Tips and Resources for Internet Security and Privacy

Written and Compiled by Kelly Hovinga

How often have you had this experience: after searching for an airline ticket to visit family, you open your computer screen to a flood of advertisements for airline tickets, hotel rooms, and car rentals? Have you ever noticed that your news feed for *The New York Times* is different than your spouse's, or your friend's? How about opening up your email to a mailbox full of spam? Have you ever used your GPS on your smartphone for directions only to have a notification ping on your screen asking you to upload a photo of yourself to the restaurant you just ate at? All these instances are examples of issues in personal internet security.

Companies use complex algorithms to track internet users' browsing habits. They then use these algorithms to target individuals for particular advertisements. If you recently searched for a house, Google might sell that information to a number of home security companies, or Bed Bath & Beyond, who will then start sending you spam.

This handout will provide you with a couple of measures to reduce the amount of information companies like Google and Facebook gather about you. With luck, you will see a distinct decrease in the amount of spam you receive on a daily bases.

- The first and most basic steps you can take to reduce the information companies have about you is to not sign into your browsing account, such as Google, or to switch to incognito mode. By not signing into your Google account, the company cannot link your browsing history to your personal account. Incognito mode keeps Google from tracking your browser history and linking it to your personal information.
    - If you are logged into your email account, log out before browsing the web.
    - Incognito mode in Google Chrome: You can access incognito mode by clicking the three vertical dots in the upper right corner of the browser window (see figure 1). Use the drop down menu to click on the "The New Incognito Window" option (see figure 2). By clicking on the option, a new window will open in Incognito mode (see figure 3), which allows you to search without google saving your browsing history or tracking your browsing habits for advertising.

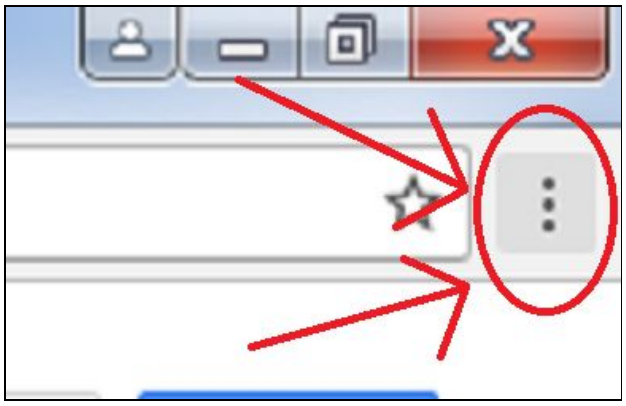

Figure 1

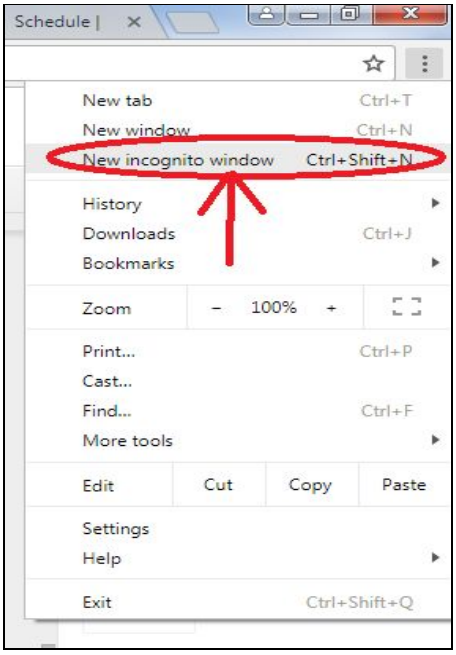

Figure 2

Figure 3

- Instead of searching using Google, you can use the search engines DuckDuckGo or StartPage. DuckDuckGo is a search engine that does not track your browsing history, while StartPage gives you Google search results while maintaining privacy protection. Another option is to download the software TOR. The software bounces internet

users' and websites' traffic through "relays," reducing companies' abilities to pinpoint your location or personal information to tie to your browsing habits.

