

# 4. Network and Browsing

- [4.1 Browser Hygiene](#)
- [4.2 Home Wifi Security](#)
- [4.3 Smart Home and IoT Devices](#)
- [4.4 Virtual Private Networks \(VPNs\)](#)
- [4.5 Travel Guide](#)

# 4.1 Browser Hygiene

*Core Concepts: Protect Yourself, Minimize Your Exposure*

Your web browser and email are your primary gateways to the internet, and the primary ways attackers try to reach you. Most cyber attacks start with either a malicious website or a phishing email. Good browser and email hygiene can stop the vast majority of these attacks before they start.

You don't need to be a technical expert. Most protection comes from recognizing common patterns, adjusting a few settings, and building good habits about what you click.

## 4.1.1. Understanding Browser Threats

**Common browser threats:**

- Malicious websites that install malware
- Fake websites that steal passwords (phishing)
- Malicious browser extensions
- Tracking cookies and fingerprinting
- Drive-by downloads (downloads that start without your permission)
- Man-in-the-middle attacks on unsecured connections

## 4.1.2. The Basics

- Use a modern browser
- Look for HTTPS and the padlock icon
- Check URLs carefully
- Minimize browser extensions

## Use a Modern, Updated Browser

Modern browsers have built-in security features that older browsers lack. Keep your browser updated to get the latest protections.

### **Recommended browsers:**

- Google Chrome - Most popular, excellent security, but heavy on tracking
- Mozilla Firefox - Good balance of security and privacy
- Microsoft Edge - Good security, integrates with Windows
- Safari - Best for Mac/iPhone users, good privacy
- Brave - Privacy-focused, blocks ads and trackers by default

### **Enable automatic updates:**

- Chrome/Edge: Updates automatically, restart when prompted
- Firefox: Settings > General > Firefox Updates > Automatically install updates
- Safari: Updates with macOS system updates

## Look for HTTPS and the Padlock Icon

HTTPS encrypts the connection between your browser and the website. Always check for it, especially on sites where you enter passwords or payment information.

### **What to look for:**

- Padlock icon in the address bar
- "https://" at the start of the URL (not just "http://")
- Modern browsers show "Not Secure" warning for HTTP sites

### **Warning signs:**

- No padlock icon
- "Not Secure" warning
- Certificate error warnings - don't ignore these!

**NEVER enter passwords or payment info on HTTP sites.** Close the site and find a secure alternative.

## Check URLs Carefully Before Clicking

Attackers create fake websites with URLs that look almost right. Always verify URLs before clicking or entering information.

### **How to check URLs:**

- Hover over links to see the actual URL (bottom left of browser)
- Look for misspellings: "amaz0n.com" instead of "amazon.com"
- Watch for extra words: "amazon-login.suspicious-site.com"

- Check the domain name “https://amazon-login.suspicious-site.com/login”
- Be suspicious of shortened URLs (bit.ly, tinyurl) from unknown sources

**Common tricks:**

- Character substitution: "paypa1.com" (number 1 instead of letter l)
- Adding words: "secure-bankofamerica-login.com"

**When in doubt, type the URL manually** rather than clicking links.

## Use Minimal Browser Extensions

Browser extensions have access to everything you do in your browser. Only install extensions you truly need from trusted developers.

**Extension safety rules:**

- Install only from official browser stores
- Check number of users (millions is better than dozens)
- Read recent reviews
- Review permissions ;if they seem excessive, don't install
- Uninstall extensions you don't actively use

**Recommended extensions:**

- Password manager extension (all, good password managers have them, install from their site)
- Privacy badger <https://www.eff.org/pages/privacy-badger>

See the Software and App Safety section for additional extension guidance.

## 4.1.3. Better Protection

- Configure browser for privacy
- Use a privacy-focused search engine
- Install a reputable add blocker

## Configure Browser for Privacy

Browsers collect data about your browsing. Review and restrict this.

**Chrome:**

- Settings > Privacy and security
- Turn on "Send a 'Do Not Track' request"
- Cookies: Choose "Block third-party cookies"
- Safe Browsing: Use "Enhanced protection" or "Standard protection"

#### **Firefox:**

- Settings > Privacy & Security
- Enhanced Tracking Protection: Choose "Strict"
- Enable "Tell websites not to sell or share my data"
- HTTPS-Only Mode: Turn on for all windows

#### **Safari:**

- Settings > Privacy
- Enable "Prevent cross-site tracking"
- Enable "Hide IP address from trackers"

## Use a Privacy-Focused Search Engine

Search engines track your searches and build profiles. Consider alternatives that don't track.

