

Protecting Your Privacy Online

Lesson Plan

A competent computer user explores some options for protecting their privacy online.

Lesson Objectives

At the end of the class, the student will:

* Be able to install and use plugins to protect privacy.
* Understand online privacy risks and know a few simple tools to combat them.
* Know how to use proxies.
* Know how to download the tor browser.

Lesson Prep Work

(30 min, at a minimum, prior to student arrival)

* Get in early to test for technology failure, because it will happen :-)
* Pre-load videos or web demos
  + *“’60 Minutes’ probes data brokers and online tracking” -*https://www.youtube.com/watch?v=\_YffwdsnKXo
  + *“What is data encryption”* - https://www.youtube.com/watch?v=ySP-dvcOgas
* Print handouts

Lesson Prerequisites

● Must be a proficient computer user. Must be well versed with navigating the internet, downloading files, and installing software.

Lesson Outline

The lesson is completed in one (90) minute class session.

*(10)* Introduction

* Introduce instructor, students.
* Ask students at introduction: What are you hoping to get out of this class? What are good reasons to stay private online?
* Let students know it is okay to take phone calls, but ask them to put their phone on vibrate and answer calls outside the classroom.
* Inform students that they can sit back and watch if the class is too advanced.
* Inform students they can go to the bathroom, they don’t need permission.
* Show order in which class will happen. Explain scope of class.
* Discuss other related classes – such as Staying Safe Online and Protecting your Computer.
* (5) What is online Privacy?
  + *Explanation*
    - Online privacy is concerned with the storing, repurposing, and provision of your data to third-parties (data brokers, governments) and the display of information pertaining to oneself via the Internet. Privacy can entail either:
      * Personally Identifying Information: Information that can be used to identify an individual (age, physical address, etc.).
      * Non-Personally Identifying Information: Behavior of a site’s visitor.
    - Invasions of privacy can come from several sources:
      * External – ISPs, NSA, Data brokers, Hackers (with key loggers and backdoors).
      * Internal – Spouses, family members, people with physical access to the computer.
    - *Activity: watch “’60 Minutes’ probes data brokers and online tracking” (*[*https://www.youtube.com/watch?v=\_YffwdsnKXo*](https://www.youtube.com/watch?v=_YffwdsnKXo)*)*
* (15) Behaviors to protect your privacy online:
  + *Explanation*
    - The best way to protect your privacy online is to make good decisions about what information you reveal. There are a few easy behavioral steps you can take to protect your privacy online.
  + *Discussion: What pieces of information do people need to steal your identity?*
    - Name
    - Birth Date
    - Social Security #
  + Lie to websites:
    - You are not required (for most websites) to give truthful and honest information. You can set your birth date to something you’ll remember, like 1/1/1984.
    - You can also set up an alternate email that you use exclusively for signing up for junk accounts online (like forums, game sites, etc.). This will help keep your personal inbox free of clutter.
  + Know and Adjust your settings for social networking services and other websites (see Facebook Privacy and Security):
    - Do you know what information Facebook is sharing? By default you share with your friends. But maybe you only want to share certain photos with certain friends? Also, understand Facebook can adjust default sharing settings at any point in time.
    - Make sure you attend the Facebook: Privacy and Security class and learn how to adjust your settings.
    - Also, most account settings (for Facebook and beyond) can be adjusted via the gear icon (or down arrow) in the upper right hand corner of the website.
  + Passwords:
    - One of the easiest ways to protect your privacy is to create strong passwords.
    - *Discussion: What makes a strong password?*
      * Lots of characters
      * Lots of different types of characters (upper and lower case letters, numbers, and special characters).
      * Not using common words or phrases
      * Using a password manager like Keepass.
    - For more information, come to the Staying Safe Online class.
    - Teachers Tip: <https://xkcd.com/936/> It’s a comic, It’s so funny.
    - *Activity: Have class use howsecureismypassword.net to figure out how long it would take a desktop PC to crack a password similar to their own (remind them NOT to use their own password).*
