Willow Valley Computer Club

Member of apcug An International Association of Technology & Computer User Groups

Project Upskill II

Virtual Private Networks

Al Williams

December 17, 2025

Why Project Upskill?

The Cybersecurity & Infrastructure Security Agency (CISA) collaborated with other US and International partners to create Project Upskill, cybersecurity guidance for high-risk communities.

Project Upskill provides users with simple steps to improve their cybersecurity.

Why Project Upskill?

While none of these steps will offer complete protection against cyber intrusions, this combination of best practices will make it harder to target high-risk individuals and organizations.

They will also limit opportunities for attackers that leverage common techniques such as ransomware or malware.

Why Project Upskill II?

Anyone over 55 who uses a computing device (iPhone, laptop, etc.) is at higher-risk due to data breaches revealing our ages.

The Willow Valley Computer Club's Project Upskill II extends CISA's Project Upskill to include illustrations, examples, additional material, suggestions, and recommendations.

After completing Project Upskill II, you should feel more confident that you can implement basic cybersecurity practices.

Threat Models

We all have personal threat models – lists of events we want to prevent or defend against, and a list of decisions of what to do if an event occurs.

None of us can physically see the threats to our computing devices and our personal information. We need advice.

CISA’s Project Upskill provides guidance but does not recommend any software or hardware.

Our Recommendations

We understand that choosing new software or hardware can be overwhelming if you’re unfamiliar with the topic and do not have the time to research the details.

Think of our recommendations as we helping you based on our knowledge of what works well with effective cybersecurity.

You are not required to use our recommendations.

Clarifying Cybersecurity Recommendations

An understanding of computer concepts will clarify our recommendations.

Exploring our source notes (on most slides) will help you build this foundation.

For hands-on experience, try our workshops (e.g., Bitwarden).

Small learning steps will go a long way in protecting your digital life with confidence.

The Project Upskill II Series –
Where we’ve been and where we’re going.

Goal for Presentation 1

We often focus on the visible risks to our data, like device security. However, hidden risks, such as overlooked privacy policies, can be just as damaging. Our first presentation shed light on this crucial area with suggested solutions.

Goals for Presentations 2, 3, and 4

To ensure the security of your personal data on your computing devices, we provided a layered security approach including:
implementing basic cybersecurity,
preventing account breaches, and
ensuring the protection of your stored data.

Goals for Presentations 5, 6, 7, and 8

To ensure the security of your personal data that isn’t on your computing devices, we provide ways to

protect your data in transit,
secure your home Wi-Fi,
manage your privacy and security online, and
use Virtual Private Networks (VPNs) appropriately.

Virtual Private Networks (VPNs)

For computer users, there are three main VPN configurations

Personal – the most common for home users

Routes your home internet through a secure server

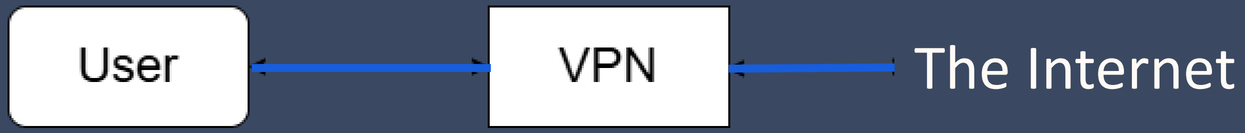
Enterprise – the most common for remote workers

Connects remote workers to company resources

Personal Mesh – Your devices connect directly to each other by VPN, providing a privacy-enhancing network that enables reliable features such as remote desktop access.

