TELEWORK CYBER SECURITY TIPS

Home Internet

- Reset your home internet password – anyone who ever visited you may have your password saved making you vulnerable
- Be aware of connected devices like doorbells, refrigerators, etc – hackers can use them as a back-channel into your computer
- Set up two channels if possible – one dedicated for work and one for phones, kids, devices, etc

Passwords

- Vary your passwords, do not use simple passwords or ones that contain important names or dates ie: Liam12.28.09
- Do not use your work password for other accounts
- Do not play Facebook games that ask for lists of potentially sensitive information ie: high school name/mascot, mother's maiden name, where you were born – hackers can use this info to get around passwords
- More info on digital password guidelines visit NIST.gov

Phishing

- Phishing emails attempt to get you to click on a link or enter sensitive data like user names & passwords - be careful opening suspicious emails
- Hackers have become more sophisticated and are able to mimic legitimate-looking emails
- If in doubt, follow company protocols for reporting, contact the person who supposedly sent the email or visit KnowBe4 Free Phishing Security Test for free testing

Sensitive Company Data

- 2 factor authentication and a VPN secure network are reported to stop 99% of hacks per Microsoft
- Limit downloading sensitive documents & data
- Do not leave your computer open and unattended
- Turn your computer off at the end of the day so it is not vulnerable when you are not using it

For these resources and services contact Mark Easteadt at 610-858-3414 or mark.easteadt@pacommuterservices.org

COMMUTE PA