* (15) Using Firefox and duckduckgo.com to protect your privacy:
  + *Explanation*
    - Beyond changing your behavior, there are a lot of software and web related options to help protect your privacy.
  + Get a good browser:
    - *Explanation*
      * Internet Explorer is notorious for having security holes, as well as not patching flaws in a reasonable time frame. You can avoid Internet Explorer entirely by downloading a different browser.
    - *Activity: Download Mozilla Firefox*
      * *Explanation*
        + We’ll be downloading Firefox, rather than Chrome, because it is open source (meaning anyone can look at the code), and is made by a non-profit corporation (rather than Google, who are also not particularly concerned with your privacy).
      * Step 1: Open Internet Explorer.
      * Step 2: Navigate to Google.com
      * Step 3: Type in Mozilla Firefox.
      * Step 4: Navigate to the following link: <http://www.mozilla.org/en-US/fir3efox/new/> (this should be the first result).
      * Step 5: Select Download.
  + Use Privacy mode in Mozilla Firefox:
    - *Explanation*
      * Mozilla Firefox comes with a feature called Privacy mode which will prevent information from being stored locally on your computer. This does not mean you are anonymous (you can still be tracked via your IP address – which is your computer’s and/or router’s specific “phone #”), but your search history, passwords, and cookies will not be saved on the local machine (this will protect your privacy from other people who use the same computer).
    - *Activity: Enable Privacy mode in Mozilla Firefox*
      * Step 1: Open up Firefox browser.
      * Step 2: Select Tools.
      * Step 3: Select “Start Private Browsing”
      * The hot key combination to create private window is CTRL+SHIFT+P
      * Point out how the Firefox menu button is now a masquerade picture (this means you are in privacy mode).
      * Google Chrome has an equivalent feature called Incognito mode (instructions for its use are in the handout).
  + Using an alternate search engine:
    - *Explanation*
      * Most people will automatically use Google.com to perform searches, but Google is a major data collector.
      * *Activity: Show* [*https://support.google.com/accounts/answer/54068?hl=en&rd=1*](https://support.google.com/accounts/answer/54068?hl=en&rd=1) *to illustrate what parts of your search Google records.*
    - *Activity: Teacher demos a series of searches with no context and class discusses.*
      * *Explanation*
        + Your search history can say a lot about you (sometimes too much). But oftentimes, people collecting your data have no context for your searches.
      * Step 1: Teacher opens up a word document.
      * Step 2: Teacher types in the following lines:
        + Best way to get away with murder.
        + How to kill someone without getting caught.
        + How to dispose of a body.
        + Kill my wife
    - *Discussion: What is the person who is performing the searches planning?*
      * Answer: He’s a writer for Cold case, a crime/mystery show.
      * NOTICE: There are other search engines that do not store your search data, like duckduckgo.com and startpage.com. They do rely on advertisements for funding, but they won’t target ads based on search history and clicked links.
    - *Activity: Use duckduckgo.com to perform a search and compare to Google’s results.*
      * Step 1: Open up Firefox.
      * Step 2: Type duckduckgo.com into the address bar.
      * Step 3: Perform a search for “Depression Symptoms” in duckduckgo.com
      * Step 4: Open up another tab and go to google.com and perform the same search.
    - *Discussion: What are the differences/similarities between these search results?*
      * They both have ads at the top!
      * Google provides a brief summary.
      * Most of the search results are the same (at least near the top).
      * Format and layout of search results is different.
* (15) Using browser plug-ins to ensure privacy browsing:
  + *Explanation*
    - Plug-ins add a specific feature to an existing software application.
    - You can add plug-ins to your current browser that can help protect your identity and ensure anonymity when online.
  + Ghostery
    - *Activity: Downloading and installing Ghostery*
      * *Explanation*
        + Ghostery will show who’s tracking you and will prevent websites and tracks from collecting user data on browsing habits. This is great for preventing data brokers from collecting information on your web browsing habits.
