

YOUR BROWSER KNOWS MORE ABOUT YOU THAN YOU THINK

Why clearing your browser isn't enough anymore



Most people think of their web browser as simply a way to visit websites. In reality, it's one of the most information-rich applications on your computer.

Every day, your browser quietly remembers details that make life more convenient, but they also make it a valuable target if someone gains access to your computer.

What Your Browser Stores

Your browser may save:

- Usernames and passwords
- Credit card information
- Home and work addresses
- Browsing and search history
- Cookies that keep you signed in
- Autofill information
- Download history

That's a lot of personal information sitting in one place. Many people are surprised to learn just how much information accumulates over time. Every saved login, remembered search and stored payment method adds convenience, but it also increases the value of your browser to anyone

trying to access your personal information.

Browser Extensions Can Be Risky

Extensions can block ads, improve productivity and add useful features, but some also collect browsing data or request access to every website you visit.

Take a few minutes to review your installed extensions. Remove anything you no longer use or don't recognize.

Not every extension is malicious, but every extension adds another piece of software with access to your browser. Keeping only the extensions you actually use reduces clutter, improves performance and lowers your overall security risk.

Convenience vs. Security

Staying signed into Google, Microsoft, Amazon or Facebook saves time, but it also means anyone using your unlocked computer could gain access to your accounts.

Logging out of important websites when you're finished adds another layer of protection.

Five-Minute Browser Checkup

Once a month:

- Remove unused extensions
- Review saved passwords
- Delete old downloads
- Check saved payment methods
- Install browser updates

These simple maintenance tasks improve both security and performance.

The Bottom Line

Your browser is much more than a window to the internet. It's a vault containing some of your most valuable personal information.

Treat it like you would your wallet or smartphone. A few minutes of maintenance each month can help protect your identity, keep your accounts secure and make your browsing experience faster and safer.



CLEARWATER
NETWORK SOLUTIONS

IS YOUR BROWSER WORKING FOR YOU... OR AGAINST YOU?

Most people use a web browser every day, yet few realize how much information it collects. Your browser doesn't just display websites. It remembers passwords, stores payment methods, saves addresses and keeps track of your browsing history to make life more convenient.

That convenience comes with responsibility.

More Than Just a Window to the Internet

Every time you click "Remember Me" or allow your browser to save a password, you're adding another piece of personal information to your browser. While these features save time, they also make your browser one of the most valuable targets if someone gains access to your computer.

Take a Look at Your Extensions

Browser extensions can block ads, improve productivity and add useful features. Unfortunately, some also request permission to read every website you visit or collect information about your browsing habits.

Review your installed extensions every few months. If you don't recognize one

or haven't used it recently, remove it. Keeping only the extensions you need reduces clutter and improves security.

Don't Forget Your Downloads

The Downloads folder is one of the most neglected places on a computer. Old installers, duplicate files and outdated documents take up valuable storage space and make it harder to find important files when you need them.

Cleaning it out takes only minutes and helps keep your computer organized.

Browser Updates Matter

It's easy to ignore the "Update Available" message, but browser updates do much more than add new features. They often fix security vulnerabilities that cybercriminals actively exploit. Running an outdated browser can leave your personal information at unnecessary risk, even if you have good antivirus software installed.

Separate Work and Personal Browsing

If you use the same computer for work and personal activities, consider creating separate browser profiles. This keeps bookmarks, passwords, browsing history and extensions organized while reducing the chance of accidentally using the

wrong account. Change that improves both productivity and security.

Keeping only the extensions you need collections of your personal information.

A Five-Minute Browser Tune-Up

Once a month, take a few minutes to:

- Remove unused extensions
- Review saved passwords
- Delete old downloads
- Check saved payment methods
- Install browser updates
- Close tabs you no longer need

These simple habits improve security, reduce clutter and often make your browser feel noticeably faster.

The Bottom Line

Your browser has become much more than a way to access the internet. It's one of the most frequently used applications on your computer and one of the largest collections of your personal information.

Treat it the same way you treat your smartphone or wallet. A few minutes of monthly maintenance helps protect your accounts and improve performance.

The better you maintain your browser today, the fewer problems you'll have to deal with tomorrow.

