Benefits of 2-Step Verification

2-Step Verification (2SV, also known as 2 Factor Authentication or Multifactor Authentication) provides an essential layer of security to online accounts. During login with the username and password, a Onetime Passcode (OTP) is also required, normally made up of 6 digits. Never share your OTP with anyone, even if they claim to be "support" for the service you are using.

Many reputable services (including email and social media) now offer 2SV, which can be found in settings. If the services you are using do not offer 2SV, you may want to consider moving to ones that do.

Popular authentication methods

- The OTP is sent to a phone as a text message or phone call
- Authenticator App stores OTPs for multiple accounts and refreshes the passcode every 30 seconds. You do not need to be connected to a phone network or Wi-Fi to get your code.

When given the option, use the Authenticator App instead of text message or voice call. This is because cyber criminals have been known to clone SIM cards and receive the OTP for themselves to get through the login process. However, the benefits for having 2-step verification far outweighs the risks, so if a message to the phone is the only option available, continue to use it.

THE CYBER RESILIENCE CENTRE FOR LONDON

This extra step comes with strategic benefits:

- Prevents a cybercriminal from gaining access and taking over your online account should the password be compromised.
- If the cyber criminal manages to get onto the account, 2SV should block them from updating the password.
- If you have chosen to receive the OTP via text message or phone call, you will receive an unexpected passcode when a criminal tries to log in, notifying you that your password is compromised.

@London_CRC Cyber Resilience Centre for London @CRCforLondon londoncrc.co.uk info@londoncrc.co.uk