      * Step 1: Perform a duckduckgo.com search for Ghostery.
      * Step 2: Select ghostery.com (duckduckgo.com labels it as official site).
      * Step 3: Select “Download for Firefox” (this would say “Download for Chrome” if you were using the Chrome browser).
      * Step 4: Select “Install now” on the dialogue box.
      * Step 5: Read the Ghostery introduction page (as well as the next three pages). These explain what Ghostery does and how it works.
      * Step 6: On the third page, “Notification”, let students know that Ghostery will alert them when they are being tracked. They can turn off this notification here.
      * Step 7: On the “Blocking” page, let students know they can block all trackers to start with, but this may have “unintended effect[s] on the sites you visit.”
      * Step 8: Close out the Ghostery tab.
    - *Activity: Seeing Ghostery in action*
      * *Explanation*
        + At the beginning of class the video mentioned the nytimes.com website as a haven for trackers. Let’s test Ghostery out at nytimes.com and see who’s tracking us.
      * Step 1: Navigate to nytimes.com
      * Step 2: Point out the Ghostery icon in upper right hand side of browser window. Mine says “16” right now.
      * Step 3: Click on the Ghostery icon.
      * Step 4: Select “Close tutorial” (for now at least, when students get home and download Ghostery, encourage them to read through EVERYTHING).
      * Step 5: Click on the top tracker result (mine says “Audience Science”).
      * Step 6: Click on “Click here for more information about <insert tracker name>”
      * Step 7: Quickly read through the blurb on the next page and then close the tab.
      * Step 8: Block that specific tracker (use the slider next to each tracker).
  + HTTPS everywhere
    - *Activity: Downloading https everywhere*
      * *Explanation*
        + HTTPS everywhere, where applicable, will add https to any and all websites that support it (automatically, rather than the user having to do it themselves).
        + HTTPS is an encryption method widely used online to create a direct connection between your computer and the server of the website your are visiting (*metaphor: Like a tunnel linking two houses, rather than walking outside (in public) to visit*).
        + *Activity: Show video “What is data encryption” - https://www.youtube.com/watch?v=ySP-dvcOgas*
      * Step 1: Perform a duckduckgo.com search for HTTPS everywhere.
      * Step 2: Select [www.eff.org/https-everywhere](http://www.eff.org/https-everywhere) (duckduckgo labels this as the official site).
        + *Teachers Tip: It might be worth letting people know that the EFF is the Electronic Frontier Foundation and is a stellar organization known for defending people’s civil rights online.*
      * Step 3: Select “Install in Firefox.”
      * Step 4: Select “install now” on the dialogue box.
      * Step 5: Restart Mozilla Firefox (https everywhere requires that you restart the browser for it to be activated).
      * Step 6: Select the https everywhere icon in the upper right hand corner and point out the “disable HTTPS everywhere” option. This is in case HTTPS breaks certain sites.
      * Step 7: HTTPS everywhere may have popped up a few windows. Open these, read them, and close them down.
      * Keep an eye on the address bar for the https to appear on websites where it didn’t previously (by default, a lot of the sites we’ll be visiting today are already https enabled).
  + Honorable Mentions
    - No-script
      * *Explanation*
        + No Script Is another addon that can prevent malicious attacks and is useful for protecting not only your computer, but also your privacy from hackers and ne’er-do wells (it can prevent people from installing spyware / adware / keyloggers, etc. onto your machine using commonly used ).
        + No script can make browsing the web a bit of a pain, so use it only if you’re trying to be extra safe. Instructions for downloading it are in your handouts.
* (15) What is a proxy and how to use one
  + *Explanation*
    - Proxies, or a proxy server, are computers which serve as a hub through which internet requests are processed. When you connect to a website, your IP address shows up to them (metaphor: like caller ID), but if you have someone connect on your behalf, they only know the “caller ID” of the proxy server (not the IP address of your computer/router).
    - There are several types of Proxies:
      * Web based (like hidemyass.com and kproxy.com)
      * Downloadable (like privoxy)