Connects your own devices directly to each other

Personal



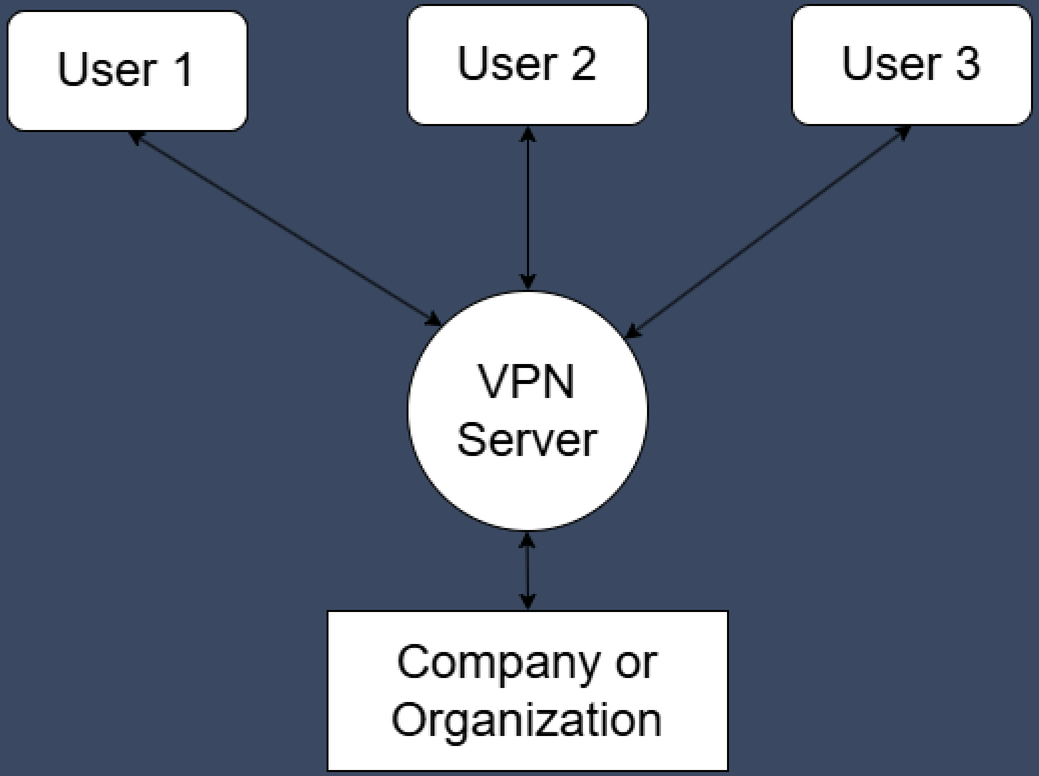
User

VPN

The Internet

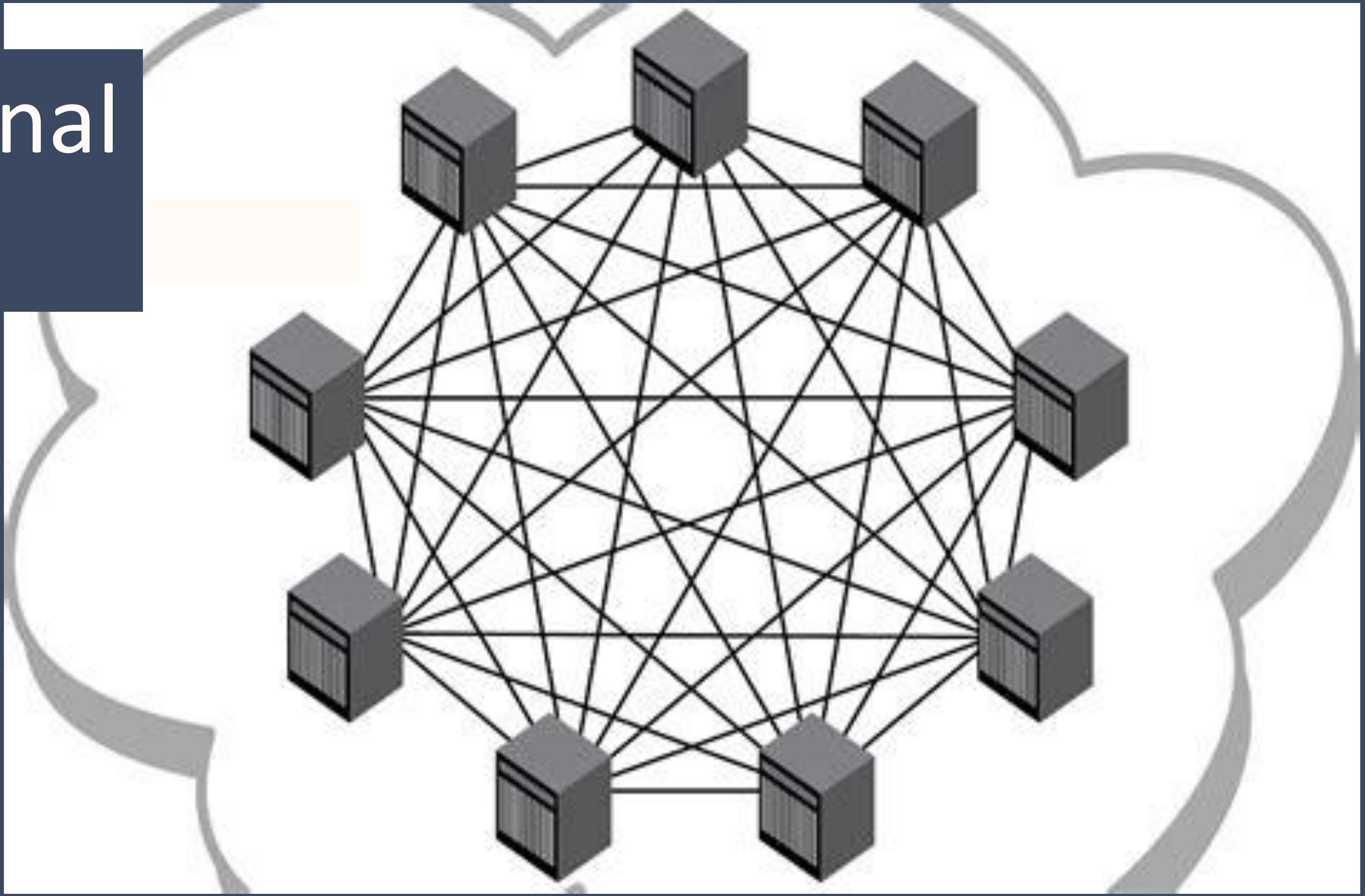
Source: open-ended VPN, draw.io, Created 5/1/2025

Enterprise



Source: closed-ended VPN, draw.io, Created 5/1/2025

Personal Mesh



Source: https://mydiagram.online/wireless-mesh-network-diagram/, Retrieved 5/1/2025

Some Virtual Private Network (VPN) Claims

Enhanced privacy

Complete security

Access geo-restricted content

Prevent website tracking and surveillance

Secure your passwords

Protect your Internet Protocol address (your device’s address on the Internet)

Protect your information while on public Wi-Fi

Some of these claims are true and some are false

Exploring Virtual Private Networks – Road Map

How the Internet works

How a VPN works

What a VPN can do for you

Are there attacks on VPNs?

