THE
EASTERN
CYBER
RESILIENCE
CENTRE

Little Steps to Becoming Cyber Resilient

What is 2FA and why should I use it?

So, at this point you should have instigated strong, unique passwords and thought about a method for you to remember your passwords.

However, no matter how good your passwords are, they can only provide so much protection. They could be stolen from your service provider or from your phone, tablet or laptop. Or you could get tricked into revealing them. Therefore, you need to consider using two-factor authentication (2FA), both at work and at home.

What is 2FA?

2FA provides a way of 'double checking' that you really are the person you are claiming to be when you are using online services, such as banking, email or social media. It is available on most of the major online services.

When setting up 2FA, the service will ask you to provide a 'second factor', which is something that you (and only you) can access. This could be a code that is sent to you by text message, or that is created by an app, biometrics or a link.

Is it really necessary for all my accounts?

You should implement 2FA for all important accounts especially email and banking. Email is essential as this is the route most services will offer for password changes and account updates, so you need to ensure that you are the only one able to access this.

What should I do now?

- **Identify your important accounts.** This will vary for each situation, but email and banking will almost certainly be key. Business social media accounts may be vital if you conduct business across these. You do not want someone else to have access and pretend to be you or wipe your customer details.
- **Enable 2FA on your key accounts.** An internet search will be able to give you detailed directions about how to do this for your specific accounts. For example, search for ‘ 2FA for Gmail’ or ‘2FA for Facebook’ and click on the relevant links for further instruction.