Online Privacy: Using the Internet Safely

Posted: Jul 01 1995 | Revised: Jan 16 2019

1. Online Tracking

Almost every major website you visit tracks your online activity. Tracking technology can follow you from site to site, track and compile your activity, and compile all of this into a database. Generally, tracking utilizes a numerical identifier, rather than your real name. This information is used to personalize the content that you see online.

The good news is that almost all browsers give you some control over how much information is revealed, kept and stored. Generally, you can change the settings to restrict cookies and enhance your privacy. Most major browsers now offer a "Private Browsing" tool to increase your privacy. However, researchers have found that "Private Browsing" may fail to purge all traces of online activity.

Most browsers also provide a Do Not Track (DNT) setting. DNT is a way to keep your online activity from being followed across the Internet by advertisers, analytics companies and social media sites. When you turn on the DNT setting in your browser, your browser sends a special header to websites requesting that don't want your activity tracked. Unfortunately, honoring the DNT setting is voluntary. Individual websites are not required to respect it. While a few websites will honor DNT, most websites will ignore your preference.

Some of the tools that are used to track you online include cookies, flash cookies, and fingerprinting.

Cookies. When you visit different websites, many of the sites deposit data about your visit, called "cookies," on your hard drive. Cookies are pieces of information sent by a web server to a user's browser. Cookies may include information such as login or registration identification, user preferences, online "shopping cart" information, and so on. The browser saves the information, and sends it back to the web server whenever the browser returns to the website.

The web server may use the cookie to customize the display it sends to the user, or it may keep track of the different pages within the site that the user accesses.

For example, if you use the internet to complete the registration card for a product, such as a computer or television, you generally provide your name and address, which then may be stored in a cookie. Legitimate websites use cookies to make special offers to returning users and to track the results of their advertising. These cookies are called **first-party cookies**. However, there are some cookies, called **third-party cookies**, which communicate data about you to an advertising clearinghouse which in turn shares that data with other online marketers. These third-party cookies include "tracking cookies" which use your online history to deliver other ads. Your browser and some software products enable you to detect and delete cookies, including third-party cookies.

Disconnect is a browser extension that stops major third parties from tracking the webpages you go to. Every time you visit a site, Disconnect automatically detects when your browser tries to make a connection to anything other than the site you are visiting. You can also opt-out of the sharing of cookie data with members of the Network Advertising Initiative.

Flash cookies. Many websites utilize a type of cookie called a "flash cookie" (sometimes also called a "supercookie") that is more persistent than a regular cookie. Normal procedures for erasing standard cookies, clearing history, erasing the cache, or choosing a delete private data option within the browser will not affect flash cookies. Flash cookies thus may persist despite user efforts to delete all cookies. They cannot be deleted by any commercially available anti-spyware or adware removal program. However, if you use the Firefox browser, there is an add-on called Better Privacy that can assist in deleting flash cookies.

Fingerprinting. A device fingerprint (or machine fingerprint) is a summary of the software and hardware settings collected from a computer or other device. Each device has a different clock setting, fonts, software and other characteristics that make it unique. When you go online, your device broadcasts these details, which can can be collected and pieced together to form a unique "fingerprint" for that particular device. That fingerprint can then be assigned an identifying number, and used for similar purposes as a cookie.

Fingerprinting is rapidly replacing cookies as a means of tracking. Tracking companies are embracing fingerprinting because it is tougher to block than cookies. Cookies are subject to deletion and expiration, and are rendered useless if a user decides to switch to a new browser. Some browsers block third-party cookies by default and certain browser add-ons enable blocking or removal of cookies.

Unlike cookies and flash cookies, fingerprints leave no evidence on a user's computer. Therefore, it is impossible for you to know when you are being tracked by fingerprinting.

You can test your browser to see how unique it is based on the information that it will share with the sites that you visit. Panopticlick will give you a uniqueness score, letting you see how easily identifiable you might be as you surf the web.

Unfortunately, fingerprinting is generally invisible, difficult to prevent, and semi-permanent. There's no easy way to delete fingerprints that have been collected. Computer users determined to prevent fingerprinting can block JavaScript on their computer. However, some parts of a website (for example, video and interactive graphics) may not load, resulting in a blank space on the webpage.

One way to block JavaScript is to use the Firefox browser with the "add-on" program called NoScript. The combination of Firefox and NoScript can stop JavaScript on websites. Disabling JavaScript stops many forms of browser fingerprinting, because it prevents websites from detecting plugins and fonts, which are necessary to effectively fingerprint a device.