Choosing a VPN for You

How the Internet Works

How the Internet Works – An Overview

Every device connected to the Internet has a unique address known as an Internet Protocol address, or IP address.

The IP address is similar to a U.S. mail address. The mail address identifies the home, apartment, office, etc. It need not identify who lives or works there.

How the Internet Works – An Overview

When information goes across the Internet, it is broken up into packets and transmitted with a From Address and a To Address.

It’s like putting information on a truck (the truck is like a packet) and shipping it from one address to another.

Image Source: myninja.ai, created 4/26

How the Internet Works – An Overview

All Internet traffic is either encrypted or unencrypted.

All Internet traffic has a To Address and a From Address

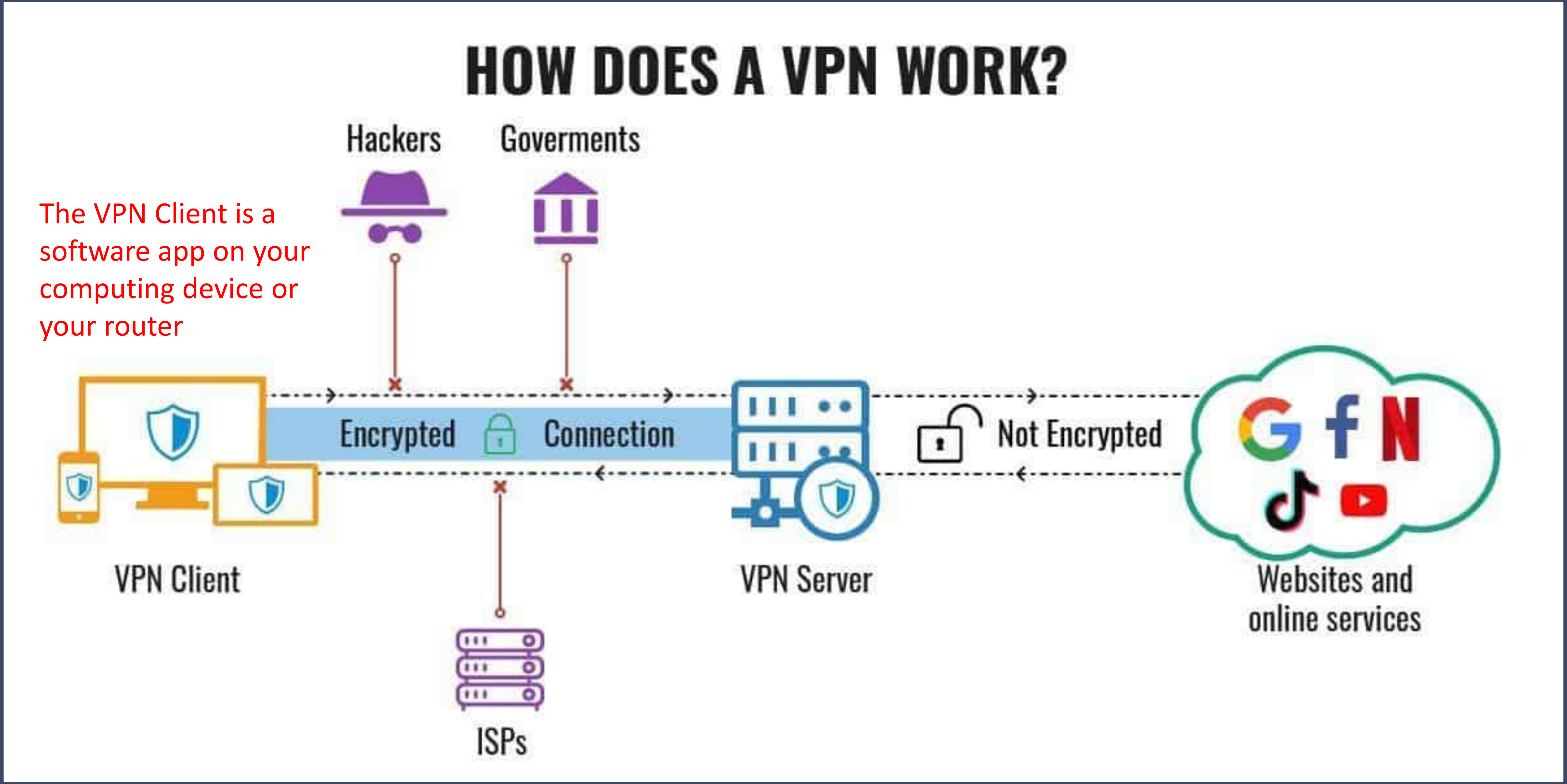
Encrypted traffic cannot be read by anyone else, assuming that best practices in cryptography are used.

