Information Security Awareness 101

People, Cyber Space and Physical Space

People (you) hold a responsibility in securing your…

Cyber Space

- Social Media
- Passwords
- Cloud and Syncing
- Downloads

Physical Space

- Surroundings
- Laptop & mobile devices
- Your identity (PII)

- Social Engineering

Sharing on Social Media

Oversharing on social profiles can lead to strangers knowing where you are and other personal information you post.

- Take control of your profile privacy settings on each site and app.
- Sharing your location risks unwanted persons showing up with *unknown intentions.*
- Think twice before you decide to share a picture of a plane ticket, paycheck, or ID card.

Protecting your Password

****

It holds the key to your account, your identity.

- Create strong passwords with a mix of letters, numbers, and symbols.
  i.e. UN1vC4L!'16
- Never share your password, it creates *RISK* of others accessing your accounts and personal information.
- Lots of passwords? Use a trustworthy password vault to store them rather than writing them down.
- Add an extra layer of *protection* to your account by enabling two-factor authentication.

Cloud Safety and Syncing

The cloud can be somewhat of a mystery. What is it really? Someone else's computer, outside of your control (maybe even outside of the US), storing data for you.

- Auto syncing your phone to cloud storage poses a risk of data exposure -take control by choosing what you sync to the cloud.

- Be cautious of uploading sensitive or private info to cloud based apps and who you are sharing it with.
  i.e. Google drive, Evernote, Snapchat, etc.

Downloads

Take caution when downloading files.
Ask yourself -is it necessary? Does it pose a risk? Is it legal?

- *Don't* download apps from unknown sources.
- Do download updates for your antivirus software, operating system, and apps.
- Downloading illegally issued (textbooks, software, music) media can not only result in legal action but it may also contain a virus or worse.

Social Engineering

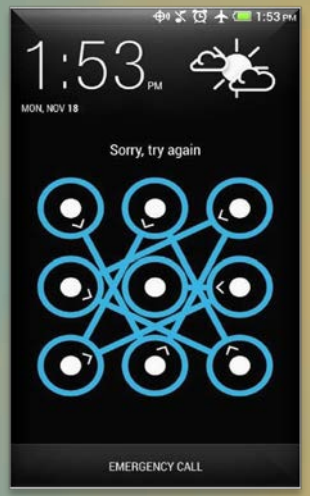
Phishing scams attempt to gain your personal information such as *account* information by appearing to be a trusted individual/source.

- *Be aware* of *who* is asking for your information and *why* they would need it.
- *Pay attention* to details such as the sender address and links by hovering over URLs to check if they are valid.
- Check your *surroundings*, you don't know who else is listening in on your conversation or looking over your shoulder.

Laptop and Mobile Devices

Your laptop and/or mobile device likely hold key information about you.

- Set Passwords and PINs on all your devices and turn auto screenlock on.
- Keep your device with you at *all* times, do not leave it lying around.
- Never leave your laptop unattended or in *plain sight* when you are not around.



Internet Safety Tips

General tips to keep in mind when online ☺

- When logging in or submitting info online, check for https:// in the URL to ensure it is a secure webpage.
- Be cautious when connecting to public WiFi networks. Cyber criminals can *track* anything you access and information used.
- Wait until you get home to share vacation pictures. *Don't* let criminals know that your home is empty.

Your identity (PII)

An important goal of Information Security is to protect your personally identifiable information (PII) -your identity.

- Keep documents with *personal information* *locked* up or shred them, *never* leave them in plain sight.
- Remember the tips covered in the previous slides, they're all about protecting YOU!