#### **Privacy-focused options:**

- DuckDuckGo: <https://duckduckgo.com/>
- Startpage: <https://www.startpage.com/>
- Brave Search: Privacy-focused, integrated with Brave browser

#### **How to change default search:**

- Chrome: Settings > Search engine > Manage search engines
- Firefox: Settings > Search > Default Search Engine
- Safari: Settings > Search > Search engine

## Install a Reputable Ad Blocker

Ad blockers prevent malicious ads and reduce tracking. Choose carefully - some ad blockers themselves track you.

#### **Recommended ad blockers:**

- Privacy Badger - Made by EFF, learns to block trackers
- uBlock Origin - Free, open-source, highly effective, no tracking

**Avoid:** AdBlock, AdBlock Plus (these allow "acceptable ads," ads that pay them)

## 4.1.4. Extra Credit

- Use a hardened browser
- Use browser profiles or containers

## Use Hardened Browser

For maximum privacy and security, use browsers with hardened default configurations.

### **Privacy-focused browsers:**

- Brave - Chromium-based, blocks ads/trackers by default
- LibreWolf - Firefox-based, pre-configured for privacy
- Tor Browser - Maximum anonymity (but slow)

### **Advanced Firefox hardening:**

- Use arkenfox user.js template
- Disables telemetry, fingerprinting, and tracking
- Warning: Can break some websites - not for beginners

## Use Browser Profiles or Containers

Separate your browsing into different profiles or containers to isolate activities.

### **Browser profiles (Chrome/Edge/Brave):**

- Create separate profiles for work, personal, shopping
- Each has its own bookmarks, history, passwords, extensions
- Prevents cross-contamination of tracking cookies

### **Firefox containers:**

- Install "Firefox Multi-Account Containers" extension
- Isolate sites into containers (Facebook, Banking, Shopping, Work)
- Sites in one container can't see cookies from other containers

# 4.2 Home Wifi Security

*Core Concepts: Protect Your Data, Minimize Your Exposure*

Your home WiFi network is the gateway to everything in your digital life, your computers, phones, tablets, smart home devices, security cameras, and more. A compromised network means all your devices are at risk. Worse, your neighbors or someone parked outside could be using your internet for illegal activities, and it would trace back to you.

Securing your home WiFi doesn't require deep technical expertise. Most protection comes from changing a few default settings that take 15-30 minutes to configure.

## 4.2.1. Understanding WiFi Security Risks

**Common WiFi threats:**

- **Unauthorized access:** Neighbors or attackers using your WiFi without permission
- **Traffic interception:** Attackers reading data sent over unsecured WiFi
- **Man-in-the-middle attacks:** Attackers positioning themselves between you and the internet
- **Router vulnerabilities:** Unpatched routers with known security holes
- **Compromised IoT devices:** Smart devices used to attack other devices on your network
- **Evil twin networks:** Fake networks that impersonate your WiFi

## 4.2.2. The Basics

- Change your router's default admin password
- Use WPA3 or WPA2/WPA3 mixed mode
- Create a strong WiFi password
- Keep router firmware updated
- Use a custom network name (SSID)

# Change Your Router's Default Admin Password

**This is the single most important thing you can do.** Routers typically come with default passwords like "admin/admin" or "admin/password" that are publicly known. Anyone on your network can access your router's settings with these defaults.

Some more modern routers like what you would get from your Internet Service Provider (ISP) may come with a unique password on a sticker on the back of the device. It is still a good idea to change this password.

## How to access your router:

- Open a web browser
- Type your router's IP address in the address bar
  - Usually 192.168.1.1 or 192.168.0.1
  - Check the sticker on your router
  - Look it up online (<https://router-network.com/default-ip-addresses>)
- Log in with the default credentials (check router manual, sticker, or <https://routerpasswords.com>)

## Change the admin password:

- Look for "Administration," "Management," or "System" settings
- Find "Change Password" or "Admin Password"
- Create a strong, unique password (16+ characters)
- Store it in your password manager
- Save/Apply changes

# Use WPA3 or WPA2 Encryption

WiFi encryption protects your wireless traffic from being read. WPA3 is the newest and most secure, but not all devices support WPA3 yet. WPA2/WPA3 (mixed mode) is fine if you have devices on your home network that don't support WPA3.

