UAW 2865 – Cybersecurity Guide

January 2017

By Zeke Trautenberg

1) *Web Browsers*

For browsing on your desktop, use **Firefox**. If you prefer to use Google Chrome, try the open source **Chromium** browser, which is based on Chrome. Always browse in "Private" or "Incognito" modes. For maximum anonymity, use the **Tor Browser**.

On your desktop browser, install Electronic Frontier Foundation's **HTTPS Everywhere** and **Privacy Badger** extensions to limit tracking of your browsing. The **Disconnect** extension is also a good tool.

For browsing on your phone, use **Firefox** mobile. For increased privacy, use **Firefox Focus**, which does not store cookies or search history.

Hot Tip: Adjust your browser's privacy and security settings on your desktop and phone. Make sure that "Do Not Track" settings are active and that your browser is storing minimal cookies. Clear your cache and search history often.

2) *Search Engines*

Use **Startpage** and **Ixquick** for increased privacy. **DuckDuckGo** is also a good option. You can add Startpage as an extension on Firefox. Follow these instructions to Startpage it to your Chrome or Chromium search box.

3) *Email*

Gmail neither free nor secure. The service scans your emails and sells your information to third-party advertisers. **ProtonMail** and **StartMail** are good options for a more secure email service. ProtonMail is based in Switzerland and StartMail is based in the Netherlands.

Use PGP (Pretty Good Privacy) protocol to encrypt your emails. To encrypt your emails with the Apple Email Client, use **GPG Tools**. You can use **Enigmail** with the **Thunderbird Email Client**.

4) *Messaging and Phone Calls*

Use the open-source app **Signal**, which is the standard for end-to-end encryption. You can also make secure phone calls. For information on their cryptographic key system works

see these instructions. Signal can also be installed on your desktop via the Chromium or Chrome browsers

5) *Passwords and Passcodes*

Use unique passwords. Make sure that they are long and include symbols. Alternatively, you can use password managers, but you can never be totally sure that they will not be hacked.

Turn on **two-factor verification** for your banking, email, and social media accounts. If you use Gmail, follow these instructions.

Hot Tip: Make sure that your passcode for your mobile device is at least six digits long. If you are going to a protest, disable the fingerprint reader.

6) *Virtual Private Networks*

When you use internet on campus or at cafés, the connection is often insecure. For more secure browsing, use a virtual private network or VPN, which creates a secure tunnel connection between your computer and server in the US or elsewhere. VPNs protect your identity by shielding your Internet Provider (IP) address and Domain Name Server (DNS). Use **NordVPN**, which is easy to install and headquartered in Panama.

7) *Additional Reading*

https://hackblossom.org/cybersecurity/

http://openpgp.org/software/