Cross-device tracking. Cross-device tracking occurs when companies try to connect a consumer's activity across their smartphones, tablets, desktop computers, and other connected devices. The goal of cross-device tracking is to enable companies to link a consumer's behavior across all of their devices. While this information serves many purposes, it is particularly valuable to advertisers.

To engage in cross-device tracking, companies use a mixture of both "deterministic" and "probabilistic" techniques. The former can track you through an identifying characteristic such as a login. The later uses a probabilistic approach to infer which consumer is using a device, even when a consumer has not logged into a service.

For example, a company called BlueCava is able to identify and track users online across multiple devices. They can associate multiple devices to the same person or household, by attaching an IP address to a BlueCava identifier and by recognizing and collecting information about the various computers, smartphones, and tablets that people use to connect the internet. Thus, your behavior on one device can be associated with other devices from both your home and office. This information can be very valuable for marketing purposes.

BlueCava's technology enables them to recognize computers and devices by collecting information about your screen type, IP address, browser version, time zone, fonts installed, browser plug-ins and various other properties of your screen and browser. This information is put into a "snapshot" and is sent to their servers to create a unique ID for every browser and to "match" the snapshot to the snapshots they receive from their marketing partners. When they use snapshots to create a unique ID, they are also able to group related screens into "households" based on common characteristics among the snapshots, such as IP addresses. BlueCava allows you to opt out of tracking.

If you are interested in some of the more technical aspects of online tracking, the Princeton Web Census measures cookie-based and fingerprinting-based tracking at one million websites and evaluates the effect of browser privacy tools.

2. Mobile Apps

If you use a smartphone or other mobile device to access the Internet, chances are that you may be using mobile applications (apps) rather than an Internet browser for many online activities. An app is a program you can download and access directly using your mobile device. There are hundreds of thousands of apps available, including numerous free or low-priced choices. Unfortunately, apps can collect all sorts of data and transmit it to the app-maker and/or third-party advertisers. This data may then be shared or sold.

Some of the data points that an app may access from your smartphone or mobile device include:

- your phone and email contacts
- call logs
- internet data
- calendar data
- data about the device's location
- the device's unique IDs
- information about how you use the app itself

Many apps track your location. There are location-based services like Yelp and Foursquare that may need your location in order to function properly. However, there are also apps (such as a simple flashlight) that do not need your location to function and yet still track it.

Smartphones and other mobile devices may ask you for specific permissions when you install an app. Read these and think about what the app is asking for permission to access. Ask yourself, "Is this app requesting access to only the data it needs to function?" If the answer is no, don't download it. Learn where to go on your particular phone to determine what you will allow the app to access, and if you are at all suspicious do more research on the app before you download.

Mobile apps generally do not provide ad networks with the ability to set a cookie to track users. Instead, ad networks may use your phone's mobile advertising identifier. These identifiers have different names depending on the brand of your phone. For example, on Android devices they are called Google Advertising ID. On iOS, they are called Identifiers for Advertisers. You can find your device's options to set an opt-out flag using these instructions.

3. Privacy Policies

One way to protect your privacy online is to understand how a site or app will use and share your personal information. Websites and apps generally provide this information in their

privacy policy.

California's Online Privacy Protection Act (CalOPPA) requires commercial websites or mobile apps that collect personal information on California consumers to conspicuously post a privacy policy. The privacy policy must, among other things, identify the categories of personally identifiable information collected about site visitors and the categories of third parties with whom the operator may share the information. The privacy policy must also provide information on the operator's online tracking practices. CalOPPA is the first law in the United States to impose disclosure requirements on website operators that track consumers' online behavior. As a practical matter, CalOPPA applies nationwide as long as the site operator collects personal information from California consumers.

According to the California Attorney General, a website, app, or other online service may violate this law if:

- it lacks a privacy policy
- its privacy policy is hard to find
- its privacy policy does not contain all the information required by law
- it does not follow its own privacy policy, or
- it does not notify users of significant changes to its privacy policy

The California Attorney General operates an online complaint form that consumers may use to report violations.

4. Accessing the Internet

You are likely to access the internet using one or more of these services:

- An Internet Service Provider (ISP)
- A Mobile (Cellular) Phone Carrier
- A Wi-Fi Hotspot

If you use a computer to access the internet and pay for the service yourself, you signed up with an *Internet Service Provider (ISP)*. Your ISP provides the mechanism for connecting to the internet.

Each computer connected to the internet, including yours, has a unique address, known as an IP address (Internet Protocol address). It takes the form of four sets of numbers separated by dots, for example: 123.45.67.890. It's that number that actually allows you to send and receive information over the internet.

