Staying Safe Online

By Matt Harmon, Jerry Michel, and Josh Heisler
October 4, 2018

Browsers

Google Chrome

- By far the most used browser in the world
- Clean, simple design
- Fast, stable, and secure
- Has MANY options for extensions

Mozilla Firefox

- Clean, simple design
- Fast, stable, and secure
- Has a lot of options for addons (not as many as Chrome
- Completely open source

Microsoft Edge

- Clean, simple design
- Fast, stable, and secure
- Cortana integration
- Best for battery life

Browser Extensions

There are many extensions that are great for security and privacy.

Adblock Plus

uBlock Origin

Search Engines

There are many search engines available to use nowadays. Here are a couple of our favorites.

Google.com

- The most used search engine in the world (Over 70% of worldwide searches use Google)
- Fast, accurate results
- Learns as you search to provide better results for you

Duckduckgo.com

- Very fast
- Completely private (Keeps no logs or information about you of any kind)
- Allows you to search thousands of other websites directly through duckduckgo.com

Passwords

Passwords are an *extremely* important part of the digital world. They help prove who you are and keep others from viewing your personal and confidential information. Don't take your passwords lightly. Here are a few tips to always remember:

- Use strong passwords for your accounts.
    - Passwords like "123456" and "password" are easy to remember but they're also incredibly easy for someone to hack.
    - Adding symbols is an easy way to make your passwords stronger (!,@,#,$,%, etc.).
- Don't use the same password for all of your accounts.
- Keep them written down or stored somewhere safe.
    - On a Google Drive sheet which is accessible anywhere
    - External hard drive or flash drive
    - Physically written in a notebook
    - In a password manager
- If you forget/lose your password or username, try recovering it before making a new account.
    - Most websites have a "Forgot your password?" or "Forgot your username?" link to help you recover your account.
    - Having multiple passwords, usernames, and emails written down for one account makes it much harder to remember your current login information.
    - If you end up having to change your username or password, write it down *immediately* and get rid of the old information.

Password Managers & Generators

Password managers store and manage all of your passwords in one secure place. Instead of remembering twenty different complex passwords you can just remember one "master" password and the manager does the rest. They come equipped with built in strong password generators to help keep your passwords more intricate. Here are a couple of our favorites.

LastPass **1Password**

Software

Antivirus

Antivirus software actively runs in the background of your computer looking for malware (viruses, spyware, adware, etc.). They typically scan sites as you visit them and files as you download them, trying to prevent malware from getting on your computer in the first place. These are your first line of defense. Below are two of the best free antiviruses you can get.

Avast Antivirus
www.avast.com/en-us/index

Kaspersky Free
www.kaspersky.com/free-antivirus

Outdated Software
Remove software on your computer that is no longer supported or updated.

Install New Software
Download programs and apps from trusted sites only. If it looks suspicious, it is better to be safe than sorry.

Updates
Keep your operating system, applications, add ons, and plugins up to date. There are serious security risks that could exist if your not up to date.

Avoid PUP - Potentially Unwanted Programs
When installing a new application, especially a free one, look for other applications that come with the program and be sure not to install those.

VPNs

What is a VPN?
Stands for “Virtual Private Network”

What do they do?
They add a layer of encryption protection when surfing the web on open and private networks.

Why use one?
They provide a way for you to access sensitive material safely (Banking, personal information). Keep Internet Provider and others from seeing your browsing history or other important information. People use them to geo-spoof their location to watch shows in locations they otherwise would not have access.

What to look for?
Does the VPN company log my browsing? What type of encryption is used? What countries are the servers offered? How many servers are offered? How much does it cost? How long is my purchase good for? What devices will this work on?

https://www.techradar.com/news/what-is-a-vpn
Here are a couple of our favorites.

NordVPN **NordVPN**

CyberGhostVPN

Miscellaneous

Backups
Make sure to backup your data regularly. You can back up to external hard drives or use a cloud based backup.

Make Sure Your Firewall Is Turned On
Whether you are running Windows or Mac OS, make sure your firewall is turned on. This may also be controlled by your antivirus software

Facebook
Beware of fake accounts and what your privacy settings are at for your account

Auto Lock Or Auto Log Out
Turn these settings on or keep them on especially if you use a laptop or mobile device and travel. This can help keep unwanted eyes from seeing or finding out your personal information.

Fake Email Accounts & Popups
Never call the number listed in an email or popup. Microsoft will not email or call you. The emails often will look legit, but are more often than not a scam. These companies look to remote in and mess your computer up so they can “fix” it for a “small” fee. Sometimes these can range up to $250.