Texas Council Risk Management Fund

BROWSER SAFETY

Threat actors often exploit vulnerabilities in web browsers to spread malware. Web browsers are very attractive targets for cyber threat actors since they are one of the most commonly used apps. If you do not take the proper security precautions, threat actors can exploit vulnerabilities in your web browser and spread malware.

Web browsers collect mountains of personal information, which could be lost or exposed in a data breach. Web browsers include several mechanisms that accumulate and store information that reveals a lot about your interests, habits, work, and identity. Since it can be hard to know who can access this information, surfing the web without taking measures to safeguard your privacy puts you at risk.

Here are some common ways that web browsers collect information about you:

Site permissions.
Websites will often request permission from your browser to access several categories of data, including your device's:

- Geolocational data
- Camera
- Microphone

Malicious websites.
Malicious websites could abuse access to your location, camera, and microphone to monitor your activity, conversations, and whereabouts. Websites might also request your permission to send you pop-up notifications. When pop-up notification permissions are enabled on your web browser, a threat actor could use pop-up notifications as part of a phishing campaign or to deliver malware. The intention is to frustrate or overwhelm the user with pop-ups to get them to click on a link they otherwise would not have. One particularly nasty exploit involves Search Engines and how they are optimized to improve quality of searches and direct traffic to sites. Search Engine Optimization poisoning, also known as Spamdexing, manipulates the search engine indexes and can produce inaccurate search results and redirect users to spam sites or malware.

Third-party cookies.
Third-party cookies instruct your web browser to collect, store, and share information about your browsing habits, including your website history, search history, the links you click on, the content you interact with on social media, etc., and share this information with the cookie owner. Data brokers and advertising networks often use third-party cookies to compile and sell your information. Threat actors can also develop third-party cookies to obtain information about potential targets. In sum, third-party cookies pose risks to your privacy due to the vast amount of intimate information they can obtain and the difficulty of knowing who is receiving the information they collect.

In addition to third-party cookies, browsers themselves also store your information, including:

- Browsing history – Your browser can record every website you have ever visited.
- Saved form data – Your browser saves your personal data to autofill certain information fields on forms for you (e.g., name, email address, date of birth, address, phone number, and credit card information).
- Locational data – Even without a Global Positioning System (GPS) device, your browser can use your IP address, Wi-Fi, and Bluetooth to collect and share information about your location with websites.
- Account credentials – Many browsers give you the option to store your account credentials. This makes your credentials vulnerable to leakage if a cyber threat actor successfully exploits vulnerabilities in the browser or your operating system.
- Download history – Your browser can show every file you have downloaded and the file path to where you have it stored on your device, making it easy for threat actors to find data of interest.
- Personal data – Your browser can also collect data about your browsing habits and device activity and share it with third parties to deliver targeted advertisements to you.

Protect yourself against malware. Keep your browser up to date with the latest security patches. If available, turn on automatic updates. Restart your browser regularly to allow the security updates to take effect. (Note: Some browsers may automatically download the newest updates but require the application to be closed and restarted to activate the newest update.)

If you are logged into an account associated with your web browser (e.g., you're logged into your Google account while using Google Chrome or logged into your Microsoft account while using Microsoft Edge), enable multifactor authentication to protect your account. Manage the advertising settings in your browser. Turn off ad personalization in your browser settings. This can help limit access to some of your browser's stored data, including your browsing history. Limit the amount of data that websites and third parties can obtain through your browser. Do not give websites access to your location, camera, or microphone unless these permissions are required for the website to function properly.

The TCRMF Cyber Risk Services Advisor is ready to schedule Cyber Risk Assessments, Incident Response Plan Tabletop Testing visits, and Cyber Presentations for members. To get on the schedule, contact Lee Cain, Cyber Risk Services Advisor by phone at 512-619-1437 or by email at Lee.Cain@sedgwick.com.