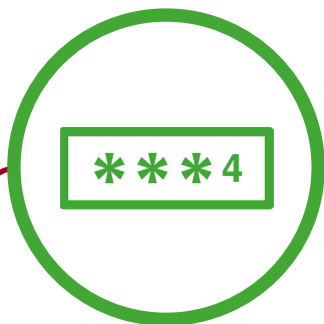
Apps that you have already downloaded may ask to change their permissions settings when installing a new update. Be careful to check exactly what you're agreeing to as an app that appeared trustworthy could later be used to [spread malware](#).



Payments

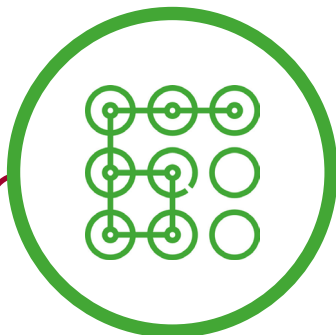
You should be informed that 'micropayments' are included when you download certain games or apps. Make sure that a passcode or fingerprint is required to verify purchases, to stop any unintentional payments being made.

How to secure your device



1. Add password or PIN

Passwords or PIN codes offer a high level of security, but can be forgotten and might be inconvenient if you lock and unlock your phone frequently.



2. Add a pattern

Patterns can be easier to remember – for example, if you use a particular shape. They can also be easier to enter, compared to a PIN code or password.



3. Add a fingerprint

Unlike patterns and passwords, you don't need to remember a fingerprint and it can be quick to use. This convenience is why more and more devices are using fingerprint or other biometric technology.



4. Use 'Find my phone' software

Both [iPhones](#) and [Android](#) phones offer software that allows you to track the location of your phone, which may be handy if it's lost or stolen. You can also lock the phone or delete files remotely, so make sure you have enabled those features.

Useful resources

Any new technology can create opportunities for fraudsters to try and exploit. This shouldn't put you off using valuable online services; it just means taking the appropriate steps. Being informed and sticking to safety guidelines should help you and your family stay safe online. We hope you found the information in this guide useful. Here are some other helpful links that you might want to check out:

Equifax Knowledge Centre – identity protection articles

[**https://www.equifax.co.uk/resources/identity_protection/identityprotection.html**](https://www.equifax.co.uk/resources/identity_protection/identityprotection.html)

ActionFraud – National Fraud & Cyber Crime Reporting Centre

[**http://www.actionfraud.police.uk/**](http://www.actionfraud.police.uk/)

Cifas – Not-for-profit fraud prevention organisation

[**https://www.cifas.org.uk/**](https://www.cifas.org.uk/)

Stay Safe – BBC guide for kids online

[**http://www.bbc.co.uk/cbbc/shows/stay-safe**](http://www.bbc.co.uk/cbbc/shows/stay-safe)

UK Safer Internet Centre

[**https://www.saferinternet.org.uk/**](https://www.saferinternet.org.uk/)

MoneySavingExpert - 30+ ways to stop scams

[**http://www.moneysavingexpert.com/shopping/stop-scams**](http://www.moneysavingexpert.com/shopping/stop-scams)

Citizens Advice – computer and online scams

[**https://www.citizensadvice.org.uk/consumer/scams/scams/common-scams/computer-and-online-scams/**](https://www.citizensadvice.org.uk/consumer/scams/scams/common-scams/computer-and-online-scams/)

Which? - keeping your mobile phone secure

[**http://www.which.co.uk/reviews/mobile-phones/article/keeping-your-mobile-phone-secure**](http://www.which.co.uk/reviews/mobile-phones/article/keeping-your-mobile-phone-secure)