Takeaways and Actions!

- ❑ Use strong, unique passwords
- ❑ Consider the use of a password manager / book
- ❑ *Always use Two Step Verification (2SV, 2FA, MFA)*
- ❑ Email/text message links – be cautious! (What is normal?)
- ❑ Privacy settings – esp. on Social Media (Reduce information to attackers)
- ❑ Update devices and software promptly
- ❑ Consider data back-ups
- ❑ Turn on Antivirus
- ❑ NCSC Cyber Aware Action Plan: https://www.ncsc.gov.uk/cyberaware/actionplan
- ❑ Stop! Think Fraud website: https://stopthinkfraud.campaign.gov.uk/
- ❑ Check data breaches on haveibeenpwned? https://haveibeenpwned.com/

Useful Links:

Advice and Tools from the National Cyber Security Centre:

https://www.ncsc.gov.uk/cyberaware/actionplan

https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

https://www.ncsc.gov.uk/cyberaware/home

Our website is filled with hints, tips and links:

https://southeastcyber.police.uk/cyber-advice-individuals/

Learn more about Phishing / Scams:

https://stopthinkfraud.campaign.gov.uk/

https://www.takefive-stopfraud.org.uk/

To contact your bank when concerned, call **159**