Step 3 - Phishing (avoiding scams)

- Do not click on any unverified emails, texts, or other messages (e.g. on any social media platform this will also include messaging apps).
- Do not respond to in app notifications asking you to log in or change your password. Instead go directly through your settings to review your security and login history.
- Verify all contact using a trusted a phone number, contact or check via their official website or app.
- Never be rushed into clicking a link that requests you to reset your password, enter a competition, or to do something on the back of a message received (e.g. a request for help, support, or financial requests).
- Scammers might urge you to use a fake login link. Or request you to share your 2-Step Verification codes. This is equivalent to handing over house keys to an account.

For further information, visit:

www.eastmidlandscybersecure.co.uk/nottinghamshire

East Midlands Special Operations Unit

In partnership with:

THE CYBER RESILIENCE CENTRE FOR THE EAST MIDLANDS

SOCIAL MEDIA AND EMAIL HACKINGS

Reports of social media and email hackings are on the increase

To help reduce the volume we are currently seeing, please review these 3 steps:

Step 1 – Password Security

- Always use a different password for each online account you have, otherwise one Data Breach or password compromise will put all your accounts at risk.
- Strong memorable passwords can easily be created by combining three random words. For example, you could use: Hippo!54Pizza-Rocket1
- Consider using a trusted password manager if you use more than one account and write down your master password somewhere secure.
- Never share passwords or authentication codes with anyone no matter who they claim to be.

Report Fraud and Cybercrime to Action Fraud to: 03001232040 or actionfraud.police.uk

Step 2 – Extra account protection

- Two-Step Verification adds an extra layer of security to your account.
- Enable 'Two-Step Verification' (via account settings) on each of your accounts such as email, social media, and shopping sites.
- Always update your device software, apps, and other programs to fix newly identified security bugs and vulnerabilities.
- Delete old contact numbers and email addresses, to ensure personal data is relevant and up to date.
- Check where you are logged in and remove old or suspicious devices logged in to the account
- Back-up all important documents, passwords, authentication apps, contacts, photos, and videos using a separate device or within the cloud.