How to Use Incognito Mode in Your Browser — and Why It Doesn’t Guarantee Privacy

Administrator | 08/11/2025 | CYBERSECURITY

Incognito mode — also known as *Private Browsing* or *InPrivate Mode*, depending on the browser — is one of the most misunderstood features in modern browsers.
Many people assume it offers complete anonymity online. It doesn’t.

When you open an incognito window, your browser simply stops **saving local data** such as browsing history, cookies, and form inputs.
That’s all. Your activity is still visible to:

• the websites you visit,
• your Internet Service Provider (ISP),
• your employer or school network administrators,
• and even advertising trackers that use device fingerprints and scripts.

In short, incognito mode hides your tracks from other people who use your computer — not from the internet itself.

What Incognito Mode Actually Hides (and What It Doesn’t)

When you browse privately, the browser creates a **temporary session**. Once you close the window, that session disappears — taking cookies, cache, and login credentials with it.
This is useful if you:

• share a device with others,
• want to log into multiple accounts simultaneously, or
• prefer not to leave traces of sensitive searches.

However, the protection stops there.
Your connection still passes through your **ISP**, which can log every site you visit, along with timestamps and bandwidth data.
Websites can still identify your **IP address** and track you via analytics and ads.
If you’re logged into Google or Facebook, your searches and visits remain tied to your profile.

That’s why cybersecurity experts consider incognito browsing **a local privacy tool**, not an anonymity solution.

The Hidden Risks: Who Can See Your Activity Anyway?

Even if your browser forgets, the internet doesn’t.
Each time you connect, your device sends requests that expose your IP, browser type, and unique fingerprint.
ISPs and online services can use these signals to build detailed user profiles.

Employers and schools often deploy network monitoring systems capable of viewing all traffic. Public Wi-Fi networks, such as those in airports or cafés, are even more vulnerable — anyone on the same network can intercept unencrypted data.

In other words: **private mode protects your device, not your data.**

Why You Need a VPN for True Online Privacy

To achieve genuine privacy, you need to **encrypt your connection** and **mask your IP address**. That's where a Virtual Private Network (VPN) comes in.

A VPN creates a secure "tunnel" between your device and the internet.
All your traffic — browser activity, apps, emails — travels through this encrypted channel, preventing your ISP, advertisers, or hackers from seeing what you do online.

Unlike incognito mode, a VPN protects **everything**, not just your browser session.

How it works

• Your internet traffic is encrypted using advanced protocols like WireGuard or OpenVPN.
• Your real IP address is hidden, replaced by the VPN server's location.
• Even on unsecured networks, your data remains unreadable to outsiders.

The result: complete confidentiality of your online activity, even when you're connected to public Wi-Fi.

The Best VPNs for Privacy and Performance

□□ NordVPN – Speed Meets Security

NordVPN operates over 7,000 servers in 118 countries and uses **NordLynx**, an optimized version of WireGuard that maintains top speeds while encrypting your traffic.
Its **Threat Protection** feature blocks malware, ads, and trackers; **Dark Web Monitor** alerts you if your credentials are leaked.

Plans include:

• Base: VPN only — fast and secure.
• Plus: adds malware protection and a password manager.
• Ultimate: includes 1 TB of encrypted cloud storage and cyber-insurance coverage.

Prices start at **€2.99/month** with a 30-day money-back guarantee.

□□ Surfshark – Unlimited Devices, One Subscription

Surfshark lets you protect **every device** — computers, smartphones, smart TVs, even consoles — under one account.
It uses RAM-only servers (no logs stored) and **CleanWeb**, which blocks malware and ads network-wide.

The **Alternative ID** feature creates anonymous email addresses for safer sign-ups.
With discounts of up to **87%**, Surfshark is ideal for families or small offices seeking full-coverage protection.

⚡ ExpressVPN – Ultimate Speed and Reliability

ExpressVPN's proprietary **Lightway** protocol ensures ultra-fast connections, even on mobile

networks.
It uses **256-bit AES encryption**, the highest standard available, and a **RAM-only infrastructure**, ensuring that no data is ever stored.

