Basics of Online Privacy (Lesson 6 Handout)

Passwords

Risks:

- Weak passwords are easy to guess, short, and only have letters or numbers
- Re-used passwords are passwords that you use for more than one online service
- Passwords are often stored somewhere accessible, like written down or in an unsecured spreadsheet

Solutions:

- Two-factor authentication: username and password PLUS an email, phone call, or text verification
- Passphrases: words and spaces that are longer than normal passwords, but still easy to remember because they are goofy or memorable. Example: “The hedgehogs are making a ruckus!”
- Password Services
    - Browsers like Chrome and Firefox can store your passwords for you
        - Don’t save your passwords on computers you don’t own
    - Third-party (Lastpass.com)

Tracking

How companies can track what you do online (and what you can do)

Companies you gave permission to

- Those service agreements none of us read
    - What do do: read about how experts rate various terms of service to make a more informed choice: https://tosdr.org/ Also, consider that in some cases you can reject parts of the access they request and still use the service, though not always.
- Access to your phone - location services, access to photos, etc.
    - What do do: you can disable app access to your phone in the settings in your phone (iPhones: Settings>Privacy)

Companies you didn’t give permission to

- Any website or app we use is usually tracking what we do, how much time we spend, and where we go online. They do this with “cookies” which are little bits of text stored in your web browser and accessed by websites to see what you do and gather information to sell space to advertisers. Cookies do some positive things, like save you time by remembering your username and password or letting you go page-to-page without re-logging back in. They can even save your recently-viewed items and serve you more relevant advertising, but it does give companies a lot of information about where you are and what you’re doing when.
    - What do do: you can limit the websites that are allowed to save cookies and/or you can delete your cookies from time to time. Do this by going into your browser settings and looking for “cookies” or “content settings”

Hacking

How you can get hacked (and what you can do)

- “Social Engineering:” someone who seems trustworthy sends you an email asking you to visit the link to log into your account; the website is fake and it captures your username/password.
    - What do do: be suspicious of any email that asks you to follow a link to log in. You can look for suspicious aspects of the email address (slight misspelling or different domain name) or go straight to the site in question rather than clicking on the link.

- Keylogging software or hardware can get installed and record what keys you type and then send that information to hackers.
    - What do do: update your antivirus software, don't download unverified software, and consider using a password management service to avoid typing your passwords.
- Fake WiFi router or public WiFi router makes you vulnerable.
    - What do do: only connect to WiFi networks you trust and preferably have a password to access.
- Someone can guess the answers to your security questions to reset your password.
    - What do do: try not to use information that can easily be found online.
- The company gets hacked and your password is captured.
    - What do do: don't re-use passwords.
- You've used a common password and someone guesses it
    - What do do: don't use a common password! Top 25 last year were: 123456, password, 12345678, qwerty, 12345, 123456789, football, 1234, 1234567, baseball, welcome, 1234567890, abc123, 111111, 1qaz2wsx, dragon, master, monkey, letmein, login, princess, qwertyuiop, solo, passw0rd, starwars

Further Resources

https://www.internetsociety.org/blog/tech-matters/2015/01/four-basic-steps-protecting-your-digital-privacy-2015 - a good overview of the risks and some solutions for online privacy
https://howsecureismypassword.net/ - test how secure your password is
http://www.makeuseof.com/tag/7-ways-to-make-up-passwords-that-are-both-secure-memorable/ - ideas for creating secure passwords
https://tosdr.org/ - rates different sites and services according to what their terms of service ask you to agree to
https://www.consumer.ftc.gov/articles/0042-online-tracking - gives a good explanation of online tracking issues