How does a VPN Work?

How does a VPN Work?

A VPN is like an encrypted tunnel that carries the trucks that carry the information.

Image Source: Gemini 2.0 Flash, created 4/26/25



The VPN Client is a software app on your computing device or your router

Source: https://cdn.comparitech.com/wp-content/uploads/2020/12/How-vpn-works-01.jpg Retrieved 4/25/25

How Does a VPN Work?

A VPN encrypts your Internet traffic, preventing anyone from watching what you’re doing online.

Why Use a VPN?

Why Use a VPN?

A user’s decision to use a VPN hinges on their online security assessment (threat model).

Another consideration is whether they need to manage their virtual geolocation (to appear to observers as if they are not at their current physical location).

Types of VPN Users

Types of VPN Users

There are two types of computing device users who might want to use a VPN:

higher-risk users and

lower-risk users,

while those with lower perceived risk typically would not.

Types of VPN Users

Higher-Risk Users: Individuals with a higher-risk threat model who often include those who have legitimate concerns about their physical safety or fear for their lives due to their online activities or presence.

Lower–Risk Users: Individuals with a lower-risk threat model generally use VPNs primarily for enhanced cybersecurity and privacy, rather than concerns about immediate physical safety.

What a VPN Can Do for Users

What a VPN Can Do for Higher-Risk Users

Higher-risk uses:

Disguise your identity and activity on the internet,

Hide your real IP address when browsing…,

Bypass censorship

What a VPN Can Do for High- & Low-Risk Users

Higher-risk and Lower-risk uses:

hide your browsing activity from your local network and ISP,

shield your activity on public Wi-Fi,

bypass geographic restrictions

Source: *What Is a VPN, and Why Would I Need One*, Chris Hoffman and Nick Lewis, https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/, Updated Feb 18, 2023

Hiding Your Browsing Activity From Your ISP

The Federal Trade Commission surveyed six major Internet Service Providers (ISPs). They found:

An ISP can *track the websites* their subscribers visit, the shows they watch, the apps they use, their energy habits, their real-time whereabouts and historical location, the search queries they make, and the contents of their email communications. Several ISPs combine their data with data from third-party brokers, revealing race, religion, national origin, sexual orientation, financial status, health status, and political beliefs.

Source: *A Look at What ISPs Know About You – Examining the Privacy Practices of Six Major Internet Service Providers*, https://www.ftc.gov/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers, October 21, 2021

Hiding Your Browsing Activity From Your ISP

The Federal Trade Commission surveyed six major Internet Service Providers (ISPs). They found:

At least three ISPs engage in *cross-device tracking*, which allows browsing behavior on one device to result in targeted ads on another.

The ISP industry is trending toward using *location information* for advertising purposes and selling this data to third parties.

Source: *A Look at What ISPs Know About You – Examining the Privacy Practices of Six Major Internet Service Providers*, https://www.ftc.gov/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers, October 21, 2021

What a VPN Can Do for High - & Low-Risk Users

Higher-risk and lower-risk uses:

hide your browsing activity from your local network and ISP, ✓

shield your activity on public Wi-Fi,

bypass geographic restrictions

Shield Your Activity on Public Wi-Fi

When connecting to public Wi-Fi, attacks are possible:

Man-in-the-middle – which enables eavesdropping:

Login credentials, credit card information, banking info,

Social media account info

Malware distribution

Source: *The Hidden Dangers of Public WiFi*, Digital Forensics Corp,
https://www.digitalforensics.com/blog/software/public-wi-fi-dangers, April 16, 2025

What a VPN Can Do for High - & Low-Risk Users

Higher-risk and lower-risk uses:

- hide your browsing activity from your local network and ISP, ✓
- shield your activity on public Wi-Fi, ✓
- bypass geographic restrictions

Bypass Geographic Restrictions

Streaming services such as Netflix restrict access to their services to specific regions because of contractual agreements with the content providers.

Some VPNs, such as Proton VPN, provide access to U.S. services from anywhere in the world.

Source: *Why You Need a VPN, and How to Choose the Right One*, PC Mag, https://www.pcmag.com/how-to/what-is-a-vpn-and-why-you-need-one, Retrieved April 28, 2025

What a VPN Can Do for High - & Low-Risk Users

Higher-risk and lower-risk uses:

hide your browsing activity from your local network and ISP, ✓

shield your activity on public Wi-Fi, ✓

bypass geographic restrictions, ✓

What a VPN Can Do for Higher-Risk Users

Higher-risk uses of VPNs:

Disguise your identity and activity on the internet,

Hide your real IP address when browsing…,

Bypass censorship

What a VPN Can Do for Higher-Risk Users

While VPNs offer various benefits, higher-risk users must exercise greater diligence when using them than lower-risk users. This heightened caution is due to the more significant potential consequences if the VPN fails or is compromised.