7 SIMPLE HABITS THAT MAKE YOU SAFER ONLINE



Cybersecurity doesn't always require expensive software or complicated settings. In fact, many of the biggest security improvements come from small habits that take only a few seconds each day. Whether you're using your computer for work, shopping or staying in touch with family, these simple practices can help reduce your risk.

1. Think Before You Click

Scammers have become experts at creating emails and text messages that look legitimate. Before clicking a link or opening an attachment, take a moment to verify who sent it. If something seems unusual, contact the sender through a trusted phone number or website.

2. Keep Your Software Updated

Updates do more than add new features. They fix security vulnerabilities that cybercriminals actively search for. Turn on automatic updates whenever possible for Windows, your browser and your most-used applications.

3. Use Strong, Unique Passwords

Reusing the same password across multiple websites means a single data breach can expose several of your accounts. A password manager makes it easy to create and store strong, unique passwords without having to remember

them all.

4. Use Multi-Factor Authentication

Whenever a website offers multi-factor authentication, enable it. Even if someone steals your password, they'll have a much harder time accessing your account without the second verification step.

5. Watch What You Download

Only download software from trusted sources. Free utilities, browser extensions and fake software updates are common ways criminals distribute malware.

6. Back Up Important Files

No security plan is perfect. Hardware failures, ransomware and accidental deletion happen every day. Keeping a current backup ensures your important files can be recovered when something goes wrong.

7. Slow Down

Most successful cyberattacks rely on people acting quickly without thinking. Taking just a few extra seconds before clicking a link, entering a password or downloading a file can prevent costly mistakes.

The Bottom Line

Good cybersecurity isn't about being an

SHINY NEW GADGET OF THE MONTH

Shokz OpenRun Pro 2 Bone Conduction Headphones

These let you take calls or listen to music without blocking outside sounds, making them ideal for working safely around the home or office.

Great for:

- Remote workers
- Walking
- Yard work
- Traveling
- Staying aware of surroundings

Features

- Open-ear design
- Excellent microphone quality
- USB-C charging
- Long battery life
- Water resistant



expert. It's about building a few smart habits and following them consistently. Small actions performed every day provide far better protection than reacting after something has already gone wrong.

“
**CYBERSECURITY
ISN'T ABOUT
NEVER BEING
ATTACKED.**
IT'S ABOUT
MAKING YOURSELF
A DIFFICULT TARGET.”





Q: Should I restart my computer or just put it to sleep?

A: Sleep mode is convenient, but restarting your computer at least once a week helps install updates, clears temporary memory and often resolves minor performance issues.



Q: How often should I change my passwords?

A: You don't need to change passwords on a schedule if they're strong and unique. Instead, use a password manager, enable multi-factor authentication, and change passwords immediately if an account is compromised.



Q: Is it safe to use public Wi-Fi?

A: Public Wi-Fi is convenient, but avoid accessing banking or other sensitive accounts unless you're using a trusted VPN or your mobile hotspot.



Q: Why is my computer getting slower over time?

A: Over time, unnecessary startup programs, outdated software, low storage space and aging hardware can all reduce performance. A periodic cleanup can often restore much of your computer's speed.



Q: Should I install every Windows update?

A: In most cases, yes. Security updates protect your computer from newly discovered vulnerabilities, while other updates improve stability and compatibility.

SECURITY SPOTLIGHT:

Secure Business Wi-Fi Protecting Your Network Access

Business Wi-Fi networks should be configured differently than home networks. A properly secured network uses strong encryption and separate wireless networks for employees and guests. Without these controls, unauthorized users may gain access to internal systems or sensitive data. Guest Wi-Fi should always be isolated from the business network so visitors cannot reach company devices. Businesses should also use WPA3 encryption whenever possible and disable outdated security protocols that can leave wireless networks vulnerable to attack. Regularly reviewing Wi-Fi settings and passwords helps ensure that only authorized users can connect to your network.

DID YOU KNOW?



Public Wi-Fi networks at airports, hotels and coffee shops are convenient, but they aren't always secure.

Avoid accessing banking or other sensitive accounts unless you're using a **trusted VPN** or a **secure connection**.