Perfect for streaming, remote work, or travel, ExpressVPN supports up to 12 simultaneous connections and even offers a custom router, **Aircove**, for whole-home protection.

How to Activate Private Browsing on Major Browsers

Even if it doesn’t make you invisible, private browsing is still useful for everyday privacy.
Here’s how to activate it on the most popular browsers:

□□ Google Chrome

• Windows/Linux: Ctrl + Shift + N
• Mac: Command + Shift + NOr click the three dots → New Incognito Window.The dark window with a hat-and-glasses icon indicates you’re browsing privately.

□□ Mozilla Firefox

• Windows/Linux: Ctrl + Shift + P
• Mac: Command + Shift + PFirefox shows a purple mask icon and deletes all session data when you close the window.You can even set Firefox to always start in private mode by default.

□□ Microsoft Edge

• Called InPrivate Mode.
• Shortcut: Ctrl + Shift + N or via the main menu → New InPrivate Window.A blue-gray interface with the “InPrivate” label confirms the session is isolated.

□□ Safari

• On Mac: Menu → File → New Private Window or Command + Shift + N.
• On iPhone/iPad: open the tabs menu → choose Private.The address bar turns dark, and Safari stops saving browsing history and cookies.

Incognito Mode + VPN: The Perfect Duo

For everyday browsing, **incognito mode** keeps your local device clean.
For real protection, **a VPN** ensures that your digital footprint is encrypted and untraceable.

Together, they provide layered security:

• Incognito keeps data from being saved locally.
• A VPN hides your identity and activity from everyone else.

So the next time you open a “private window,” remember: it’s only private from your laptop — not from the world.

□□ Key Takeaways

Tool	Protects You From	Hides Local Data	Encrypts Connection	Hides IP
Incognito Mode	Other users on your device	□	□	□

Tool	Protects You From	Hides Local Data	Encrypts Connection	Hides IP
VPN	ISPs, websites, hackers			

In the digital age, privacy isn’t automatic — it’s a choice.
Incognito mode is a start, but not the finish line.
If you truly value your online anonymity, a reliable VPN is **your only real shield**.
Incognito mode — also known as *Private Browsing* or *InPrivate Mode*, depending on the browser — is one of the most misunderstood features in modern browsers.
Many people assume it offers complete anonymity online. It doesn’t.

When you open an incognito window, your browser simply stops **saving local data** such as browsing history, cookies, and form inputs.
That’s all. Your activity is still visible to:

• the websites you visit,
• your Internet Service Provider (ISP),
• your employer or school network administrators,
• and even advertising trackers that use device fingerprints and scripts.

In short, incognito mode hides your tracks from other people who use your computer — not from the internet itself.

What Incognito Mode Actually Hides (and What It Doesn’t)

When you browse privately, the browser creates a **temporary session**. Once you close the window, that session disappears — taking cookies, cache, and login credentials with it.
This is useful if you:

• share a device with others,
• want to log into multiple accounts simultaneously, or
• prefer not to leave traces of sensitive searches.

However, the protection stops there.
Your connection still passes through your **ISP**, which can log every site you visit, along with timestamps and bandwidth data.
Websites can still identify your **IP address** and track you via analytics and ads.
If you’re logged into Google or Facebook, your searches and visits remain tied to your profile.

That’s why cybersecurity experts consider incognito browsing **a local privacy tool**, not an anonymity solution.

The Hidden Risks: Who Can See Your Activity Anyway?

Even if your browser forgets, the internet doesn’t.
Each time you connect, your device sends requests that expose your IP, browser type, and unique fingerprint.
ISPs and online services can use these signals to build detailed user profiles.

Employers and schools often deploy network monitoring systems capable of viewing all traffic.
Public Wi-Fi networks, such as those in airports or cafés, are even more vulnerable — anyone on the same network can intercept unencrypted data.

In other words: **private mode protects your device, not your data.**

Why You Need a VPN for True Online Privacy

To achieve genuine privacy, you need to **encrypt your connection** and **mask your IP address**. That’s where a Virtual Private Network (VPN) comes in.

