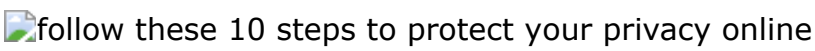
How to Protect Your Online Privacy: A Practical Guide

By John Mason • TechNewsWorld • ECT News Network

Print
Email



Do you take your online privacy seriously?

Most people don't. They have an ideal scenario of just how private their online activities should be, but they rarely do anything to actually achieve it.

The problem is that bad actors know and rely on this fact, and that's why there's been a steady rise in identity theft cases from 2013 to 2017. The victims of these cases often suffer a loss of reputation or financial woes.

If you take your online privacy seriously, follow this 10-step guide to protect it.

1. Beware of Internet Service Providers

You may not be aware of it, but your ISP already might know all about your online searches.

Each time you search for something online, your browser sends a query to a DNS server. Before the query reaches a DNS server, however, it first has to go through your ISP. Needless to say, your ISP easily can read and monitor these queries, which gives it a window into your online activity.

Not all ISPs monitor your browser queries but the ones that don't are the exception and not the rule. Most ISPs will keep records of your Web browsing for a period of a few months to a year. Most ISPs don't record your texts, but they do keep records of who texted you.

There are two ways to protect your privacy if you don't want your ISP monitoring your browser queries: 1) Switch to an ISP that doesn't monitor your online data, if practicable; or 2) Get a VPN to protect your data (more on this later).

2. Strengthen and Protect Your Login Credentials

One thing most people take for granted is the login credentials they use to access their many online accounts. Your username and password are the only things keeping your information and privileges from getting into the wrong hands. This is why it's important to make them as strong as possible.

Choose a strong username that is simple and easy to remember but can't easily be linked to your identity. This is to prevent hackers from correctly guessing your username based on your name, age, or date of birth. You'd be surprised just how cunningly hackers can find this information. Also, never use your Social Security Number as your username.

Next, pick a strong password. There are many ways to do this, but we can narrow them down to two options: 1) Learn how to make strong passwords; or 2) Use a password manager app.

Learning how to make a strong password requires time and imagination. Do you want to know what the most common passwords are? They are "1234," "12345," "0000," "password" and "qwerty" -- no imagination at all. A password combining your name and date of birth won't cut it. Nor will a password that uses any word found in the dictionary.

You need to use a combination of upper and lower case letters, numbers, and even symbols (if allowed). Complexity is what matters, not length, since a complex password will take centuries for a computer to figure out. In fact, you

can try your password if you want to see just how long it will take to crack.

If you don't have the time and imagination to formulate a strong and complex password, you can use one of the six best password managers. These apps not only save you the hassle of memorizing your complex passwords but also auto-fill online login forms and formulate strong passwords for you.

Whether you want to learn how to make strong passwords or choose to install a password manager app is up to you. What you should never neglect, though, is 2FA (2-factor authentication). 2FA adds an extra layer of protection for your passwords in case someone ever does learn what they are. In fact, you may already have tried it when logging into an account on a new device.

The app or service requires you to key in the access code sent to another one of your devices (usually your phone) before you are given access to your account. Failing to provide this access code locks you out of your account. This means that even if hackers obtain your login credentials in some way, they still can't log into your account without the access code.

Never use the same usernames or passwords for different accounts. This prevents hackers from accessing multiple accounts with just one or more of your login credentials. Also, never share your login credentials with anybody --not even your significant other.

3. Check the WiFi You're Using

Have you ever heard of a KRACK attack? It's a proof-of-concept cyberattack carried out by infiltrating your WiFi connection. The hacker then can steal information like browsing data, personal information, and even text message contents.

The problem is that not even WPA2 encryption can stop it. This is actually why The WiFi Alliance started development of WPA3, which it officially introducedthis summer.