Higher-Risk VPN Users May Want to Consider

VPN Attacks or Weaknesses

- The user can misunderstand VPNs
- The provider can misconfigure VPNs
- The operating system can circumvent VPNs
- An ISP may be able to block VPN activity
- A threat actor can circumvent VPNs
- A cell phone’s hotspot will not support the VPN
- Browser fingerprinting

The User Can Misunderstand VPNs

A VPN’s default choices are usually appropriate. However, it is important to understand that a Kill Switch stops ALL Internet traffic if the VPN disconnects unexpectedly – this prevents accidental exposure of your real IP address.

Cell Phones: The cell phone's VPN software app provides VPN services for its software apps.

The VPN app does not provide VPN service for the phone’s hotspot. When using a hotspot, the VPN app must be installed on the device (laptop, desktop, etc.) or on a router connected to the hotspot.

Higher-Risk VPN Users May Want to Consider

The user can misunderstand VPNs ✓

The provider can misconfigure VPNs

The operating system can circumvent VPNs

A threat actor can circumvent VPNs

An ISP may be able to block VPN activity

The cell phone’s hotspot will not support the VPN

Browser fingerprinting

The Provider Can Misconfigure the VPN

It is crucial to select a highly reputable VPN provider.

Higher-Risk VPN Users May Want to Consider

The user can misunderstand VPNs ✓

The provider can misconfigure VPNs ✓

The operating system can circumvent VPNs

A threat actor can circumvent VPNs

The cell phone’s hotspot will not support the VPN

Browser fingerprinting

The Operating System Can Circumvent the VPN

Several iOS, macOS, and Android apps and services bypass a user's VPN

Windows has telemetry that bypasses a VPN

A Linux distribution may have telemetry that bypasses a VPN

Check your specific OS version

Source: *Most Apple apps on iOS 16 bypass VPN connections*, Andrew Orr, https://appleinsider.com/articles/22/10/12/most-apple-apps-on-ios-16-bypass-vpn-connections, Oct 12, 2022

The Operating System Can Circumvent the VPN

This bypass activity can reveal the user’s IP address to observers, which allows the observer to know where the user is.

Solution: A router incorporating a VPN will force those apps to use the VPN.

Examples: Asus and Netgear routers typically support VPNs.

Examples: Asus RT-AC86U and Netgear Nighthawk R7000.

Source: *Which Routers Support VPN*, https://robots.net/tech/which-routers-support-vpn, September 17, 2023

Higher-Risk VPN Users May Want to Consider

The user can misunderstand VPNs ✓

The provider can misconfigure VPNs ✓

The operating system can circumvent VPNs ✓

An ISP may block a VPN

A threat actor can circumvent VPNs

The cell phone’s hotspot will not support the VPN

Browser fingerprinting

An ISP May Block a VPN

A country may want to block VPN traffic. They will attempt to identify VPN traffic using techniques such as deep packet inspection.

VPNs use obfuscation techniques to prevent traffic identification.

If your VPN stops working, it is likely the country blocked your VPN service.

Source: *What is deep packet inspection?*, Douglas Crawford, https://protonvpn.com/blog/deep-packet-inspection/, January 27, 2023

Higher-Risk VPN Users May Want to Consider

The user can misunderstand VPNs ✓

The provider can misconfigure VPNs ✓

The operating system can circumvent VPNs ✓

An ISP may block a VPN ✓

A threat actor can circumvent VPNs

The cell phone’s hotspot will not support the VPN

Browser fingerprinting

A Threat Actor Can Circumvent the VPN

A threat known as TunnelVision can force Internet traffic that should go through the VPN to bypass the VPN.

VPNs can set firewall rules to prevent TunnelVision activity. You do not need to know anything about the firewall.

Threat Source: *Novel attack against virtually all VPN apps neuters their entire purpose*, Ars Technica https://arstechnica.com/security/2024/05/novel-attack-against-virtually-all-vpn-apps-neuters-their-entire-purpose, May 6, 2024

Firewall Source: *TunnelVision and Proton VPN*, https://protonvpn.com/support/tunnelvision/, Retrieved April 25, 2025

Proton VPN - TunnelVision

Is my device vulnerable on my home or office network?

Almost certainly not. The local network would need to be compromised by a malicious attacker, which is very unlikely. Public Wi-Fi networks may be unsafe, however.

Is my mobile device vulnerable?

Devices using mobile (cellular) connections aren’t vulnerable to TunnelVision attacks. iPhones and iPads may be vulnerable if connected to a local network (e.g., by WiFi or ethernet cable), but this can be mitigated against by enabling the kill switch.

Source: *TunnelVision and Proton VPN*, Proton VPN, https://protonvpn.com/support/tunnelvision/, April 25, 2025

Higher-Risk VPN Users May Want to Consider

The user can misunderstand VPNs ✓

The provider can misconfigure VPNs ✓

The operating system can circumvent VPNs ✓

A threat actor can circumvent VPNs ✓

The cell phone’s hotspot will not support the VPN

Browser fingerprinting

The Phone’s Hotspot Will Not Support the VPN

Cell phone hotspots cannot use VPN software installed on your phone.

The hotspot uses a different network stack (software and hardware) and other IP addresses, requiring the VPN to be on the device using the hotspot or on a router connected to the hotspot.

Higher-Risk VPN Users May Want to Consider

The user can misunderstand VPNs ✓

The provider can misconfigure VPNs ✓

The operating system can circumvent VPNs ✓

A threat actor can circumvent VPNs ✓

The cell phone’s hotspot will not support the VPN ✓

Browser fingerprinting

Browser fingerprinting may uniquely identify a computing device.

