How To STAY SAFE ONLINE

Keep Calm & Stay Safe!

Everyone will have heard the stories of people being scammed online and losing lots of money, so it is important to stay safe when using the internet. With some easy steps and following some simple rules, you can keep yourself, your computer, your identity, and money safe. So, Keep Calm & Stay Safe!

Passwords and PIN numbers

Choose your passwords carefully. They normally need to be more than 6 characters including a capital letter (not necessarily at the front) and a number. It is safer to have a different password for each account. Your computer should have a password to protect it and your mobile devices such as phones or tablets should be protected either by a PIN number or a password in conjunction with eye and fingerprint recognition.

Virus protection and keeping up-up-date

Make sure that you have internet security software installed on your computer and a security app on your phone and tablet. Some of these are free which may mean that they have limited features and some a paid for on a subscription basis but it is essential to have protection.
Always install updates to your computer and mobile devices when prompted. The companies that make software are always patching security holes as soon as they are discovered.

Fakers – Phone Calls *(also see* Fakers – Phishing *overleaf)*

Because security software for computers is so good, many scammers rely on the weakest link – YOU. They will use several methods to try to convince you to do something which will put your data or money at risk.
WHAT THEY DO - You may get a phone call claiming to be from Microsoft or a computer manufacturer or even your bank claiming that there has been some kind of security breach, or that your account has been suspended. They will either tell you that you to give them your bank account details or download a bit of software to 'patch' your computer.
WHAT YOU SHOULD DO FIRST - Hang up immediately. Banks don't ask for your details over the phone and computer companies don't phone their customers about security.
WHAT YOU SHOULD DO NEXT – Keep calm. You have identified and dealt with a potential threat – well done! If you can check their phone number, you should take a note of the number and block them if possible. If they were pretending to be a bank, you should contact the bank and let them know.

Always check that there is an HTTPS rather than HTTP or a padlock symbol when using a website to buy anything

Buying safely online

There are some fantastic bargains online and if you want to save money, often buying from an online store is cheaper than the high street. Buying online is safe as long as you follow these guidelines;

- Check reviews of online stores and products
- Buy from recognised websites
- Use a credit card – this has better protection than other methods
- Never pay by direct bank transfer
- Don't use public WiFi to buy anything
- Only use sites that the padlock symbol or HTTPS (not HTTP)
- Take your time and think twice before buying
- Check that they have a contact number or email address

How To STAY SAFE ONLINE

Fakers – Phishing (email scams)

Remember – YOU are the weakest link! Fakers and scammers will try to trick you into making a security mistake and giving away passwords or sending money to a fake company or bank.

WHAT THEY DO - You may get an email which is from your bank. It will look like a legitimate email with proper logos, style and colours of the bank. They will try to get you to provide them with your log-in details for your bank, or your PIN number or password. There may be a button or link that they ask you to click.

HOW YOU CAN TELL IT IS FAKE

- you should be suspicious of any email claiming that you need to put your details into a website – whether it seems to be from a bank or social media platform or online shop.
- Check the email address it has been sent from – this will either be nothing like the bank's email address or it may have a subtle difference in the spelling.
- Links can be disguised with different text – it may say 'Click Here' but not show where it is taking you. If you hover your pointer over the link, after a second or two, the actual link will be revealed. This address may look similar to the expected website name but will have subtle differences in spelling.
- If you DO click on a link, it may take you to a website which is an exact replica of your bank's website. It may ask you to log in with your account details. **DO NOT LOG IN. CLOSE THE WEBSITE. ALERT YOUR BANK.**
- As many of these phishing emails come from non-English speaking countries, the grammar or phrasing may seem strange.

WHAT YOU SHOULD DO – Do NOT click any links on the email. Close the email and mark it as 'spam'. This will put any future emails from that source straight into a special safe folder.

Too Good to be True

One way that scammers try to entice people into divulging account details is by setting up fake offers which seem just too good to be true – perhaps a new iPhone for £50, or a way to make lots of money very quickly. If it SEEMS too good to be true, then it PROBABLY is.

The process of signing up for these offers will either require you to pay money up-front, or include you providing enough information that they will be able to take control of some of your online accounts.

Over-sharing on social media

Don't give away too much personal information on social media, especially financial information. Do not post your bank details publicly or send a stranger any financial details or passwords or clues to passwords (for example – "my password is the name of my dog") in a direct message.

It is also very tempting to let everyone know that you are going on holiday, or post pictures from your holiday abroad while you are there – but this is announcing that your home is empty, and you won't be home for several days!

- **SPAM** – unwanted emails from companies trying to sell you a product or service, sometimes offensive, explicit, or dangerous to open.
- **VIRUS** – a computer programme which will either damage your computer or as **SPYWARE** steal your details.
- **PHISHING** - an email which tries to con you into giving details to online accounts.