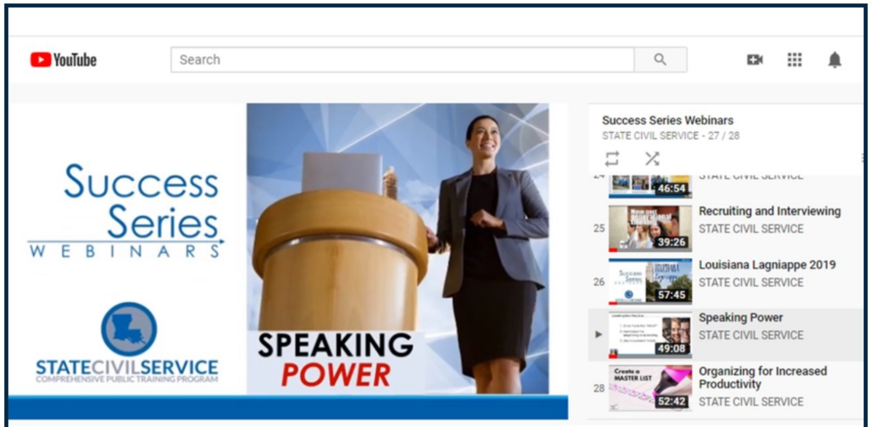

Check the State Civil Service YouTube Channel for all the Success Series episodes at:

https://goo.gl/Yc1PdK

Success Series WEBINARS
Download Handouts
STATECIVILSERVICE
COMPREHENSIVE PUBLIC TRAINING PROGRAM
CHARLES E. DUNBAR, JR. CAREER CIVIL SERVICE AWARD
LAYOFF INFORMATION FOR STATE EMPLOYEES
TALENT DEVELOPMENT
Contact Talent Development
HACKERS & SCAMMERS & THIEVES. OH MY!

For handouts from all the Success Series Webinars, visit:

https://bit.ly/2Kbn6Qa

Success Series WEBINARS
STATECIVILSERVICE
COMPREHENSIVE PUBLIC TRAINING PROGRAM
HACKERS & SCAMMERS & THIEVES. OH MY!
CYBER SAFETY

Protecting Your Data

This is perhaps the most important topic we can discuss at this time, considering the recent escalation of hackers and ransomware around the world. As we deal with electronic data and our personal identification information (PII), we need to take every opportunity to ensure their safekeeping.

This handout includes a collection of practices and tips that can protect your information and help keep you from being a victim of cyber crime.

APPS

- Clean out those old apps that you haven't used in 6 months or longer. Those are just extra opportunities for cyber criminals to sneak in.
- Remove or update apps regularly. Those updates are not only new features but also protection from the latest threats.

- Install apps from official websites and app stores only. And even those aren’t 100% secure because even Apple and Google can miss some threats. Read reviews first to see if others have experienced issues.
- Revoke permissions on apps that require access to sensitive information unrelated to their functions.
- Revoke access on Facebook, Twitter, LinkedIn, and Instagram to third party apps.

WEBSITES

- Do an inventory of your digital footprint.
    - Make a list of online accounts.
    - Set strong passwords for all of them.
    - Delete accounts you haven’t used in the past 6 months.
- To see if a website can securely handle your data, check to see if it starts with *https.*
    - A website starting with https encrypts the data you put in the website and the data you get from it, so no one can eavesdrop or tamper with the data flow.
    - If a website doesn’t start with https, don’t give them confidential info (card details, social security number, address, etc.).
- Practice regular patching to increase safety when online.
    - Patching is the application of updates to protect against the latest threats. A recent survey noted that almost half (47%) of the firms that had been breached were compromised because of a vulnerability where a patch was available, but hadn’t been applied.
- Keep your browser and internet-connected devices up to date with the latest versions.
    - Make sure to do this on a trusted home or work network -- not on public Wi-Fi.
    - Travelers connecting to public or hotel Wi-Fi networks have had their device prompt them to update a software package. This allowed malware to be installed on their machines.
- If you're on a mobile device, don't assume that your apps are automatically secure or using *https.* Check by using your browser to log on to the service, and look for the *https* connection in the status bar.
    - According to Extreme Networks, a global networking solutions provider, a Wi-Fi attack on an open network can take less than 2 seconds.

You don’t have to click to be infected.

- You can be subject to an attack without any user action, such as clicking, downloading, or even hovering. These are called drive-by attacks and they can come from something as simple as an ad or that strange news banner on the side of the page of a legitimate website.
- A drive-by scans your system for security holes. These holes can be security flaws in any of your apps or an outdated operating system or web browser. When it finds a hole, it downloads a virus or malicious software (malware) onto your system.