A VPN does not protect a computing device from browser fingerprinting.

Browser Fingerprinting

Browser fingerprinting is a tracking method that combines multiple data points from your browser and computing device to create a unique identifier, similar to a human fingerprint.

Browser fingerprinting is passive, gathering information from your computing device without informing you of the activity.

Source: *Browser Fingerprinting – What It Is and How to Block It*, https://techreviewadvisor.com/browser-fingerprinting/, November 7, 2024

Browser Fingerprinting

Browser fingerprinting collects these types of data:

System Information

- Operating system version and architecture (Windows, x64)
- Screen resolution and color depth (1080, 16-bit)
- Available system fonts (Names of font types)
- Time Zone settings (EST)
- System language preferences (English)

Source: *Browser Fingerprinting – What It Is and How to Block It*, https://techreviewadvisor.com/browser-fingerprinting/, November 7, 2024

Browser Fingerprinting

Browser fingerprinting collects these types of data:

Hardware-Related Information

- CPU class (Intel, AMD)
- Device memory (64GB of RAM)
- Graphics card details (NVIDIA Quadro P400)
- Audio processing capabilities (RealTek HD Audio)

Source: *Browser Fingerprinting – What It Is and How to Block It*, https://techreviewadvisor.com/browser-fingerprinting/, November 7, 2024

Browser Fingerprinting

Browser fingerprinting collects these types of data:

Behavioral Parameters

- Mouse movement patterns
- Typing rhythm
- Touch screen behavior
- Battery status

Source: *Browser Fingerprinting – What It Is and How to Block It*, https://techreviewadvisor.com/browser-fingerprinting/, November 7, 2024

Reasons for Browser Fingerprinting

Advertisers use it to track users across websites and deliver targeted ads

Ad networks use it to build detailed user profiles

Companies and banks use it to prevent fraud and for security purposes

Websites can detect suspicious activities when the same device attempts to create multiple accounts or access restricted content

Source: *Browser Fingerprinting – What It Is and How to Block It*, https://techreviewadvisor.com/browser-fingerprinting/, November 7, 2024

Browser Fingerprinting – Privacy Concerns

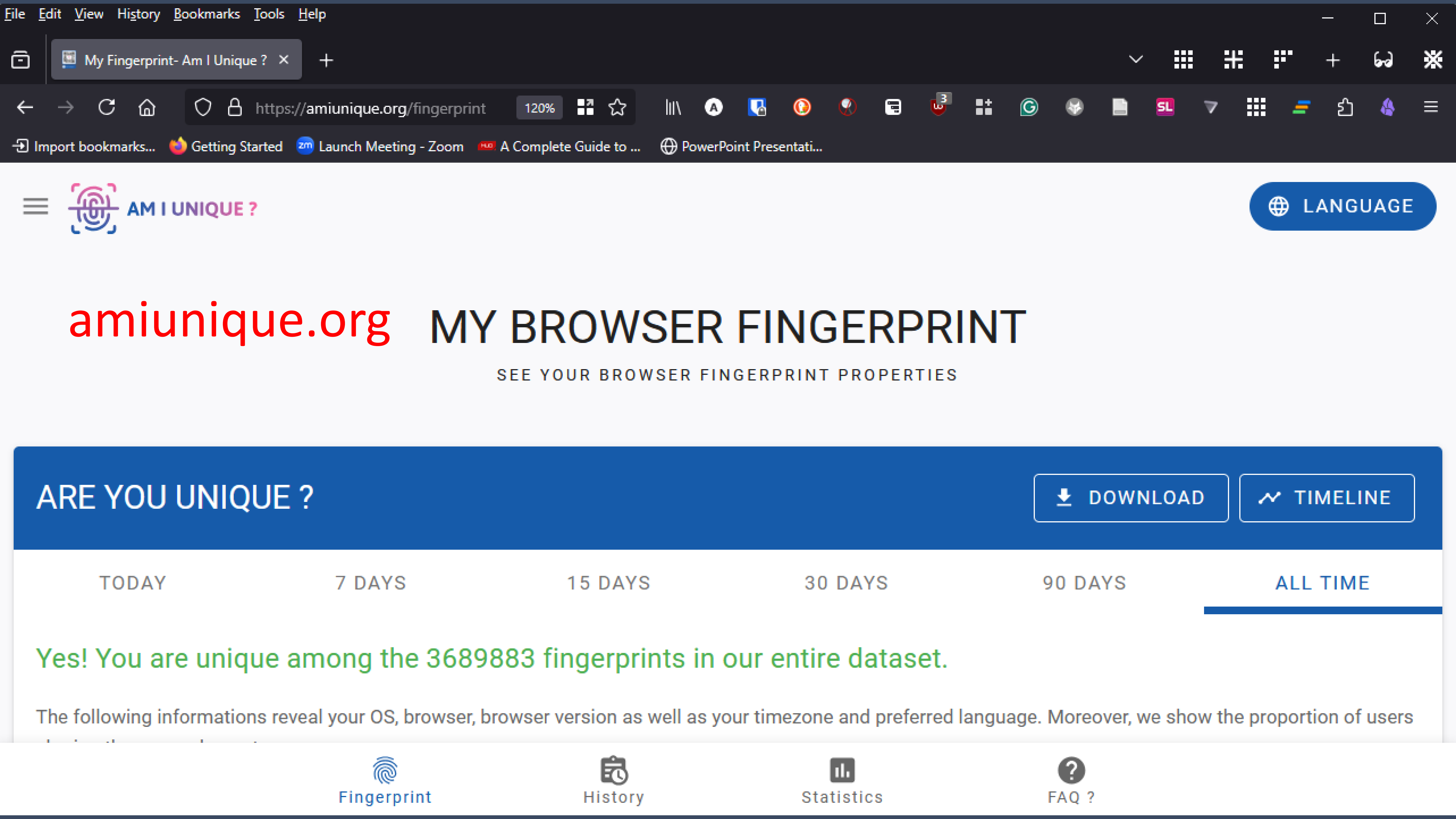
Users are not aware of the data collection, and there is no explicit consent

