



Protecting Your Privacy: Cookies, Incognito Mode, Secure Text Messaging

BY THE END OF THIS COURSE YOU WILL BE ABLE TO:

Understand and know how to protect your privacy using cookies, incognito mode, and secure text messaging.

Protecting Your Privacy: Cookies, Incognito Mode, Secure Text Messaging

- [Definitions](#)
- [How to Manage](#)
- [PRO TIPS](#)

Definitions

Cookies: Cookies are small text files that websites save on your computer to remember your device, browsing preferences, and activity. They function like a digital ID, allowing websites to keep you logged in, save items in a shopping cart, and personalize your overall web experience.

Common Types of Cookies:

- **First Party Cookies:** Created by the website you are actively visiting. They are usually essential for the site to function properly, such as holding items in your cart or keeping you logged into an account.
- **Third-Party Cookies:** Created by a different website than the one you are visiting (like an advertiser or analytics company). They track your habits across the web to display targeted ads or gather data.

The Pros and Cons:

- **The Good:** They make the internet convenient. You don't have to log into your favorite sites every time you visit, and you don't lose your progress if you close a shopping tab.
- **The Bad:** They can raise privacy concerns. Because they track your behavior, third party cookies allow companies to build a profile of your online habits.

Incognito Mode: Incognito mode (also known as private browsing) is a privacy feature that prevents your web browser from saving your browsing history, cookies, and form data on your device. When you close the window, your temporary session data is erased, ensuring other users of your computer cannot see what you did.



Waseca-Le Sueur Regional Library System Digital Skills Instructions

What it does:

- **Erases session data:** Deletes temporary cookies, cache files, and search history as soon as you close the window.
- **Starts fresh:** Opens a clean window that does not log you into your usual accounts or pull up your saved autofill information.

What it does not do:

- **Does not provide anonymity:** Websites, your Internet Service Provider (ISP), and your employer can still see your IP address and track your online activity.
- **Does not block ads or tracking:** Websites can still use tracking pixels and identifiers to follow you across the web.

Best uses:

- **Planning surprises:** Searching for gifts or travel on a shared computer without alerting others in the household.
- **Logging into multiple accounts:** Checking a second email or social media account without logging out of your primary one.
- **Avoiding targeted ads:** Preventing your normal browsing habits from skewing search results or pop-up ads.

Secure Text Messaging: A secure text message is a communication protected by end-to-end encryption (E2EE), ensuring only the sender and recipient can read it. Unlike standard SMS, which travels in plain text, secure messages scramble content into unreadable code that cannot be accessed by hackers, governments, service providers, or advertisers.

Key Features of Secure Text Messaging:

- **End-to-End Encryption (E2EE):** Data is encrypted on the sender's device and only decrypted upon reaching the recipient's device.
- **Decryption Keys:** Unique keys are stored solely on user devices, not on central servers.
- **Privacy & Integrity:** Ensures that messages cannot be tampered with or intercepted in transit.
- **No Access by Third Parties:** Platforms like Signal, WhatsApp, and Google Messages (using RCS) prevent third parties from accessing message contents.
- **Protection against "Smishing":** Secures against phishing scams that try to steal information via text.

How it Differs from Normal SMS:

- **SMS:** Lacks robust encryption; messages are stored in readable formats on carrier networks.
- **Secure Messaging:** Uses modern protocols to ensure confidentiality, often featuring automatic deletion or disappearing messages for added security.



How to Manage

Cookies: Manage cookies to protect your privacy and fix browsing issues by tweaking settings or deleting saved data directly in your browser. Access your browser's "Privacy and Security" or "Settings" menu to block third-party trackers, clear existing cookies, or set rules for specific websites.

- **Google Chrome:** Navigate to **Settings > Privacy and security > Third-party cookies**. You can toggle options to block third-party tracking or allow related sites.
- **Microsoft Edge:** Go to **Settings > Privacy, search, and services > Cookies and site data**. Select options to block third-party cookies or preload pages for faster browsing.
- **Apple Safari (Mac):** Open **Safari > Settings > Privacy**. Choose to "Block all cookies" or restrict access to the current website only.
- **Safari (iPhone/iPad):** Go to **Settings > Safari**, scroll to **Privacy & Security**, and toggle on options like "Prevent Cross-Site Tracking" or "Block All Cookies."

Best Practices:

- **Clear Regularly:** Deleting outdated cookies removes tracking data, though it will require you to sign back into frequently visited websites.
- **Block Third-Party Trackers:** Prevents advertisers from following you across multiple websites while still allowing the sites you actively visit to remember your login preferences.
- **Use Extensions:** Add-ons like Privacy Badger can automatically manage, limit, and block invasive trackers for you.
- **Review Cookie Banners:** Always review options before clicking "Accept All" on website pop-ups to ensure you aren't consenting to unnecessary data collection.

Incognito Mode: Controlling incognito mode depends on what you want to do: exit a session, restrict access for parental controls, or manage app features.

To Turn On or Off:

- **Computer:** Open your browser's menu (three dots in the top right) and select **New Incognito Window**. To turn it off, simply close all Incognito windows.
- **Phone (Android/iOS):** Open the tabs view and swipe left or tap the mask/hat icon to switch between regular and private tabs.

Secure messaging: Managing secure messaging involves protecting your data from interception and unauthorized access using encryption and strict privacy practices. To get started, implement **end-to-end encryption**, enforce **two-factor authentication (2FA)**, and use apps that obscure user data, like Signal or WhatsApp.



Waseca-Le Sueur Regional Library System Digital Skills Instructions

Choose the Right Platform:

- **End-to-End Encryption (E2EE):** Use apps where messages are scrambled on the sender's device and only unlocked on the recipient's. Not even the server provider can read them.
- **Top Recommendations:** Consider privacy-focused apps like Signal or Telegram (for Secret Chats). For standard text, make sure Google Messages or Apple iMessage has end-to-end RCS/iMessage encryption enabled.

Lock Down Your Accounts:

- **Two-Factor Authentication (2FA):** Always enable 2FA on your messaging apps. This prevents a bad actor from accessing your chats if they steal your password or SIM-swap your phone number.
- **Privacy Features:** Hide your last seen, profile picture, and phone number. Many platforms allow you to hide your phone number entirely and connect with contacts via unique usernames.

PRO TIPS:

Practice good information hygiene for secure messaging:

- **Disappearing Messages:** Turn on expiring or disappearing messages for highly sensitive conversations to ensure they leave no permanent footprint.
- **Avoid Sending Sensitive Data in Text:** If you are forced to use standard email, place sensitive information in a password-protected document and share the password over a completely separate secure channel (like a phone call).