What is Two-Factor Authentication?

Whats is Two-Factor Authentication (2FA) and do I need it?

Firstly, What is 2FA?

2FA is an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are. First, a user will enter their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information. This is most commonly a verification code received by email or by text message. Your bank may even need you download an app to your smart phone.

Why do I need 2FA?

Humans have lousy memories and also have bad habits! Today nearly everything we do is online and this means more and more online accounts. The chances are you have reused the same password (or variations of the same password) across multiple accounts. 2FA helps mitigate the risk of an account being taken over and personal details (or money!) being lost. With 2FA having the password alone is not enough to allow a hacker to access what they shouldn't.

Now that I have Two Factor Authentication am I safe?

Not exactly. Whilst 2FA will definitely bring a boost to your online security, no security measure is bulletproof. For example, a hacker could theoretically gain access to your recovery email or intercept your text messages and acquire the code for access. They might try to sign in from a trusted device without your knowledge or use social engineering to figure out your recovery questions. All this is to say no one security measure will guarantee your protection.

However, 2FA remains highly effective in protecting your accounts and along with a sensible approach to online security it should protect you from a majority of hacking attempts.

If you are concerned with your online security and would like advice please give us a call! We're here to help!