Age 14-16

Fraud and scams – how to stay safe

Stay safe!

On social media:

If you use social media, then you need to take care with what you share.

What to look out for:

- Strange requests from family or friends: if you get an unusual request from family or a friend, call them on a number you trust to make sure it's real.
- Spelling mistakes: fake messages and accounts can look odd. They could have a messy layout or spelling mistakes.
- Fake quiz: if you need to give personal details to enter a competition or quiz, it could be fake.

What you can do:

- Think about what you share. Don't use your personal details for passwords. Fraudsters may use social media to see your details and try to guess your passwords or steal your identity.
- Go private. Check your settings often and make sure they're on private.
- Only connect with people you know. If you're not sure who a person is, then don't connect with them. Some accounts are fake and just try to steal details.

Act fast:

- Report to your service provider.
- Virus check your phone or device.
- Change passwords.

Age 14-16

Fraud and scams – how to stay safe

With your identity:

You need to keep your identity safe online. If your personal or banking details are stolen, they could be used to commit fraud. This may harm your personal finances and credit rating.

What to look out for:

- Odd transaction: check your bank or credit accounts.
- Unexpected post: letters may arrive that you didn't expect. Even credit cards that you didn't apply for.
- Credit is refused: your credit score is good, but you get turned down for credit.
- Calls about debt: you could get calls from debt collectors or companies about things you didn't buy.
- Credit history: unknown entries that show up.

What you can do:

- Check your account statements on a regular basis.
- Check the details your bank holds are still correct i.e. no changes have been made to address or telephone number.
- Contact your bank if you think you have been a victim of ID Theft/Account Takeover.
- Your details can be found in many places, so you need to keep them safe.
- File or shred paperwork.
- Be safe on social media. Be careful of what information you share – even photos. For example, photos outside of your house that show your house number. Be vigilant. Don't share banking or payment details, even to friends.
- Be wary of strange emails or texts. Don't reply until you've double checked. And don't reply with your personal details.
- Cancel lost cards or documents right away.

Act fast:

- Change your security questions – as your personal details may help someone to guess them.
- Contact **Action Fraud***. They can help you to report a crime or give general advice.
- Tell other sites: if your details are on other sites, tell them about the theft.
- Contact Royal Mail – if you think your mail has been stolen or redirected.
- You could also register with CIFAS**. This could help to protect you and stop fraudsters using your details to apply for products or services in your name.

* Action Fraud is the UK's national reporting centre for fraud and cybercrime where you should report fraud if you have been scammed, defrauded or experienced cyber crime in England, Wales and Northern Ireland.

** CIFAS: Credit Industry Fraud Avoidance System. Is the UK's leading fraud prevention service. They offer members of the public increased security against identity fraud, as well as expert advice on how to protect personal data in our increasingly tech-reliant world.

Age 14-16

Fraud and scams – how to stay safe

Using your devices:

There are threats that can harm your devices even if you're not aware that anything is wrong.

What to look out for:

- Alerts from your anti-virus software.
- Unfamiliar downloads.
- Unexpected files and programmes.
- Slow running programmes.

What you can do:

- Log off after banking online to stop anyone else getting into your account.
- Lock your device – when not in use, you should lock your device with a PIN or password so others can't use it.
- Keep up to date. Make sure you update your device's operating system, internet browser and software as often as you can.
- Use an anti-virus: install it on your computer and keep it up-to-date.
- Scan for viruses at least once a week and follow its advice.
- Be careful what you download. Only download files and programs you know are genuine and come from a source you trust. Fake downloads can harm your device with a virus. A virus can also be used to try and steal your details. Get your mobile apps from an official store such as the App Store or Google Play.
- Keep your firewall on – a firewall helps prevent hackers from getting into your computer. Only a computer expert should turn it off.
- Only use secure Wi-Fi. Make sure it's genuine and secure. Be careful of sites that want payment or banking details.

Act fast:

- If you think your device has been infected by a virus, get it checked out.
- Change your Wi-Fi password.

If you think someone has used your account without your approval contact your service provider or bank immediately.