Protect your privacy during turbulent times—a hacker's guide to being cyber-safe

December 8 2016, by Timothy Summers

Credit: AI-generated image (disclaimer)

Protecting individual privacy from government intrusion is older than American democracy. In 1604, the attorney general of England, Sir Edward Coke, ruled that a man's house is his castle. This was the official declaration that a homeowner could protect himself and his privacy from the king's agents. That lesson carried into today's America, thanks to our

Founding Fathers' abhorrence for imperialist Great Britain's unwarranted search and seizure of personal documents.

They understood that everyone has something to hide, because human dignity and intimacy don't exist if we can't keep our thoughts and actions private. As citizens in the digital age, that is much more difficult. Malicious hackers and governments can monitor the most private communications, browsing habits and other data breadcrumbs of anyone who owns a smartphone, tablet, laptop or personal computer.

President-elect Donald Trump's criticism of encryption technology and interest in expanding government surveillance have technologists and civil libertarians deeply concerned.

As an ethical hacker, my job is to help protect those who are unable, or lack the knowledge, to help themselves. People who think like hackers have some really good ideas about how to protect digital privacy during turbulent times. Here's what they – and I – advise, and why. I have no affiliation or relationship with any of the companies listed below, except in some cases as a regular user.

Phone calls, text messaging and email

When you're communicating with people, you probably want to be sure only you and they can read what's being said. That means you need what is called "end-to-end encryption," in which your message is transmitted as encoded text. As it passes through intermediate systems, like an email network or a cellphone company's computers, all they can see is the encrypted message. When it arrives at its destination, that person's phone or computer decrypts the message for reading only by its intended recipient.

For phone calls and private text-message-like communication, the best

apps on the market are WhatsApp and Signal. Both use end-to-end encryption, and are free apps available for iOS and Android. In order for the encryption to work, both parties need to use the same app.

For private email, Tutanota and ProtonMail lead the pack in my opinion. Both of these Gmail-style email services use end-to-end encryption, and store only encrypted messages on their servers. Keep in mind that if you send emails to people not using a secure service, the emails may not be encrypted. At present, neither service supports PGP/GPG encryption, which could allow security to extend to other email services, but they are reportedly working on it. Both services are also free and based in countries with strong privacy laws (Germany and Switzerland). Both can be used on PCs and mobile devices. My biggest gripe is that neither yet offers two-factor authentication for additional login security.

Avoiding being tracked

It is less straightforward to privately browse the internet or use internet-connected apps and programs. Internet sites and services are complicated business, often involving loading information from many different online sources. For example, a news site might serve the text of the article from one computer, photos from another, related video from a third. And it would connect with Facebook and Twitter to allow readers to share articles and comment on them. Advertising and other services also get involved, allowing site owners to track how much time users spend on the site (among other data).

The easiest way to protect your privacy without totally changing your surfing experience is to install a small piece of free software called a "browser extension." These add functionality to your existing web browsing program, such as Chrome, Firefox or Safari. The two privacy browser extensions that I recommend are uBlock Origin and Privacy Badger. Both are free, work with the most common web browsers and

block sites from tracking your visits.

Encrypting all your online activity

If you want to be more secure, you need to ensure people can't directly watch the internet traffic from your phone or computer. That's where a virtual private network (VPN) can help. Simply put, a VPN is a collection of networked computers through which you send your internet traffic.

Instead of the normal online activity of your computer directly contacting a website with open communication, your computer creates an encrypted connection with another computer somewhere else (even in another country). That computer sends out the request on your behalf. When it receives a response – the webpage you've asked to load – it encrypts the information and sends it back to your computer, where it's displayed. This all happens in milliseconds, so in most cases it's not noticeably slower than regular browsing – and is far more secure.

For the simplest approach to private web browsing, I recommend Freedome by F-Secure because it's only a few dollars a month, incredibly easy to use and works on computers and mobile devices. There are other VPN services out there, but they are much more complicated and would probably confuse your less technically inclined family members.

Additional tips and tricks

If you don't want anyone to know what information you're searching for online, use DuckDuckGo or F-Secure Safe Search. DuckDuckGo is a search engine that doesn't profile its users or record their search queries. F-Secure Safe Search is not as privacy-friendly because it's a

collaborative effort with Google, but it provides a safety rating for each search result, making it a suitable search engine for children.

To add security to your email, social media and other online accounts, enable what is called "two-factor authentication," or "2FA." This requires not only a user name and password, but also another piece of information – like a numeric code sent to your phone – before allowing you to log in successfully. Most common services, like Google and Facebook, now support 2FA. Use it.

Encrypt the data on your phone and your computer to protect your files, pictures and other media. Both Apple iOS and Android have settings options to encrypt your mobile device.

And the last line of privacy defense is you. Only give out your personal information if it is necessary. When signing up for accounts online, do not use your primary email address or real phone number. Instead, create a throw-away email address and get a Google Voice number. That way, when the vendor gets hacked, your real data aren't breached.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Protect your privacy during turbulent times—a hacker's guide to being cyber-safe (2016, December 8) retrieved 21 May 2024 from https://phys.org/news/2016-12-privacy-turbulent-timesa-hacker-cyber-safe.html