Websites and advertisers actively circumvent user privacy preferences

User trust is undermined

The principle of respect for individual privacy choices (you can’t opt out) is contradicted

Source: *Browser Fingerprinting – What It Is and How to Block It*, https://techreviewadvisor.com/browser-fingerprinting/, November 7, 2024



amiunique.org

MY BROWSER FINGERPRINT

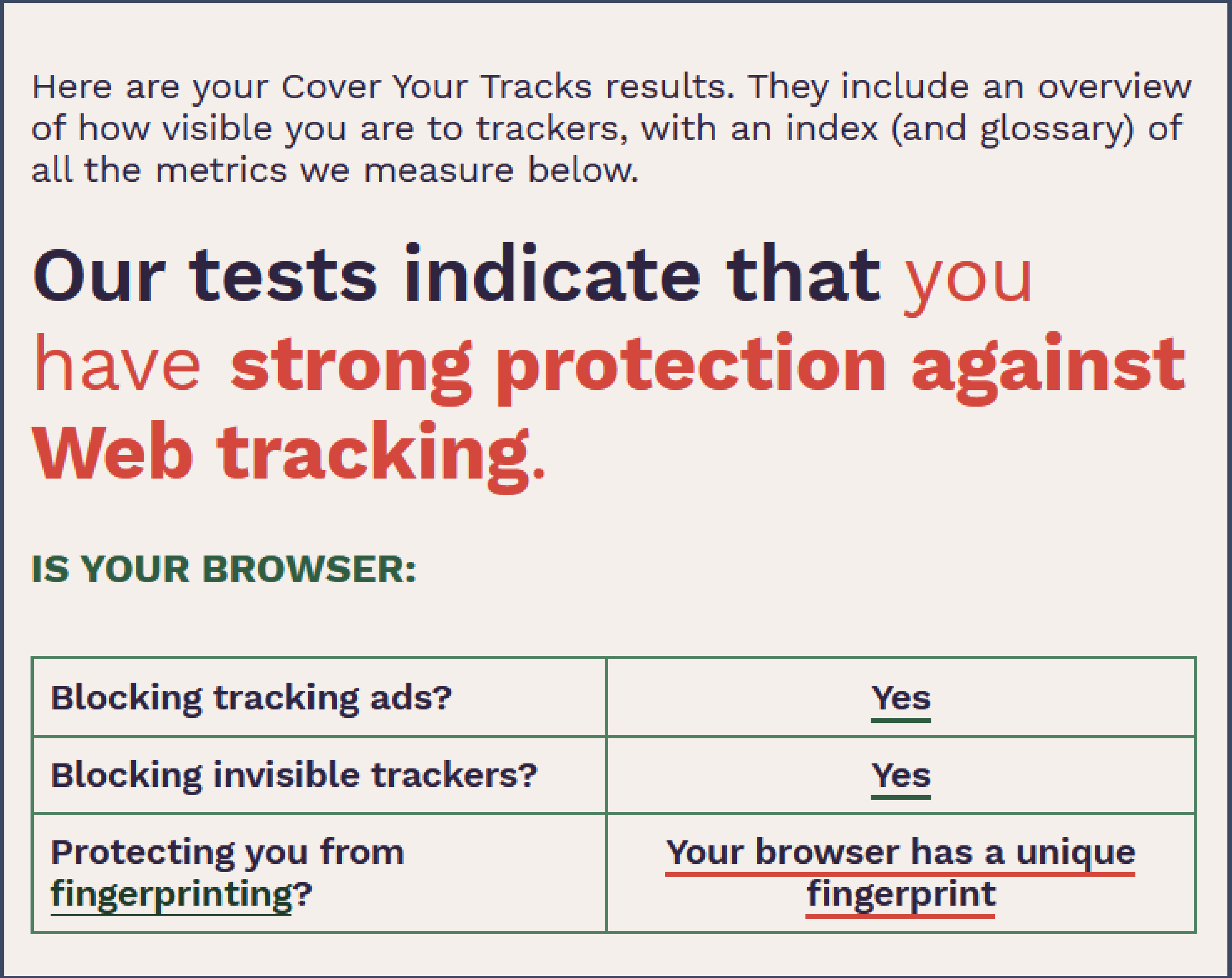
SEE YOUR BROWSER FINGERPRINT PROPERTIES

ARE YOU UNIQUE ?