## How to enable:

- In router settings, look for "Wireless Security" or "WiFi Security"
- Set Security Mode to:
  - WPA3-Personal (best, if available)
  - WPA2/WPA3 Mixed Mode (good compatibility)
- Save changes

### **NEVER use:**

- WEP - Completely broken, can be cracked in minutes
- WPA1 (original) - Outdated and insecure
- Open/None - Anyone can connect without a password

## Create a Strong WiFi Password

Your WiFi password (also called the network key or passphrase) protects who can connect to your network.

### **Password requirements:**

- Mix of letters, numbers, and symbols OR simple but long
- Not your address, phone number, or birthdate

### **How to change:**

- In router settings, find "Wireless Security" or "WiFi Password"
- Enter your new strong password
- Save/Apply
- You'll need to reconnect all your devices with the new password

**Tip:** Consider creating a passphrase from 4-5 random words: "Correct-Horse-Battery-Staple-47!" is both strong and easier to type on phones than random characters.

## Keep Router Firmware Updated

Router firmware is like the operating system for your router. Manufacturers release updates to fix security vulnerabilities.

### **How to update:**

- In router settings, look for "Firmware Update," "Router Update," or "Administration"
- Check for updates
- If available, click Update/Upgrade
- Wait for update to complete (don't unplug router during update!)
- Router will restart automatically

### **Enable automatic updates if available:**

- Many modern routers can auto-update
- Look for "Automatic Firmware Updates" setting
- Enable it (likely already enabled by default)

**If no auto-update:** Check manually every 3 months.

## Use a Custom Network Name (SSID)

Your network name (SSID) shouldn't reveal your router model or personal information.

### Why change it:

- Default names like "NETGEAR-5G" or "Linksys" tell attackers what router you have
- Attackers can look up known vulnerabilities for that specific model
- Makes your network easier to identify among neighbors

### What NOT to use:

- Your name or address: "Smith Family WiFi" or "123 Main St"
- Anything personally identifiable
- Provocative or offensive names (neighbors can see it)

### Good options:

- Random words: "BlueElephant" or "QuietMountain"
- Numbers/letters: "Network7845"
- Anything generic and non-identifying

### How to change:

- Router settings > Wireless Settings > SSID or Network Name
- Enter new name
- Save/Apply
- Reconnect devices to the new network name

## 4.2.3. Better Protection

- Disable WPS (WiFi protected setup)
- Set up a guest network
- Disable remote management
- Disable Universal Plug and Play (UPnP)
- Review connected devices regularly

## Disable WPS (WiFi Protected Setup)

WPS was designed to make connecting devices easier, but it has a critical security flaw that makes it easy to crack your WiFi password.

**Why disable it:**

- WPS PIN can be brute-forced in hours
- Once cracked, attacker has your WiFi password
- No legitimate reason to keep it enabled

**How to disable:**

- Router settings > Wireless or WPS settings
- Find "WPS" or "WiFi Protected Setup"
- Disable it (turn off)
- Save/Apply

## Set Up a Guest Network

A guest network gives visitors internet access without exposing your main network and devices.

**Benefits:**

- Guests can't see your computers, phones, or shared files
- Infected guest devices can't spread malware to your devices
- You can give out the guest password without compromising your main network
- Can disable guest network when not needed

**How to set up:**

- Router settings > Wireless Settings > Guest Network
- Enable Guest Network
- Set a different SSID (network name): "Guest" or "Visitors"
- Set WPA2/WPA3 encryption
- Create a separate guest password (simpler than main network is OK)
- Enable "Client Isolation" or "AP Isolation" if available (prevents guest devices from seeing each other)
- Save/Apply

**What to put on guest network:**

- Visitor devices
- Smart home devices (doorbell, thermostat, smart lights)

## Disable Remote Management

Remote management allows you to access router settings from outside your home network. Unless you specifically need this, disable it.

#### **Why disable:**

- Opens your router to the entire internet
- Attackers can try to access your router from anywhere
- Most people never need this feature

#### **How to disable:**

- Router settings > Administration or Advanced Settings
- Find "Remote Management" or "Remote Administration"
- Disable it
- Save/Apply

## Disable Universal Plug and Play (UPnP)

UPnP allows devices to automatically open ports in your router. This is convenient but can be exploited by malware.

#### **Why disable:**

- Malware can use UPnP to open ports and bypass your firewall
- Creates security holes without your knowledge
- Most services work fine without it

#### **How to disable:**

- Router settings > Advanced Settings or WAN settings
- Find "UPnP" or "Universal Plug and Play"
- Disable it
- Save/Apply

Note: Some gaming consoles and P2P applications prefer UPnP. If you have issues, you can manually configure port forwarding instead, or enable UPnP again.

