Cybersecurity 101

Protecting your work environment from Social Engineering

Tailgating: allowing someone to follow you into a door that otherwise is secured for one person authenticated entry. We do not have these entry ways at CCRI, but if you were going into a locked building/hotel with a key code, you would not "hold the door" or allow another person to enter behind you without them entering their code.

Shoulder-Surfing: do not allow others to see data on your computer screen, watch you enter your password or press buttons on a key pad entry.

Dumpster Diving: This could be outside dumpsters or your individual trash barrel at your desk. Shred documents before placing in garbage. CCRI has Shredding Stations; if you do not have a document shredder in your department, always use the Shredding Bins to dispose of your paper trash that has sensitive data.

Lock your Workstation: When you walk away from your workstation or go to lunch, always make sure your workstation is locked to protect the data on your computer hard drive and CCRI's network shared drives.

Protecting your Identity and Credit

Visit the 3 credit bureaus and freeze your credit. This is a free service. Your credit can be thawed and re-frozen whenever you need to apply for credit. A credit freeze will not allow inquiries into your credit worthiness, nor will it allow new credit accounts to be opened.

Get a copy of your credit report free once a year. You should check your credit with all 3 bureaus for accuracy and report anything false on your report to each of the 3 bureaus.

WWW.EXPERIAN.COM

WWW.TRANSUNION.COM

WWW.EQUIFAX.COM

WWW.ANNUALCREDITREPORT.COM

Password Security

Do not reuse passwords; create a new password for each account. This can be difficult, using a Password Manager can help.

Use long passwords or a passphrase. Using 3 random words, a number, and special character is actually easier than you might think example: friend built butterfly friend_builtbutterfly33!

Use multi-factor authentication when available. Most websites, banks, email accounts offer this protection.

Use a password manager. Some are free, others are a subscription. The top 10 for 2022 by PC Magazine are: Keeper, Zoho Vault, bitwarden, LastPass, 1Password, LogMeOnce Password, RoboForm Everywhere, Password Boss, Dashlane, NordPass,

Protecting your Devices

Home Devices & Portable Devices:

Change your router default settings. When you signed up for your wifi and rented or bought the router, it came pre-configured with a password. Routers with generic pre-configured passwords are widely available through a google search. A hacker could use the admin password to reconfigure your network and/or steal your personal data.

Public Wifi: Should not be used unless you have a secure VPN. A better choice is to use your mobile data.

If you do use public Wifi you should not connect to a financial institution. You should sign out of accounts properly and clear the cache on the website immediately.