Online Privacy Considerations
Part Two
Participants will:
- Consider the benefit of using tools to make your browsing experience faster and more secure with the benefits of greatest convenience
- Discuss best practices in password creation and use
- Play a jeopardy games to test their recall
- Help to make the world a better place by suggesting how cybersecurity principles might best be shared with students in school settings
Cookies?

- What is an electronic cookie?
Cookies

- Small files that your browser saves on your computer.
- They often include things like your login and password.
- Cookies can stay on your computer for months and may even record everywhere you go online.
- Watch the next video and come up with a list of Benefits and Risks of cookies
Cookies Anyone??

Watch this video and come up with a list of benefits and risks of cookies.

Video Source: https://www.youtube.com/watch?feature=player_embedded&v=JYCpiZKY30E
Password Development and Practices: Significant IT Security Vulnerabilities

THE WEAKEST LINK: YOUR PASSWORDS

With too many accounts and log-ins, users mostly tend to choose weak, easy to guess passwords, and rarely change passwords, hence placing themselves at risk from fraud and identity theft.

Your Password, the Weakest Link....

Users may use the same password, or a derivative of the same password for every account which makes them easy targets for hackers from 3rd party vendors.

"Credentials Used For Target Hack Reportedly Stolen From HVAC Vendor"  CONSUMERIST, February 5, 2014

The Problem: You want to protect yourself when you go online, but you also need to access your accounts, whether for work or for your personal life. But managing a gazillion unique and complicated passwords can deter you from getting anything done.

Images source: https://www.logmeonce.com/dangers-of-weak-password/
Passwords

- Passwords are a weak link in the computer security chain because they rely on us being good at something we find extremely difficult.
- Let’s assume you log onto many different websites on daily basis.
  - Do you use unique passwords for all your accounts?
  - Do you put your password in each time instead of allowing the browser to store it?
  - Do you change your passwords frequently?
  - Do you always use different character types such as uppercase and lowercase letters, numbers and punctuation?
  - If you can’t answer “yes” to these questions, you are an easy target for hackers.
Creating Secure Passwords: How do you do it?

Image source: http://www.technorms.com/14327/warning-secure-password-risk
A password is like a toothbrush

- Choose a good one
- Don't share it with anyone
- Change it occasionally
Secure Password Creation

Choose something that you can remember, but:

- Use letters and numbers
- Use a minimum of eight characters
- Don’t use personal information
- Don’t use dictionary words
- Use characters like brackets or asterisks
- Use a mixture of capital and lower case letters
- Use a sentence or song lyric and use only the first letters of the words
- Use different languages
Secure Password Use

- Never provide your username and password to someone who calls on the telephone or emails you
- Don’t keep a list of passwords printed out and posted in your home or in a little book called passwords
- Change your password if anyone finds out what it is
- Use different passwords for different accounts
- Change passwords frequently
- Don’t link accounts together
WHAT KIND OF DATA DOES GOOGLE COLLECT ON ITS USERS?

**Personal info**
Name, email address, telephone number, photo, everything shared on your G+ profile; Google synchronizes your info and contacts from all Google products into a single profile.

**Financial info**
Credit cards.

**Activity-related info**
Usage data, preferences, Gmail messages, photos, videos, browsing history, map searches, docs and other files hosted on Google; views and interactions with ads; log info; search queries; the date and time of your request and referral URL.

**Device info**
Device type and unique device identifier; phone number; calling party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.

**Location info**
GPS signals, location; sensor data from the device used that provides info on nearby Wi-Fi access points and cell towers.

**Interaction**
Keeps a record of all communications with you.

Image source:
https://www.rankranger.com/blog/duck-duck-go-google-privacy
What do search tools collect?

- **IP Address:** Your personal computer IP address can be traced back to you through a reverse DNS lookup with tools finding out not only your ISP but also your approximate location such as State or Province.

- **Date & Time:** The exact date and time you were searching for a certain keyword will be logged. The browser you use is normally also stored in search engines logs.

- **Query Terms:** The terms your searched for will be stored.

- **Cookie ID:** A unique code is embedded into the cookie and assigned to a particular computer by the search engine. It allows a search engine to learn if requests came from a particular computer, as long as that identifiable cookie is still stored in the browser Internet searches can be linked and traced back to you independently of what computer IP you use.

- **Not all search tools do track you though!!!
DuckDuckGo Doesn’t Track You

- Duck Duck Go

Video image: https://duckduckgo.com/about-video.html
Consider Using Disconnect

Source image: https://www.youtube.com/watch?v=L vem1Z66C7Q
Installing Disconnect

- Open Chrome
- Go to settings
- Extensions
- Get more extensions
- Search for disconnect
- Click on “Add to Chrome”
- Add extension
Look for Https on your browser

- Encryption allows information to be hidden so that it cannot be read without special knowledge (such as a password). This is done with a secret code or cypher. The hidden information is said to be encrypted.
- If you see https on your browser, the session between the web server and the browser on the mobile device you are using is encrypted. You can easily identify web servers that have https configured by looking at the Uniform Resource Locator (URL) in the web address bar of your browser.
Final Tips

- **Remember:**
  - NEVER CLICK ON LINKS in unsolicited email.
  - NEVER DOWNLOAD FILES from suspicious email.
  - NEVER GIVE OUT YOUR PASSWORD to anyone.

- **Consider**
  - Blocking cookies
  - Using extensions like disconnect to make the web faster and more secure
  - Searching with search tools that do not track you
Play GenCyber Privacy Jeopardy

Source: https://jeopardylabs.com/play/gencyber-privacy-jeopardy
How to spread Safe Computing Practices

- With a few others discuss how you think schools might best spread awareness of safe computing practices.
- Be ready to make suggestions to the larger group after small group sharing.