## Review Connected Devices Regularly

Check what's connected to your network to spot unauthorized devices.

#### **How to check:**

- Router settings > Connected Devices, Attached Devices, or Device List

- Review the list of connected devices
- Look for:
  - Unknown device names
  - More devices than you expect

**If you find an unknown device:**

- Disconnect it from the router interface
- Change your WiFi password immediately

**Do this monthly:** Set a calendar reminder to review connected devices.

## 4.2.4. Extra Credit

- Use VLANs to segment your network
- Install a custom router

## Use VLANs to Segment Your Network

VLANs (Virtual LANs) separate devices into isolated network segments. This is advanced but powerful.

**Example segmentation:**

- VLAN 1: Trusted devices (computers, phones)
- VLAN 2: Smart home/IoT devices (can't access VLAN 1)
- VLAN 3: Guest network

**Benefits:**

- Compromised IoT device can't access your computers
- Better control over device communication
- Improved network performance

**Requirements:**

- VLAN-capable router (not all consumer routers support this)
- Managed network switch (if hardwired devices)
- Technical knowledge to configure properly

Note: This is advanced. Most people should use guest networks instead, which provide similar isolation with much easier setup. You will need to search online to contact an IT support person for specific instructions for your equipment.

# Install a Custom Router

You can turn any PC into a custom router by installing open source router software, such as OPNSense. This is relatively advanced, so not for the faint of heart, but worth the effort if you are willing to learn a bit about networking and OK with spending a few hundred dollars for a truly secure, custom solution. You can view my guide on TheDen Home Network Runbook if you are curious about what is involved.

# 4.3 Smart Home and IoT Devices

*Core Concepts: Minimize Your Exposure, Protect Your Data*

Smart home and other Internet of Things (IoT) devices make life convenient; smart speakers, security cameras, thermostats, door locks, light bulbs, refrigerators, and more. But these devices are often the weakest link in your home network. Many ship with poor default security, rarely get updated, and connect to the internet 24/7.

A compromised smart device can become a gateway for attackers to access your entire network, spy on you through cameras and microphones, or recruit your devices into a botnet (an army of hacked devices used for cyberattacks).

With some basic precautions, you can enjoy the convenience of smart devices without compromising your security.

## 4.3.1. Understanding IoT Security Risks

### **What are IoT devices?**

Any device that connects to the internet but isn't a traditional computer or phone:

- Smart home: Speakers (Alexa, Google Home), thermostats, light bulbs, plugs
- Security: Cameras, video doorbells, smart locks, alarm systems
- Entertainment: Smart TVs, streaming devices, game consoles
- Appliances: Refrigerators, ovens, washing machines, robot vacuums
- Wearables: Fitness trackers, smartwatches
- Health: Baby monitors, medical devices

### **Common IoT security problems:**

- **Weak default passwords:** Often "admin" or "12345"
- **No security updates:** Many manufacturers abandon support after a couple years
- **Always listening:** Smart speakers and cameras can be compromised for spying

- **Excessive data collection:** Many devices send usage data to manufacturers
- **No encryption:** Some send data unencrypted over your network
- **Unnecessary features:** Open ports, remote access enabled by default

#### **Real-world consequences:**

- Hackers streaming from home security cameras
- Smart speakers recording conversations and sending them to strangers
- Compromised devices used in massive DDoS attacks (e.g., Mirai botnet)
- Smart locks unlocked remotely by attackers
- Baby monitors accessed by strangers

You don't need to avoid IoT devices, they're useful and can make life easier. But treat them with appropriate caution. An IoT device is basically a tiny computer, running software, connected to the internet 24/7. Would you leave a computer with default password "admin" connected to the internet? No? Then don't do it with your TV either.

## 4.3.2. The Basics

- Change all default passwords
- Keep firmware updated
- Disable unnecessary features
- Review device permissions and privacy settings
- Use strong authentication for device apps

## Change All Default Passwords

Default passwords are publicly available and attackers scan for devices using them.

#### **For each IoT device:**

- Check if it has a default password (look in manual or on device label)
- Log into the device's app or web interface
- Find password/security settings
- Change to a strong, unique password
- Store password in your password manager

## Keep Firmware Updated

IoT devices need security updates just like computers. Enable automatic updates where possible.

#### **How to update:**

- Open the device's mobile app
- Look for Settings > About > Firmware or Software Update
- Enable automatic updates if available
- If not available, check for updates manually

#### **For devices without apps:**

- Check manufacturer's website for updates
- May need to download and install manually

**Create a quarterly reminder** to check for updates for your IoT devices that don't auto-update.

## Disable Unnecessary Features

IoT devices often have features enabled by default that you don't need. Turn them off.