Do you need WPA3 to defend against KRACK attacks? No. You just need to install security updates when they become available. This is because security updates ensure that a key is installed only once, thereby, preventing KRACK attacks. You can add additional layers of protection by visiting only HTTPS sites and by using a VPN.

You also can use a VPN to protect your device whenever you connect to a public network. It prevents hackers from stealing your information via a MitM (Man in the Middle) attack, or if the network you've connected to is actually a rogue network.

4. Watch Your Browser

If you read through your browser company's Terms of Use and Privacy Policy, you might find that they actually track your online activities. They then sell this information to ad companies that use methods like analytics to create a profile for each user. This information then is used to create those annoying targeted ads.

How do they do this?

Answer: Web cookies.

For the most part, Web cookies are harmless. They're used to remember your online preferences like Web form entries and shopping cart contents. However, some cookies (third-party cookies) are made specifically to remain active even on websites they didn't originate from. They also track your online behavior through the sites you visit and monitor what you click on.

This is why it's a good idea to clear Web cookies every once in a while. You may be tempted to change your browser settings to simply reject all cookies, but that would result in an overall inconvenient browsing experience.

Another way to address the monitoring issue is to use your browser's Incognito mode. Your browser won't save any visited sites, cookies, or online forms while in this mode, but your activities may be visible to the websites you visit, your employer or school, and your ISP.

The best way I've found so far is to replace your browser with an anonymous browser.

One example is TOR (The Onion Browser). TOR is a browser made specifically to protect user privacy. It does this by

wrapping your online data in several layers of encryption and then "bouncing" it for the same number of times before finally arriving at the right DNS server.

Another example is Epic Browser. While this browser doesn't run on an onion network like TOR, it does do away with the usual privacy threats, including browsing history, DNS pre-fetching, third-party cookies, Web or DNS caches, and auto-fill features. It automatically deletes all session data once you close the browser.

SRWare Iron will be familiar to Google Chrome users, since it's based on the open source Chromium project. Unlike Chrome, however, it gets rid of data privacy concerns like usage of a unique user ID and personalized search suggestions.

These three are the best ones I've found, but there are other alternatives out there. Whatever privacy browser you choose, make sure it's compatible with your VPN, as not all privacy browsers are VPN-compatible -- and vice-versa.

5. Use a Private Search Engine

Presenting risks similar to popular browsers are the search engines many people use. Most browser companies also produce their own search engine, which -- like the browser -- also tracks your online searches. These searches then can be traced to your personal identity by linking them to your computer, account, or IP address.

Aside from that, search engines keep information on your location and usage for up to several days. What most people don't know is that persons in the legal field actually are allowed to use the information collected by search engines.

If this concerns you at all, you may want to switch to a private search engine. These private search engines often work in the same way: They obtain search results from various sources, and they don't use personalized search results.

Some of the more popular private search engines include DuckDuckGo, Fireball, and Search Encrypt.

6. Install a VPN

What is a VPN, and why do I strongly recommend it?

A VPN (virtual private network) is a type of software that protects your Internet browsing by encrypting your online data and hiding your true IP address.

Since you already know how online searches are carried out, you already know that browser queries are easily readable by your ISP -- or anyone else, for that matter. This is because your online data is, by default, unencrypted. It's made up of plain text contained in data packets.

You also already know that not even built-in WPA2 encryption is good enough to protect against certain attacks.

This is where a VPN comes in. The VPN courses your online data through secure tunnels until it gets to its intended DNS server. Anyone intercepting your browsing data will find unreadable jargon instead.

You may hear advice against trusting VPNs with your security. I'm actually inclined to partially agree -- not all VPNs are secure. However, that doesn't mean all VPNs are not secure.

The unsecured VPNs I'm referring to are the "free lunch" types that promise to be free forever but actually use or sell your data to ad companies. Use only the safest VPN services you can find.

A VPN is primarily a security tool. While you may enjoy some privacy from its functions, you will want to pair it with a privacy browser and search engine to get the full privacy experience.