A VPN creates a secure “tunnel” between your device and the internet.
All your traffic — browser activity, apps, emails — travels through this encrypted channel, preventing your ISP, advertisers, or hackers from seeing what you do online.

Unlike incognito mode, a VPN protects **everything**, not just your browser session.

How it works

• Your internet traffic is encrypted using advanced protocols like WireGuard or OpenVPN.
• Your real IP address is hidden, replaced by the VPN server’s location.
• Even on unsecured networks, your data remains unreadable to outsiders.

The result: complete confidentiality of your online activity, even when you’re connected to public Wi-Fi.

The Best VPNs for Privacy and Performance

□□ NordVPN – Speed Meets Security

NordVPN operates over 7,000 servers in 118 countries and uses **NordLynx**, an optimized version of WireGuard that maintains top speeds while encrypting your traffic.
Its **Threat Protection** feature blocks malware, ads, and trackers; **Dark Web Monitor** alerts you if your credentials are leaked.

Plans include:

• Base: VPN only — fast and secure.
• Plus: adds malware protection and a password manager.
• Ultimate: includes 1 TB of encrypted cloud storage and cyber-insurance coverage.

Prices start at **€2.99/month** with a 30-day money-back guarantee.

□□ Surfshark – Unlimited Devices, One Subscription

Surfshark lets you protect **every device** — computers, smartphones, smart TVs, even consoles — under one account.
It uses RAM-only servers (no logs stored) and **CleanWeb**, which blocks malware and ads network-wide.

The **Alternative ID** feature creates anonymous email addresses for safer sign-ups.
With discounts of up to **87%**, Surfshark is ideal for families or small offices seeking full-coverage protection.

⚡ ExpressVPN – Ultimate Speed and Reliability

ExpressVPN’s proprietary **Lightway** protocol ensures ultra-fast connections, even on mobile networks.
It uses **256-bit AES encryption**, the highest standard available, and a **RAM-only infrastructure**, ensuring that no data is ever stored.

Perfect for streaming, remote work, or travel, ExpressVPN supports up to 12 simultaneous connections and even offers a custom router, **Aircove**, for whole-home protection.

How to Activate Private Browsing on Major Browsers

Even if it doesn’t make you invisible, private browsing is still useful for everyday privacy.
Here’s how to activate it on the most popular browsers:

□□ Google Chrome

• Windows/Linux: Ctrl + Shift + N
• Mac: Command + Shift + NOr click the three dots → New Incognito Window.The dark window with a hat-and-glasses icon indicates you’re browsing privately.

□□ Mozilla Firefox

• Windows/Linux: Ctrl + Shift + P
• Mac: Command + Shift + PFirefox shows a purple mask icon and deletes all session data when you close the window.You can even set Firefox to always start in private mode by default.

□□ Microsoft Edge

• Called InPrivate Mode.
• Shortcut: Ctrl + Shift + N or via the main menu → New InPrivate Window.A blue-gray interface with the “InPrivate” label confirms the session is isolated.

□□ Safari

• On Mac: Menu → File → New Private Window or Command + Shift + N.
• On iPhone/iPad: open the tabs menu → choose Private.The address bar turns dark, and Safari stops saving browsing history and cookies.

Incognito Mode + VPN: The Perfect Duo

For everyday browsing, **incognito mode** keeps your local device clean.
For real protection, **a VPN** ensures that your digital footprint is encrypted and untraceable.

Together, they provide layered security:

• Incognito keeps data from being saved locally.
• A VPN hides your identity and activity from everyone else.

So the next time you open a “private window,” remember: it’s only private from your laptop — not from the world.

□□ Key Takeaways

Tool	Protects You From	Hides Local Data	Encrypts Connection	Hides IP
Incognito Mode	Other users on your device	□	□	□
VPN	ISPs, websites, hackers	□	□	□

In the digital age, privacy isn’t automatic — it’s a choice.
Incognito mode is a start, but not the finish line.
If you truly value your online anonymity, a reliable VPN is **your only real shield**.