#### **Common features to disable:**

- **Remote access:** Unless you need to control devices away from home
- **Cloud recording:** For cameras, use local storage if you can
- **Voice purchasing:** On smart speakers (someone could order without your permission)
- **Always-on microphones:** If you don't use voice commands
- **Usage analytics:** Data sharing with manufacturer

#### **How to find these:**

- Device app > Settings > Privacy or Security
- Look through all settings
- Default to "off" or "disabled" for things you don't actively use

## Review Device Permissions and Privacy Settings

IoT device apps request permissions on your phone. Review and restrict them.

#### **Check app permissions:**

- Phone Settings > Apps > [IoT Device App] > Permissions
- Ask yourself: "Does my smart bulb app really need my location?"
- Deny unnecessary permissions

#### **Common unnecessary permissions:**

- Smart bulb app requesting location (unless for automation)
- Thermostat app wanting microphone access
- Any device requesting contacts

# Use Strong Authentication for Device Apps

The apps that control your IoT devices should have strong passwords and MFA.

## **For each device manufacturer account:**

- Create unique, strong password (use password manager)
- Enable two-factor authentication if available
- Use different email for IoT accounts vs banking/primary email

See the Authentication section for detailed password and MFA guidance.

## 4.3.3. Better Protection

- Research before you buy
- Put IoT devices on guest network
- Use physical controls for cameras and microphones
- Review smart speaker voice history

# Research Security Before Purchasing

Not all IoT devices are created equal. Buy from manufacturers with good security track records.

## **Before buying, check:**

- Does it receive regular firmware updates?
- How long does manufacturer support it?
- Does it require account creation or work locally?
- Does it support WPA3 WiFi encryption?
- Are there known security issues? (search "[device name] security vulnerability")
- What data does it collect and where does it go?

## **Good signs:**

- Manufacturer offers multi-year support commitment
- Automatic firmware updates
- Local control option (doesn't require internet)
- End-to-end encryption for data

- Two-factor authentication support

**Red flags:**

- Unknown or generic Chinese manufacturer
- No firmware updates in 6+ months
- Must have cloud account to function
- Vague privacy policy
- Price seems too good to be true

## Put IoT Devices on Your Guest Network

IoT devices shouldn't have access to your computers and phones. Use your guest network to isolate them.

**Why this matters:**

- Compromised smart bulb can't access your laptop
- Hacked security camera can't see your file shares
- Infected smart TV stays contained

**What to do:**

- Set up guest network on your router (see Home WiFi section)
- Connect IoT devices to guest network instead of main network
- Keep computers, phones, tablets on main network

**Exception:** Devices that need to communicate with your phone/computer (like Chromecast, AirPlay, or printer) may need to be on the main network. This is a tradeoff where you weigh convenience against security for each device.

## Use Physical Controls for Cameras and Microphones

Cameras and microphones in IoT devices can be compromised. Use physical controls.

**For cameras:**

- Focus on entry points (doors, windows) not living spaces
- For smart displays, use the physical camera cover if available
- Tell guests if cameras are present
- Use motion-activated recording instead of continuous
- Store locally instead of cloud when possible

- Set auto-delete for old footage (30 days is reasonable)
- Enable encryption if available

**For microphones:**

- Many smart speakers have physical mute buttons; use them when you want privacy
- Consider where you place always-listening devices

## Review Smart Speaker Voice History

Smart speakers record your voice commands. Review and delete this history regularly.

**Amazon Alexa:**

- Alexa app > More > Settings > Alexa Privacy
- Review Voice History > Filter by date
- Delete recordings or enable auto-delete

**Google Home:**

- Google Home app > Settings > Google Assistant > Your data
- Review and delete activity
- Enable auto-delete for activity older than 3-18 months

**Apple HomePod:**

- Apple doesn't store Siri recordings by default
- Check opt-in settings: Settings > Siri & Search > Siri & Dictation History

## 4.3.4. Extra Credit

- Use local control instead of cloud
- Use VLAN for advanced network segmentation

## Use Local Control Instead of Cloud

Devices that work locally don't require internet and can't be compromised through manufacturer's cloud.

**Local control options:**

- Home Assistant - Open-source home automation platform

- Hubitat - Local smart home hub
- Devices with Zigbee or Z-Wave (don't require manufacturer cloud)

**Benefits:**

- