AtNetPlus

National Cybersecurity Awareness Month

Common Security Tips for Employees

- **End-users are often one of the biggest security risks to an organization**
  - Be aware of the information or documents that you keep out on your desk
  - Passwords should NEVER be written down anywhere central to your device on post-its, paper, within documents, etc.
  - Be wary of sending passwords through email or instant message
  - Do not store sensitive information (such as credit cards) under your keyboard, in your drawers, etc.

Common Security Tips for Employees (cont.)

- Do not use the same password for all of your business systems when possible – we use active directory as a master password, but that’s why MFA being enabled is incredibly important
- Make sure that programs you download onto your computer are business-approved and the files are safe
- Be conscious of the websites you visit while you are at work
- Phishing testing and training is critical and should make you hyper-aware of the threats that phishing poses to a business - be extra careful not to click on any unknown links
- LOCK your computer when you’re away from your desk, even for brief time periods

Internal Security Auditing

- If your business was to do a security audit and simulated hacking, would you be "left standing"?
  - Do you have passwords written down or in your email?
  - Do you have a habit of leaving your computer unlocked?
  - Do you have any client information printed out or on your desk?
  - How is the strength of your passwords? Are you using the same passwords for multiple sites?
  - Do you have MFA enabled for any system that you can?
  - Have you downloaded any programs that are not on the approved programs list for business use?
  - Have you ever visited a website that may have had questionable links, downloads, or content?
  - Do you use your work device on networks outside of the office?

MFA – Is it Enabled?

- Do you have Multi-Factor Authentication enabled for all possible systems and accounts?
- Do you make sure that your MFA is working properly? (i.e. Do you notice that it doesn't prompt you for an MFA code outside of the office when you know it should be?)
- MFA is not 100% full proof
    - There are various forms of social engineering built to trick you into sending a hacker your text verification codes