      * VPN (virtual private networks – which we won’t talk about today)
    - The easiest one’s to use are hidemyass.com or kproxy.com
  + Using a Proxy website
    - *Activity*: *use a proxy website*
      * Step 1: Open up Firefox browser
      * Step 2: Go to hidemyass.com (or kproxy.com)
      * Step 3: Type in a website (like google.com)
      * NOTICE: The URL in the address bar (and also the format of the screen). The url might have something like, “http://kproxy.com/servlet...” rather than the typical google.com.
    - *Explanation*
      * The proxy service still knows your IP address (so it should be a service you trust, and also, most proxy services will cooperate with law enforcement if you do anything particularly illegal, so don’t).
      * Because using a proxy is like relaying a message through a middle man to another party, it will slow down your browsing experience.
    - *Explanation*
      * You can also download a proxy. One good one is privoxy (privoxy.org).
      * Privoxy is always active, but is difficult to initially set up (there is no GUI).
  + Downloading a Proxy
    - *Activity: Download Privoxy*
      * Step 1: Open up the Firefox Browser
      * Step 2: Go to privoxy.org
      * Step 3: Click download recent releases
      * Step 4: Point out the “looking for the latest version” (click on download Privoxy setup…)
      * Step 5: Install and run Privoxy
      * Notice “P” icon in system tools tray, this means Privoxy is running, but there’s still some set up to do.
        + *Teachers Tip: Recommend students write down these instructions if they’re at all interested in using Privoxy.*
    - *Activity: Set up Privoxy to work in Firefox*
      * Step 1: Open Firefox browser
      * Step 2: Click on Tools
      * Step 3: Click on Options
      * Step 4: Click on Advanced
      * Step 5: Click on the network tab
      * Step 6: Under connections, click on settings
      * Step 7: Click on Manual Proxy configuration
      * Step 8: Type in “localhost” under HTTP Proxy, and set the port to 8118.
        + *Metaphor: Computer ports work like a harbor. You have different ships that are coming and going and they use different ports. In this case, you’re saying I want to put the information I send out on the ship in port # 8118.*
        + *Teachers Tip: If anyone asks why port 8118, it’s because that port is meant specifically for proxies (Privoxy in particular) and won’t interfere with any other online functionality.*
      * You’re done! Celebrate!
      * Now Privoxy will prevent websites you visit from viewing your IP address (as best as it can) and it will also block advertisements – YAY!
* (10) Downloading Tor
  + *Explanation*
    - Tor is free software (It’s a browser) for enabling online anonymity. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than three thousand relays to conceal a user's location or usage (this works in the same way a proxy service does, but it is bundled with the browser).
    - Tor will slow down your internet browsing (and may make certain browsing very difficult). Use it only if you are very concerned about your online privacy. Tor is great general searches online, and also for making your browsing safer (from viruses and malicious attacks). It is not so great for watching videos or playing online games.
  + *Activity: Download the Tor browser*
    - Step 1: Navigate to duckduckgo.com.
    - Step 2: Type in Tor into the address bar.
    - Step 3: Select the first result ([www.torproject.org](http://www.torproject.org)).
    - Step 4: Select Download Tor from the main page.
    - Step 5: Select Download Tor browser.
    - Step 6: Save the file.
    - Step 7: Navigate to your download file.
    - Step 8: Run the executable file.
    - You should now have the Tor browser installed. The icon appears as an onion.
  + *Activity: Open the Tor browser*
    - Step 1: Double-click the Tor icon on the desktop. There is a startup screen for Tor where it connects to the Tor network, so it may take a while.
  + Discussion: What’s different about this browser?
    - By default, you go to startpage.com (which is like duckduckgo and doesn’t store your searches).
    - It takes a while to start up.
    - Step 2: Navigate to [www.youtube.com](http://www.youtube.com)
    - Step 3: Now wait… and wait some more.
    - Tor is slow for bandwidth heavy browsing.

**(5)** **Conclusion**

* Go over handout, review material, and emphasize contact info & further resources on handout.
* Any questions? Final comments?
* Remind patrons to come to second part of series for more in depth stuff.
* Remind to take survey.