Multi-factor authentication

Multi-factor authentication, often called MFA or 2-step verification (2FA), is an extra layer of security for your online accounts. Instead of relying only on a password, it requires a second "factor" to prove it is really you, such as a code sent to your mobile phone, a notification on an app, or a fingerprint scan.

Passwords can unfortunately be stolen or guessed by scammers. MFA is vital because even if a criminal gets hold of your password, they still cannot access your account without that second piece of evidence. It is one of the most effective ways to stop unauthorised access to your banking, email, and social media.

While safety tools help you manage who you interact with and what you see, MFA is a specific technical barrier. It is purely designed to secure the "front door" of your accounts, ensuring that only you can walk through it.

Below are 5 top tips if you are considering using MFA:

- 💻 **Enable it for your most sensitive accounts:** Prioritise your email and banking first, as these are the keys to your digital life.
- 📱 **Use an Authenticator App:** Apps like Google or Microsoft Authenticator are more secure than receiving a code via SMS, as they don't rely on your mobile network.
- 🤐 **Don't share your codes:** A genuine company will never call you and ask for your MFA code. Treat these codes with the same secrecy as your bank PIN.
- 🔐 **Keep your backup codes safe:** When you set up MFA, you will often be given "recovery codes." Print them out or write them down and keep them in a safe place at home in case you ever lose your phone.
- 🚨 **Check for "Push" notifications:** Many apps now allow you to simply tap "Yes" on your phone to log in. Always check that the login request matches the time and place you are actually trying to sign in.