Internet Beyond Basics

Tips and tools for online security and privacy
Course Learning Objectives

By the end of class students will

• Know strategies for online account security
• Be familiar with privacy settings and how to clear browser data
• Know ways to identify phishing scams and malware
• Be able to change browser features and settings
Staying Secure Online

When using online accounts, it is important to use security measures to protect personal information. The more secure your accounts the less likely it is that your personal information will be compromised.
Creating Strong Passwords

- Use upper and lowercase letters
- Use numbers
- Use symbols
- Create a long password
- Use different passwords for each account
Strategies for Strong Passwords

• Try password "padding." To keep complexity and length but making a password memorable, try placing symbols in order at the beginning and ending of your password: [*]cAtL0v3r[*]
• Use the first letter of each word in a song lyric:
Password Generators

Password generators create complex strings of characters to be used as passwords for online accounts. These generated passwords do not contain words and are not easily guessed by computer hackers. Some good password generators include:

- Norton
- LastPass
- Web browsers including Edge, Firefox, and Chrome
Remembering Passwords

- Keep a written log of passwords and store it in a secure place.
- Use a digital password keeper.
  - Bitwarden
  - Norton
  - Myki
  - 1Password
Security Feature: Two Factor Authentication

- Account security requiring two of three types of information for access:
  - Something you **know**
    (e.g. password or PIN)
  - Something you **have**
    (e.g. ATM card or phone)
  - Something you **are**
    (e.g. fingerprint or voice print)

Definition and illustration from GCF Learn Free: [https://edu.gcfglobal.org/en/thenow/what-is-twofactor-authentication/1/](https://edu.gcfglobal.org/en/thenow/what-is-twofactor-authentication/1/)
Security Feature: Screen Lock

Screen locks are a security feature available on most smartphones. A screen lock allows you to set a password for your device preventing anyone else from accessing the information on your phone if it is lost or stolen. Lock screen options can include:

- **Passcodes** – mix of letters and numbers
- **PINs** – numbers
- **Patterns** – connecting dots in a specific order
- **Fingerprint, voice, or facial recognition**

Definition and illustration from LearnMyWay: [https://www.learnmyway.com/course-launcher/en-keeping-your-device-safe/v1/course-wrapper.html#/id/5c348959b95e7d69de8f92ce/](https://www.learnmyway.com/course-launcher/en-keeping-your-device-safe/v1/course-wrapper.html#/id/5c348959b95e7d69de8f92ce/)
Phishing Scams

Phishing scams are attempts to retrieve your personal information by posing as a trusted service or offering a reward. Phishing scams often come in the form of emails or social media messages that mimic legitimate messages.

Avoiding Phishing Scams

• Check the sender's email address for errors
• Review the content – is it asking for sensitive information?
• When in doubt, call the company directly to see if the email is legitimate
• Hover over links to see where they go

Let’s Take a Quiz

https://phishingquiz.withgoogle.com/
Malware

Malware can prevent your computer from working, cause frequent crashing, or even corrupt data. For malware to get onto your device, you must click on or download a malware file. Malware includes trojans, spyware, viruses, and ransomware.

Identifying Secure Sites

• Look for https
  – indicates the site is a secure site
  – data sent is encrypted
• Check your browser’s security symbol
• Use Google's Safe Browsing tool to see if a website is safe to visit: https://transparencyreport.google.com/safe-browsing/search

Secure example:

Insecure examples:
Staying Private Online

With many hidden trackers across websites, it can be difficult to know how to keep your activity online private. Today, we are going to look at some ways to take charge of your privacy online including:

• Managing browser settings
• Evaluating privacy policies
• Using privacy tools
Understanding Browser Data

• **History** – A list of webpages visited in the browser beginning with most recently visited webpages.

• **Cache** – Information on webpages, such as, logos or images, saved in your browser's memory for quicker loading times.

• **Cookies** – Small files that record activity on a website, such as, logging into an account. Some cookies are required for a website's features to work. Other cookies are used to track user behavior.

References:

https://techboomers.com/t/what-is-cache-browsing-history
https://techboomers.com/t/what-are-cookies
An essential part of digital decluttering is periodically clearing your browser's history, cache, and cookies to keep your browser running optimally. It also helps with online privacy and browser troubleshooting.
How to clear browser data

Step 1 - Access Settings in your browser
Step 2 - Look for Privacy/Security
Step 3 - Choose option to clear browsing data
Tips: Private Browsing

- **Incognito Mode** – Does not keep browsing history. Open settings in your browser and look for the option for opening a new window in Incognito or Private mode. This is especially important on a shared computer.
- **Browsers** – Try the Firefox or Brave browsers which offer strict privacy settings. Visit the settings page to view all the privacy options.
- **Search Engine** - Try DuckDuckGo instead of Google search. DuckDuckGo does not track your location or searches.
- **Privacy/Security Options** – Whatever browser or online account you use, review the Privacy/Security section to make adjustments that fit your privacy and security preferences.
- **Privacy Extensions** – Try a web browser extension to help block trackers. Some suggestions: Privacy Badger, DuckDuckGo Privacy Essentials
Reviewing Privacy Policies

• What information does the website require me to provide to use it?
• Does the website collect any information from me besides what is required to use it?
• Am I consenting to the website being able to collect information from me by using it?
• What reasons does the website give for collecting or requiring certain types of information?
• Does the website share, sell, or trade any of the information that it collects from me?

https://techboomers.com/t/privacy-policies
Reviewing Privacy Policies

• If the website shares, sells, or trades my information, with whom do they do so?
• When does the website release my information to anyone else?
• How long does the website keep any information that it collects from me?
• Does the website delete any information that they collect from me, or do they simply remove any parts of it that could personally identify me?
• Does the website allow third parties to collect information from me while I use their website?
Accessing Pop-Ups

• As a safety feature, browsers will block pop-up windows. Since many times pop-up windows are scams or simply annoying, this can be a good thing. In some instances, however, it may be necessary to access a pop-up window to complete an action.

• When you need a pop-up window that your browser has blocked, click on the alert by the address bar. Then, choose to allow/show the pop-up.
Customizing Browsers

• Set the homepage for your browser
• Set your default search engine
• Change the theme
• Explore Add-Ons or Extensions
Additional Resources

• Digital Learn
  – Online Scams https://www.digitallearn.org/courses/online-scams
  – Internet Privacy https://www.digitallearn.org/courses/internet-privacy

• GCF Learn Free
  – Safe Online Shopping https://edu.gcfglobal.org/en/internetsafety/safe-online-shopping/1/

• TechBoomers
  – Passwords https://techboomers.com/p/passwords

• Library Courses https://poudrelibraries.evanced.info/signup/
Questions? Comments?
Did we meet your needs?

• [https://www.surveymonkey.com/r/2021PRPLD](https://www.surveymonkey.com/r/2021PRPLD)
Thank-you for using

POUDRE RIVER PUBLIC LIBRARY DISTRICT