Yes! You are unique among the 3689883 fingerprints in our entire dataset.

The following informations reveal your OS, browser, browser version as well as your timezone and preferred language. Moreover, we show the proportion of users

CoverYourTracks.eff.org



Here are your Cover Your Tracks results. They include an overview of how visible you are to trackers, with an index (and glossary) of all the metrics we measure below.

Our tests indicate that you have **strong protection against Web tracking.**

IS YOUR BROWSER:

Blocking tracking ads?	**Yes**
Blocking invisible trackers?	**Yes**
Protecting you from fingerprinting?	**Your browser has a unique fingerprint**

Browser fingerprinting is a concern when accessing the Internet, whether or not a VPN is used.

Mitigating Browser Fingerprinting Risks

Use privacy-focused browsers

- Tor Browser (strongest protection)
- Firefox (fingerprinting protection by obfuscation)
- Brave (fingerprinting protection by randomization)

Source: *Browser Fingerprinting – What It Is and How to Block It*, https://techreviewadvisor.com/browser-fingerprinting/, November 7, 2024

Mitigating Browser Fingerprinting Risks

Use effective browser extensions

- uBlock Origin
- Privacy Badger

Source: *Browser Fingerprinting – What It Is and How to Block It*, https://techreviewadvisor.com/browser-fingerprinting/, November 7, 2024

Mitigating Browser Fingerprinting Risks

Advanced protection methods

- Use virtual machines—their standardized configurations make it harder for websites to obtain consistent fingerprinting data.

Source: *Browser Fingerprinting – What It Is and How to Block It*, https://techreviewadvisor.com/browser-fingerprinting/, November 7, 2024

Higher-Risk VPN Users May Want to Consider

The user can misunderstand VPNs	✓
The provider can misconfigure VPNs	✓
The operating system can circumvent VPNs	✓
A threat actor can circumvent VPNs	✓
The cell phone’s hotspot will not support the VPN	✓
Browser fingerprinting	✓

Choosing a VPN

Choosing a VPN

Understand your needs

Emphasize security and privacy

Consider features and ease of use

Evaluate the VPN’s performance

Choosing a VPN – Understand Your Needs

What do you want to use the VPN for?

What devices do you need to protect?

Where are you located, and where do you need VPN server locations?

What is your technical comfort level? Some VPNs are user-friendly, while others offer advanced configurations

Choosing a VPN – Emphasize Security & Privacy

Strong encryption protocols like OpenVPN or WireGuard

No-Logs Policy – don’t log Internet activity

Jurisdiction – consider the country’s privacy laws

Kill Switch – immediately blocks all Internet traffic if the VPN connection drops, preventing your real IP address from exposure.

Leak protection – offers protection against any type of leak that can reveal your real Internet address

Choosing a VPN – Features and Ease of Use

User-friendly interface

Customer support

Specialized servers – streaming, bypassing strict firewalls

Split tunneling – route some traffic through the VPN while other traffic uses the regular Internet connection

Multi-Hop (Double VPN, or Secure Core) – routes traffic through two VPN servers

Choosing a VPN – Evaluate Performance

A large and diverse network generally offers better speeds and more reliable connections.

Speed tests indicate a VPN’s speed performance

Most VPNs offer unlimited bandwidth (the amount of data per second), but double-check

Our Recommended VPN:

Free:	Proton VPN
Paid:	Proton VPN

If we offered a class on VPNs, how many of you would be interested?

This Concludes the

Project Upskill II Cybersecurity Series

for

Spring 2025

Updated

Project Upskill II Cybersecurity Series

Fall 2025

Thank You,
Bill Skelly

Articles

For the latest cybersecurity information, these are accurate and reliable sources:

Ars Technica	arstechnica.com
Bleeping Computer	bleepingcomputer.com
CISA	cisa.gov
Forbes	forbes.com
Proton Blog	proton.me/blog
Proton VPN Blog	protonvpn.com/blog

Books

Beginner’s Introduction to Privacy, Naomi Brockwell, (Independently Published, 2023)

Means of Control: How the Hidden Alliance of Tech and Government is Creating a New American Surveillance State, Bryon Tau, (Crown, 2024)

Your Face Belongs to Us: A Tale of AI, A Secretive Startup, and the End of Privacy, Kashmir Hill, (Crown, 2024)

Extreme Privacy: What It Takes To Disappear, 5th Edition, Michael Bazzell, (Independently Published, 2024)

Firewalls Don’t Stop Dragons, 5th Edition, Carey Parker, (Apress, 2024)

YouTube Channels

David Bombal, [Cybersecurity, Privacy, IT] https://www.youtube.com/@davidbombal

Naomi Brockwell TV, [Privacy]
https://www.youtube.com/channel/UCSuHzQ3GrHSzoBbwrIq3LLA

PC Security Channel, [Cybersecurity, Malware]
https://www.youtube.com/channel/UCKGe7fZ_S788Jaspxg-_5Sg

Questions?