- DuckDuckGo: https://duckduckgo.com/
- StartPage: https://www.startpage.com/
- TOR: https://www.torproject.org/

- Another option to secure your internet privacy is to use a browser plug in. A browser plug in allows you to use your normal search engine while still protecting your privacy. Two options we suggest are Ghostery and TrackMeNot. Ghostery sends a pop up window to your screen that tells you how many "trackers" are on a particular web page; a "tracker" being a company that is documenting your browsing history and connecting it to your personal information. Additionally, Ghostery blocks advertisements and their advertisers from tracking you (See figure 4). TrackMeNot on the other hand periodically issues false search leads, and thus feeds corporate trackers false information.
  - Ghostery: https://www.ghostery.com/
  - TrackMeNot: https://cs.nyu.edu/trackmenot/

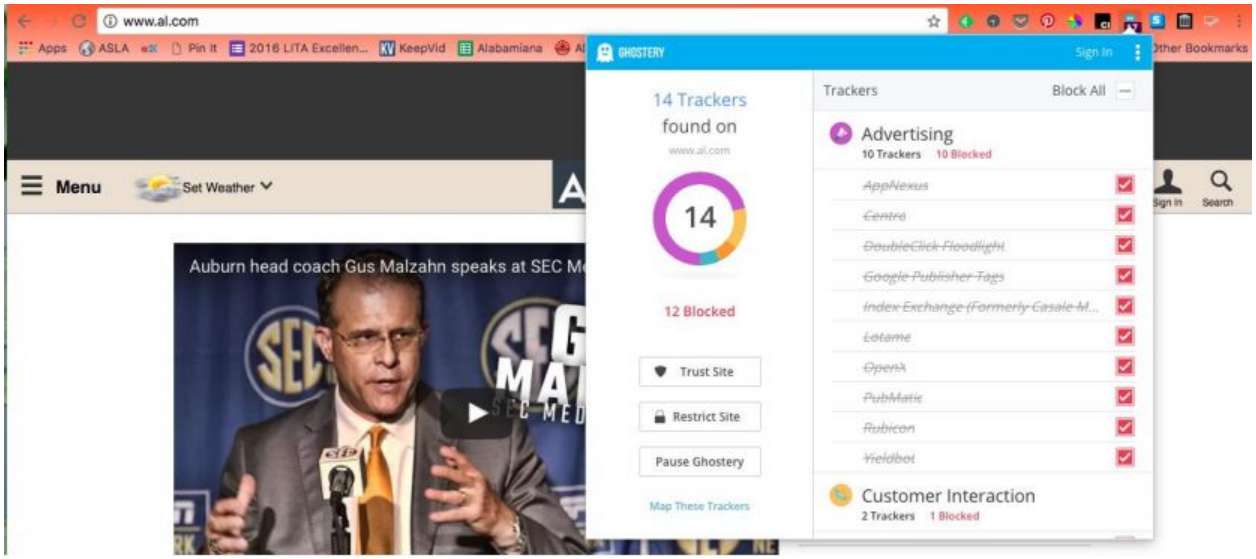

Figure 4.

- Companies track you on your smartphone as easily as they do on your computer, if not more so. There are a number of precautions to take when protecting your privacy on a smartphone. The first two are to turn off your GPS tracker when you are not expressly using it, and the other is to check the privacy settings on any apps you have on your phone. For example, even a popular, free flashlight app has access to your microphone and location information. Keep in mind, if an app is free, then the

company who created it has to be making money somewhere, and that is often through selling your personal information.

- There a number of apps you can use to protect your personal information on your phone. Ghostery and TrackMeNot both have app versions. Also, there is an app called Signal that encrypts your communication, including audio, and visual. That way, any apps that require access to your microphone will not be able to record your calls or use any pictures you take.
    - Signal iOS: https://itunes.apple.com/us/app/signal-private-messenger/id874139669?mt=8
    - Signal Android: https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=en
- If you have a yahoo email account, consider switching email providers. Yahoo email accounts have been hacked multiple times in the last five years and are highly insecure. If you wish to see if your email account has been hacked, you can check through the website Have I Been Pwned? If so, consider switching to a different email, such as ProtonMail. ProtonMail is a secure email provider that encrypts all of the hard code for your email and is accessible from your smartphone.
    - Have I Been Pwned?: https://haveibeenpwned.com
    - ProtonMail: https://protonmail.com/

Currently, internet browsing is a no-holds-barred field. There is no legislation limiting how browsers and internet providers can track you, no limitation on who they can sell your personal information, and no limitation on what companies can do with that personal information. Although there are laws limiting the sale of and sharing of medical and credit card information, there are loopholes around those laws. As such, it is in your best interest to limit how you can be tracked on the internet and how your information can be bought and sold.

*This list is derived from a webinar given by Wendy Stephens from Jacksonville State University called “Tools for Preserving Your Personal and Intellectual Privacy” given on July 20, 2017, and hosted by the University of Michigan.