WhatDoIDoAboutTrump.com
DIGITAL SECURITY CHECKLIST

You're worried. We want to help.

Digital security can seem complicated. At WhatDoIDoAboutTrump.com, we are hearing from folks who want to know if they are doing everything they can to protect themselves. Our volunteers have worked with several digital security experts to create this guide to answer just that question. These basic steps can help, whether you are worried about trolls, online harassment, or an overreaching government.

Please remember that the internet still presents risk, even if you practice these habits. This list is a consolidated starting point for mitigating your risk. Try to learn more about digital security via our online resource library!

COMMON THREATS

Hacking

Strategies (including those at right) to gain unauthorized access to computer systems.

Ransomware

A type of malware that locks you out of your computer until you pay the source.

Phishing

Deceiving users into revealing information, often by posing as legitimate.

Malware

Unwanted programs that spy on you, hinder operations, or cause other harm.

PREVENTION HABITS

Keep personal details off the web - most hackers use personal relationships, public wifi, or the techniques above to guess your passwords and access your accounts.

Be careful what you download, and scan your computer regularly.

Hover over URLs before clicking on them to check the link.

Always consider e-mail insecure! Never send passwords, credit card #s, or other important info. Avoid logging into sites via an email. Go directly to the URL instead.

Watch out for e-mails with "urgent action" pleas, or redirects to fake websites.

Know what your privacy settings are on social media!

What a Trump Administration means for web security.

Realistically, it is hard to say. The government's ability to conduct surveillance on US citizens has grown dramatically over the previous two administrations, and Trump will inherit that expanded apparatus.

Trump has supported surveillance of Mosques and expressed comfort with the NSA's discontinued bulk phone call metadata collection program. He will be able to undo executive orders Obama used to constrain the NSA and refocus surveillance efforts. Some Silicon Valley companies have expressed a concern that Trump's Department of Justice will put more pressure on companies to release data to law enforcement, which could be another risk to citizens using mainstream, unencrypted software.

See the security tips that can get you started on the next page.

Made by volunteers. Got feedback? Want more? Ask for **Micah** at WhatDoIDoAboutTrump@gmail.com

WhatDoIDoAboutTrump.com

DIGITAL SECURITY CHECKLIST

Easy! Everyone should do it. **Takes work,** but worth it. **Advanced.** Only if you're really worried.

?	!	Action	Resources & Tips
PASSWORDS	🟢	☐ Password protect every device you own	The #1 way to get hacked is using passwords across accounts!
	🟢	☐ Passwords use a diverse set of 10+ characters	Generate passwords with Diceware or a password generator
	🟠	☐ Use a different password on every site	LastPass and KeePass are free password managers
	🟠	☐ Enable two-factor authentification	Authy sets up two-factor authentication with your phone
WEB BROWSING	🟢	☐ Avoid public/open Wi-Fi	Open networks are vulnerable to hackers and data thieves
	🟢	☐ Stop using Internet Explorer	These days, IE is less secure and buggier than other browsers
	🟢	☐ Use HTTPS (in the web address) if available	The HTTPS Everywhere extension automates using HTTPS
	🟢	☐ Turn off Flash and Java browser plug-ins	Learn why and how in this article
	🟢	☐ Turn off Geotagging on all devices	Learn why and how in this article
	🟠	☐ Prevent cookies from being logged	Extensions like Privacy Badger or Disconnect.me can do this
	🟠	☐ Scan for and prevent malware intrusions	uBlock Origin blocks it, while Malwarebytes can scan for it
	🔴 $	☐ Use a Virtual Private Network for encryption. Only encrypted traffic (VPN, HTTPS) is private.	Consider Cloak for Mac and SurfEasy for PC. iPhones have an app, "VPN." On Androids get OpenVPN.
	🔴	☐ Use an anonymous web browser like Tor. Tor encrypts your data, connects you anonymously, and obscures your location. Few (but some) alternatives exist.	Tor is anonymous, but not private. Avoid downloads or using Tor on sites that reveal your identity (i.e. a log in). "Eavesdroppers" can see you use Tor - just not your content.
E-MAIL & TEXTS	🟢	☐ Check "haveibeenpwned.com" to see if you're at risk	They will run your e-mail against a database of exposed accounts
	🟠	☐ Encrypt cell phone calls, texts, and videos. SMS can rarely be encrypted with pre-installed programs. iMessage is the exception.	Signal encrypts (only with other Signal users). Also encrypted are Knox, WhatsApp, iMessage and Telegram - some collect user data. For video, Jitsi Meet, Facetime and Talky.
	🟠 $	☐ Use private e-mail systems. Free e-mail systems sell your info to advertisers or the government.	Hushmail (free) and Startmail ($60/year) don't sell your information. PGP is the standard protocol.
SOFTWARE & STORAGE	🟢	☐ Turn on automatic software updates wherever you	Let the experienced folks keep your systems secure!
	🟢	☐ Back up your files locally (i.e. not just on the cloud)	Use an external hard drive. No sensitive info in the cloud.
	🟢	☐ Routinely empty your "Trash" folders	Understand how files are deleted - it can be complicated!
	🟠	☐ Encrypt Cloud-stored data	Do your research - lose your password, you lose your files!
	🟠	☐ Encrypt your hard drives	Use FileVault for Mac, BitLocker for Windows. iPhones are automatically encrypted - Androids can easily be encrypted
	🔴	☐ Use an encrypted operating system	Tails automates traffic through Tor, e-mail through PGP, and contains no personal identifyng info. Qubes is also good.