Depending upon your type of service, your IP address may be "*dynamic*", that is, one that changes periodically, or "*static*", one that is permanently assigned to you for as long as you maintain your service.

Your IP address by itself doesn't provide personally identifiable information. However, because your ISP knows your IP address, it is a possible weak link when it comes to protecting your privacy. ISPs have widely varying policies for how long they store IP addresses. Unfortunately, many ISPs do not disclose their data retention policies. This can make it difficult to shop for a "privacy-friendly" ISP. Some ISPs may share their customers' internet activity with third parties and/or collect your browsing history to deliver targeted advertisements.

When you visit a website, the site can see your IP address. Your IP address can let a site know your geographical region. The level of accuracy depends upon how your ISP assigns IP addresses.

You can block your IP address by utilizing a service such as Tor which effectively blocks this information. Another alternative is to use a Virtual Private Network (VPN). A VPN replaces your IP address with one from the VPN provider. A VPN subscriber can obtain an IP address from any gateway city the VPN service provides. You will have to pick a VPN provider very carefully. Unfortunately, experts can't agree upon which VPN services are best. Some VPNs have potential security flaws that could put your data at risk. It can be difficult to determine how secure a VPN is, and precisely what it is doing with your data. Most experts advise avoiding free VPNs, which may monetize your data in exchange for the free service.

If you access the internet with a phone or other mobile device, you may access the internet using a data plan tied to your cellular phone service. If you have a data plan, your service provider (such as AT&T, Sprint, Verizon, and T-Mobile) collects data about your usage.

5. Passwords

Whenever you have an opportunity to create and use a password to protect your information, make sure that you use a strong password. Passwords are the first line of defense against the compromise of your digital information. Revealing the data on your phone, your banking information, your email, your medical records, or other personal information could be devastating. Yet many people fail to follow proper practices when selecting the passwords to protect this important information. Many websites that store your personal information (for example web mail, photo or document storage sites, and money management sites) require a password for protection. However, password-protected websites are becoming more vulnerable because often people use the same passwords on numerous sites. Strong passwords can help individuals protect themselves against hackers, identity theft and other privacy invasions.

Here are some password "dos" and "don'ts" that can help you to maintain the security of your personal data.

- **Do** use longer passwords. Passwords become harder to crack with each character that you add, so longer passwords are better than shorter ones. A brute-force attack can

easily defeat a short password.

- **Do** use special characters, such as $, #, and &. Most passwords are case sensitive, so use a mixture of upper case and lower case letters, as well as numbers. An online password checker can help you determine the strength of your password.
- **Don't** "recycle" a password. Password-protected sites are often vulnerable because people often use the same passwords on numerous sites. If your password is breached, your other accounts could be put at risk if you use the same passwords.
- **Don't** use personal information (your name, birthday, Social Security number, pet's name, etc.), common sequences, such as numbers or letters in sequential order or repetitive numbers or letters, dictionary words, or "popular" passwords.
- **Don't** feel obligated to change your passwords frequently, unless you believe that your password has been stolen or breached. Conventional wisdom considered changing passwords to be an important security practice. Recent research suggests that people who change their passwords frequently select weaker passwords to begin with, and then change them in predictable ways. Of course, if you believe that your password has been breached or compromised, it is essential to change it immediately.
- **Don't** share your passwords with others.
- **Do** enable two-factor authentication (when available) for your online accounts. Typically, you will enter your password and then a code will be sent to your phone. You will need to enter the code in addition to your password before you can access the account. Twofactorauth.org has an extensive list of sites and information about whether and how they support two-factor authentication. It's best to use an option that isn't SMS-based, such as an authentication app on your smartphone.
- **Don't** write down your passwords or save them in a computer file or email. Consider a password manager program if you can't remember your passwords. Alternatively, keep a list of passwords in a locked and secure location, such as a safe deposit box.

Password recovery methods are frequently the "weakest link", enabling a hacker to reset your password and lock you out of your account. Be sure that you don't pick a question which can be answered by others. Many times, answers to these questions (such as a pet's name or where you went to high school) can be ascertained by others through social networking or other simple research tools. It's also a good idea to have your password resets go to a separate email account designed for resets only.

6. Wireless Networks and Wi-Fi

Households and businesses establish wireless networks to link multiple computers, printers, and other devices and may provide public access to their networks by establishing Wi-Fi hotspots. A wireless network offers the significant advantage of enabling you to build a computer network without stringing wires. Unfortunately, these systems usually come out of the box with the security features turned off. This makes the network easy to set up, but also easy to break into.