- Go to the browsers you use and uninstall/delete old browser plugins and extensions, and make sure the ones you use are up to date.
- There are free extensions such as *Https Everywher*e (https://www.eff.org/https-everywhere) that will encrypt the data you receive and share with many major websites and increase your browsing security.
- There are various tools to help you detect dangerous websites.
    - https://www.virustotal.com/
    - http://global.sitesafety.trendmicro.com/
    - http://zulu.zscaler.com/
    - Also, pay attention to your antivirus solution’s icons or blocks that warn you about potentially dangerous pages.

- When choosing a service provider of any kind:
    - Consider the general reputation of the organization.
    - Do a Google search for past security incidents.
    - Check to see if their website is secured by ‘https’.
    - Review their privacy policy.
    - Note the contact information.
    - Consider how much data they ask for and, if it seems excessive, ask why they want it.
- You can track your web traffic around the world with: http://www.monitis.com/traceroute/

EMAIL

- Perform a review of the security for your email account, including updates to:
    - Your recovery information
    - Your recent activity
    - Your account permissions
    - Your app passwords
    - Your 2-step verification settings
    - Ensure that your personal email autoresponder replies are not too detailed. (For example, don’t tell people the dates you’re going to be on vacation. Don’t make it that easy for burglars to plan to visit your home.)
- Create separate email accounts with different purposes.
    - One for newsletters and shopping
    - One for online accounts, such as social media
    - An account for work
    - A personal account
- Check your email’s activity log.
    - For example, with Gmail, you can scroll to the bottom of the page to find “Last Account Activity”. Click on “Details.” You’ll see recent Gmail access information.
    - If there’s something that you don’t recognize there or an old session from a different computer, you can choose to terminate it.
- Reduce your spam to reduce your risk. Spam campaigns are still one of the main attack vectors that cyber criminals use, so less spam means you’ll be a bit more secure.
    - Be careful where you submit your email address.
    - Unsubscribe from any unnecessary newsletters.
    - Use filters and mark emails as spam to help your email provider block it more effectively.
    - Never click on links in spam emails.
    - Never download and open attachments in spam emails.
    - Disable the automatic downloading of HTML graphics in your mails.
    - When using social media, set your privacy settings so no one can see your email account.
    - Be careful when visiting your Junk folder. Many ransomware infections begin with someone looking to see if an expected email ended up in there.
    - Check to see if headers match your friend’s address exactly. If not, it’s a fake.
    - Check attachments. No photo archive will ever be an .exe.
    - Office files can contain malicious code. Disable the Macros function in Microsoft Office before opening any Documents or Excels.
    - Check emails and links by rolling your cursor over them with your mouse before actually clicking on the link. Look at the destination URL is to see if it looks legitimate or not.

- Elements to watch out for to avoid phishing email that is attempting to collect your personal data:
    - Serious websites will never display your email address in the subject line.
    - Check out the sender's email to verify the validity of the email.
    - Don't be pressured into clicking on anything. Often, the more urgent the email sounds, the higher the chances of infection.
    - Don't click or respond to emails from online retailers. Go directly to the official website to confirm any issues with your orders.

PASSWORDS

- Take a moment to protect your passwords.
    - Check who's looking over your shoulder.
    - Use 2-factor authentication everywhere you can. Set it up to receive authentication codes via sms or on an authenticator app.
- Don't be lazy with passwords. They're the easiest way for intruders to get your information.
    - Beef up your passwords with combinations of symbols, letters, and numbers.
    - Never reuse passwords! Would you use the same key for everything you own?
    - Check your password's strength: https://howsecureismypassword.net/
    - Can't remember them? Use a password manager.
- Never use:
    - Any variation of the word "password" or "admin"
    - Your name or surname
    - Your partner's name or surname
    - Name or surname of any member of your family
    - Your pet's name
    - Birthdate or birth location
    - 12345, "qwerty" or "abcde"

- What kinds of information can your online accounts give hackers access to?
    - Email: Information about your accounts, confidential work and personal information
    - Social Media: Details about your preferences and views, your friends and family, vacation spots
    - Amazon: Items you've bought, wishlist items, even credit card and shipping details

PHONE

- Use antivirus on your phone as well as your computer.
- Turn your Wi-Fi and Bluetooth off when you don't use them.
- Never share passwords.
- Teach your family and friends what you know. They could share their viruses with you.
- Turn on your screen lock and use it at all times.
- Activate remote device locator for your smartphone and keep the option to track its location turned on.
- Back up your info and then perform a Factory Data Reset before you sell or give your phone away.