Best Security Practices

Fake email addresses

To ensure you're not replying to a **fake** email address, check the address of the email you have received, especially the **domain**. (the domain is what follows the @ in the email).
E.g. **@Barclays.corporate.com** may look real, but it isn't **@Barclays.com**, it's **corporate.com** since the "**.**" separates them.

Another thing to look out for is **incorrect** letters, e.g. **techfcrce.uk** isn't the same as **techforce.uk** and **barklays.co.uk** isn't **barclays.com**.

Spoofed Emails and Phone numbers

Even if someone emails from a **known** address or calls from a **known** telephone number, they may still be a **scammer**. Email address and telephone numbers can be **spoofed**.
Spoofing is the act of disguising a communication from an **unknown** source as being from a **known**, **trusted** source.

If unsure, call the company on a telephone number you know is them to check, **don't** use a number from an email or link they have sent you.

Asking to change bank payment details

NEVER trust an email or phone call asking you to change **bank payment details** or to make a payment even if this appears to be from a person you know. It could always be a **fake** email or a **spoofed** email, so it's never worth the risk.

Always call back on a known number to check if it's **genuine**.

Clicking on links for buttons

If you are going to click any **links** or **buttons**, firstly **hover** over the link and a box will pop up showing you the link to the site it will take you to, does it look **genuine**?

Never click a link on an email that asks you to verify sign in details.

Things to look out for

Don't trust emails that have **poor grammar** and **spelling errors**, **urgent action demands**, an **unfamiliar greeting** or **salutation**, requests for **login credentials**, **payment information** or **sensitive data** as well as **offers that are too good to be true**.

Passwords

Always use **strong** passwords. One way of doing this is to pick **3 random words**, include **capitals**, **lowercase** letters as well as a **number** and/or special **character**.

Don't pick words that include anything to do with **yourself** that people may guess such as a **pet's name**, part of your **home** or **work address** etc.
For example, a good strong password would be: **RedBrushOpen21%**

Don't use the **same** password for everything. We recommend using a **password manager** such as **KeePass** or **LastPass** to store your passwords.

Extra Tips

Always log out of online accounts when you're finished, especially on **shared** or **public** computers.

Be aware that phishing can occur via **email**, **phone calls**, **text messages**, or even through **social media**. **Always** be sceptical of unsolicited communications requesting sensitive information.

Avoid sharing **personal information** such as your full name, address, phone number, or financial details on social media or **untrusted** websites.