STAYING SAFE ONLINE

East London Age UK

TEAM CONNECT

This e-sheet is part of a larger information pack which also includes pages on Cash and Other Payment Methods and Paying Bills and Switching Providers. All three are available as summarised hand-held versions.

We would kindly appreciate your time to provide us with feedback on our information sheets. Please click here to access our survey.

New technology has transformed the way we live; we are more connected than ever – to new information, to our loved ones and so much more.
However, Staying Safe Online can be a daunting prospect. From creating secure passwords **(and remembering them!)** to avoiding scams, there are a variety of things that need to be considered when accessing online services.

To help with **Staying Safe Online**, the information in this guide aims to present information on best practices to follow to help you navigate the internet confidently and safely.

ONLINE SAFETY TIPS

Make strong passwords and don't tell them to others.
Reputable companies do not need to know your password, and you should not tell people your passwords even if they are helping you with your account.

Check internet addresses.
Scammers will often make websites that look like the real thing. Always check the addresses to make sure you are on the right site.

https://

The padlock symbol indicates the connection to a website is secure, looking for this is one of the checks you can make to make sure a website is legitimate. This **article on Which?** has more information on other things to look out for.

Use up to date virus protection on your computer and other devices.

Call a bank/company back if you're contacted unexpectedly.
Most banks and the government don't call or email with unsolicited advice, so if someone calls you claiming to be from a bank or other known company, you can phone them back after you find the company's phone number from a letter or their website to make sure they are who they say are.

Don't make large financial decisions hastily.
It is good practice to take time and consider a new financial product or investment, this gives you time to reflect and research.

Seek further guidance if you're unsure about something.
This could be asking a family member or close friend as well as utilising helpful resources online or over the phone such as **The National Cyber Security Centre**, **Citizens Advice** and **Which?**

WANT TO SHARE INFORMATION ONLINE?

Social media is great for keeping in contact with friends and family but be careful with what you share and with whom.

Make sure you **keep your privacy settings up to date** & regularly review who can see what you share.

Be aware of what information you share on your social media; scammers often use it to gain access to personal information.

Details such as your relatives and friends, address, phone number and which bank you use is all information that scammers may exploit.

The **Data Protection Act** controls how your personal information is used by organisations, businesses and the government.

It was established in 1998 and was updated in 2018 to implement the **General Data Protection Regulation** (GDPR).

Under this Act, you have rights as to how your data is stored and used as well as being able **to find out** what personal information an organisation has stored about you.

SCAMS

Though scammers frequently change their tactics, they always rely on catching people out. Being informed of their methods and keeping an eye out for tell-tale signs of a scam will help protect you from their schemes. You can check if a pension or investment opportunity is on FCA Warning List on **ScamSmart website**.

This section provides information about how you can avoid being scammed, and what to do if this happens to you or someone you know.

Scams you are likely to encounter:

- Email scams (also called phishing)
- Text message scams
- Pension & investment scams
- Door to door Scammers

If you do think you've found a scam, you can report it by forwarding it to report@phishing.gov.uk.

Scams will often have one or more of the following traits, but they won't necessarily have all of them. Some scams include logos and graphics to lend themselves validity:

- **Unfamiliar contact methods** - banks send letters, emails and will phone, but they won't contact you through social media sites like Facebook. Most banks also won't send unsolicited emails about new products. Some scammers may even go door-to-door.
- **Closely matched email or web addresses** – e.g., mis-spelled name of a bank or provider.
- **A sense of urgency** - Scammers will often suggest you have to act quickly or that an "amazing" deal is only available for a limited time.

REMEMBER THE GOLDEN RULE

"IF IT SOUNDS TOO GOOD TO BE TRUE, IT PROBABLY IS."

- **A sure bet** – this could be a mention of a "guarantee" of high returns for little input.
- **Asking for your password & personal details** – Banks and bill providers won't ask for your password or personal details in an email, though they may ask security questions.
- **Out of the blue** – cold calls, emails, text messages from unknown contacts, or someone new showing up at your door are a red flag.
- **Secrecy** - Scammers may urge you to not discuss their proposal with anyone else.
- **Personal** - Scammers may address emails to a 'valued customer' or 'friend', and not to you personally.

BUT WHAT DOES A SCAM EMAIL LOOK LIKE?

From: Taxes <taxes@crediunionauthorities.org>
Subject: Online Submission for Reference 830618913

Is this a real email address?

Dear taxpayer,

Not addressed to you.

Generic subject name.

We are pleased to confirm that your claim form has been successfully submitted.

Please find and download the attached "Department_of_refunds_your_tax_is_ready" and follow the instruction.

For your security, you must review these refunds by April 1.

Generic attachment which is not an official document (PDF, Word Doc).

Thank you!
Rose Harvey
Tax Associate

Incorrect spelling is common.

Please note:

Urgency – This asks you to act immediately.

If you will not complete the required form, you will not be able to claim your tax refund online.

IMPORTANT: IF YOU FEEL THREATENED, CALL THE POLICE ON 101.

CHECKLIST

Realising you have been scammed can be frightening. The following checklist provides some actions you can take to protect yourself and prevent further harm should you find yourself in this situation.

- **Identify what has happened** – for example, has money been transferred & by what method? Have they gained access to your device? Have your personal or account details been stolen?
- **Stop transferring money** – contact your bank immediately to stop any Direct Debits that may have been set up.
- **Document what has happened** – write down what you can remember about what happened, these details will help the authorities take the right course of action and may prevent others from being a victim of the same scam.
- **Report the scam** to **Action Fraud** or phone them on **0300 123 2040**.
- **Contact the police** - If money has been stolen you can contact your local police on their non-emergency number by dialling **101**. You can also report to the police on this **website**.
- **Tell someone you trust** – ask someone for help, a family member or friend can offer much needed support in difficult circumstances.
- **Change your passwords –** Change passwords to any accounts which may have been accessed, including email and bank passwords.

Roughly 95% of scams are not reported! Remember, there is no shame in being a victim of a scam, it can happen to anyone.

- **Check if you can get your money back** – Whether this is possible depends on what has happened. More information is available through **Citizens Advice** (**0800 144 8848**).

CONTACTS

There are several services across the UK which can provide further information on staying safe online and what to do if you think you have been scammed. A few are:

- **AGE UK** – **Support for Scam Victims** webpage. You can also contact the Age UK Advice line on **0800 678 1602**.
- **VICTIM SUPPORT** have an **online form** for advice and support. If you require urgent help, you can call them on **08 08 16 89 111**.
- **ACTION FRAUD** allow you to report crimes on their **website** if you have lost money.
- **PHISHING** – You can reporting suspicious emails to **report@phishing.gov.uk**.
- **SCAMSMART** – The FCA has lots of resources online on their **website**.

This sheet is an extended version of the summary sheet and has been produced by graduates and apprentices as part of the Financial Conduct Authority (FCA) CEO Challenge, which is a mandatory part of the Graduate and Apprentice Development Programme. The FCA sponsors the challenge to encourage graduates to come up with innovative ideas to help members of our community. The content does not form part of any FCA policy. This extended sheet does not address your individual requirements and is for information purposes only. This does not constitute any form of advice and should not be relied on by you making (or refraining from making) any specific decisions. The information presented is correct at the time of research in March 2021.