DID YOU KNOW?

Importance of Using a Password Vault

HOW TO KEEP INFORMATION PRIVATE AND SECURE

WHAT'S INSIDE?

When Creating a Password

By PrivacyandSecurity.org

- Use a password or other function on your computer or mobile device so that you are the only one who can access your information
- Use a strong password and update often
- Do not share your password with anyone!
- Use a password vault to store your password

WHEN USING SOCIAL MEDIA

by Healthit.gov

- Think carefully before you post anything on the internet that you do not want to be made public - do not assume that an online public forum is private or secure
- If you decide to post sensitive information on social media, consider using privacy settings to limit access by the public
- Remember how many times Facebook has been breached and other sites like Snapchat
- Be aware that anything you post may remain permanently!

"13 million consumers fell victim in 2019 and it cost them $3.5 billion in out-of-pocket costs"

by Javelin Strategy & Research

Identity Theft is a major problem in the United States. With technology evolving so rapidly, fraudsters now have more opportunities than ever before to access your data for their own gain. It is very important to safeguard your information and protect you and your organization from becoming victims!

There are many different types and for this training, we will introduce Account Takeover Fraud.

Account Takeover Fraud is when someone gains access and takes control of one or more of your accounts without your knowledge or permission.

It is important to use strong passwords and VPN when working from home.

WHEN USING MOBILE DEVICES

by Healthit.gov

Important: For work devices, call your IT department for questions!

Research mobile apps – software programs that perform one or more specific functions – before you download and install any of them. Be sure to use known app websites or trusted sources.

Read the terms of service and the privacy notice of the mobile app to verify that the app will perform only the functions you approve.

For your own personal devices: Consider installing or using encryption software for your own device. Encryption software is now widely available and affordable.

WHAT IS PHISHING

by Phishing.org

Phishing is a cybercrime in which targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.

10 Ways to Avoid Phishing Scams

by Phishing.org

1. Keep informed about phishing techniques through security awareness training
2. Think before you click!
3. Install an anti-phishing toolbar to alert you if sites are compromised
4. Verify a Site's Security such as looking at their website certificate. Never download or open files from unknown source!
5. Check your online accounts regularly - read your monthly statements
6. Keep your browser up to date with security patches (Don't be lazy and put it off)
7. Use firewalls for your desktop and network to help filter and reduce hackers getting in!
8. Be wary of pop-ups - block them
9. Never give out personal and work information
10. Use antivirus software

Remember: There is no single way to avoid phishing attacks!