Most **home** wireless access points, routers, and gateways are shipped with a default network name (known as an SSID) and default administrative credentials (username and password) to make setup as simple as possible. These default settings should be changed as soon as you set up your Wi-Fi network. In addition, some routers are equipped by default with "Guest" accounts that can be accessed without a password. "Guest" accounts should be disabled or password protected.

The typical automated installation process disables many security features to simplify the installation. Not only can data be stolen, altered, or destroyed, but programs and even extra computers can be added to the unsecured network without your knowledge. This risk is highest in densely populated neighborhoods and office building complexes.

Home networks should be secured with a minimum of WPA2 (Wi-Fi Protected Access version 2) encryption. You may have to specifically turn on WPA2 to use it. The older WEP encryption has become an easy target for hackers. Also, do not name your home network using a name that reveals your identity. Setting up your home Wi-Fi access point can be a complex process and is well beyond the scope of this fact sheet. To ensure that your system is secure, review your user's manuals and web resources for information on security.

The number of **Wi-Fi hotspot** locations has grown dramatically and includes schools, libraries, cafes, airports, and hotels. With a Wi-Fi connection you can be connected to the Internet almost anywhere. You can conduct the same online activities over Wi-Fi as you would be able to at home or work, such as checking email and surfing the web. However, you must consider the risks to your privacy and the security of your device when using a Wi-Fi hotspot. Most Wi-Fi hotspots are unsecured and unencrypted. Even the expensive pay Wi-Fi service available in many airplanes may be as insecure as the free Wi-Fi offered at your corner coffee house. Therefore, you must take additional steps to protect your privacy.

Because the network at a Wi-Fi hotspot is unsecured, Internet connections remain open to intrusion. Hackers can intercept network traffic to steal your information. There are 3 major privacy threats in a Wi-Fi hotspot:

- Man-In-The-Middle Attack refers to the act of intercepting the connection between your computer and the wireless router that is providing the connection. In a successful attack, the hacker can collect all the information transferred and replay them on his computer.
- Eavesdropping refers to the act of using sniffer software to steal data that is being transmitted over the network. A sniffer is an application or device that can read, monitor, and capture network data. This is particularly dangerous when conducting transactions over the internet since sniffers can retrieve logon details as well as important information such as credit card numbers.
- Looking over the shoulder is the simple act of others looking over your shoulder to see your activities.

There are various ways to help protect your privacy when using Wi-Fi. Begin with basic common sense. Look around to see if anyone is surreptitiously trying to look at your computer. Do not leave your computer unattended. Never conduct unsecured transactions over unsecured Wi-Fi. When entering sensitive information (such as your Social Security number, password, or credit card number), ensure that either the webpage encrypts the information or that your Wi-Fi connection is encrypted. Disable your wireless adapter if you are not using the Internet. Otherwise, you leave your computer open to vulnerabilities if it accidentally connects to the first available network.

VPN (Virtual Private Network). This is the first line of defense against vulnerabilities created by Wi-Fi. A VPN provides encryption over an unencrypted Wi-Fi connection. This will help ensure that all web pages visited, log-on details, and contents of email messages remain encrypted. This renders intercepted traffic useless to the hacker. You can obtain software to set up a VPN through your office or home computer, or you can use a commercial provider's hosted VPN service.

Secure surfing/SSL. When checking your email or conducting any important transaction, adding an "s" after "http" may give you a secured connection to the webpage. Many webmail services provide this feature. This ensures that your login details are encrypted thereby rendering it useless to hackers. Although your email login may be encrypted, some webmail providers may not encrypt your Inbox and messages.

Check for SSL (Secure Sockets Layer) certificates on all websites on which you conduct sensitive transaction. SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely.

Wi-Fi settings. Ensure that your computer is not set to automatically connect to the nearest available Wi-Fi access point. This may not necessarily be a legitimate connection point but instead an access point on a hacker's computer.

Disable file-sharing. Ensure that file sharing is disabled on your computer to ensure that intruders cannot access your private files through the network.

Firewall. Install a firewall on your computer and keep it enabled at all times when using Wi-Fi. This should prevent intrusion through the ports on the computer.

Security updates. Keep your computer's software and operating system up-to-date. This will help plug security holes in the software or operating system.

Communications
Education
Employment
Financial
Health
Personal
Retail
Security
Technology

Background Checks
Credit Reports
Data Breaches
Data Brokers
Debt Collection
Government IDs
Identity Theft
Spam

Speak Up

Share Your Story

Support Us

Donate

Sign Up

Last Name (optional)

Email

☐ I want to receive email updates.

Subscribe