Cybersecurity Tonight: Resources

livingsecurity

Rings of Privacy

Public - ***in order of least private to most private***

- Resume
- Social media handles
- Relationships
- Your name

Less Protected - ***in order of least private to most private***

- Place of employment
- Pet names & family/friend names
- Salary information
- Email address
- Phone number

Somewhat Protected - ***in order of least private to most private***

- Home address
- Date of birth
- Employee number/ID

Most Protected - ***in order of least private to most private***

- Government ID
- Company files
- Passwords
- Customer information
- Banking information

Cybersecurity Tonight: Resources

“Talking Points” Notebook

Handwritten notes for reference in an interview for a Cybersecurity Episode

- Review password safety
- Passphrases are best - they’re long and strong - think movie quotes and song lyrics
- Don't share passwords with anyone
- Don’t reuse password - every account should have their own unique password
- Talk about password managers (they remember your passwords for you)
- MFA (multi-factor authentication) like text codes keep accounts extra secure

“I Have Ransomware” Article

Article by Cyber Safety explaining what to do after you get ransomware and how to identify ransomware.

Signifiers of what you may see on your ransomware screen...

- **Lock icons** are a common theme in ransomware screens; they show your files are encrypted or locked.
- **Pay with Bitcoin** options are almost always available; in fact, Bitcoin is the preferred currency in ransomware schemes because it’s harder to trace. Most won’t let you pay with a credit card or cash.
- The **countdown timer** is designed to make you panic. It adds a sense of urgency and encourages you to react immediately instead of thinking through your options.
- Many ransomware schemes threaten to **double the payment** if the ransom is not paid within a certain amount of time. This is another way to add urgency and make you panic.
- If you see a **Contact Us** button, it’s probably not a good idea to click it. You may end up giving away more personal information or making things worse on accident.
- Never copy, paste, or click on **unknown links** - there’s no telling what it might do, and the bad guys aren’t exactly trustworthy.

Cybersecurity Tonight: Resources

The Cyber Chronicles Article

5 Phishing Email Red Flags

- A forced sense of urgency (*Act NOW, Limited Time Offer!)*
- Misspellings in the email body or subject
- Phony website domains in sender address (*g00gle.com*)
- Suspicious attachments or links that disguise their location (*bit.ly, goo.gle*)
- Promises of financial benefits (*winning a prize, inheritance from unknown relatives*)

These are not the only things to watch out for, but looking out for these 5 red flags will definitely help you decide which emails are too risky to click on. When in doubt, report any suspicious activity by using the “Report phishing” button if it’s available or by notifying your security team in your email options menu. If you haven’t already, check in with your company and find out what phishing security policies should be followed for your work device.

Security Basics Checklist

Security Basics Checklist to remember:

- I have set my computer to install updates automatically
- I have set up my password manager and set a STRONG master password
- I have read the travel policy on working remote and understand I must use either the company-provided VPN or a personal hotspot
- I have installed the company-approved anti-virus software on my computer
- I have located the ‘Report-Phish’ button in my email
- I have changed the default passwords to my accounts
- I am ready to be a great cybersecurity ambassador

Cybersecurity Tonight: Resources

Web Article

Article from Cyber Safety explaining how physical security is cybersecurity.

Common cybersecurity missed include:

- Unlocked or unattended devices
- Sharing bags, keys, and login credentials
- Improperly disposed of documents
- Having sensitive conversations in public

When you walk away from a computer or workstation, lock the screen or log out. If a device isn't in your sights, it could be in someone else's. A password is only good at keeping people out if no one else knows it, so keep your credentials and ID badges to yourself. Not all threats are on purpose. Even accidental insider threats from well-meaning employees can be devastating.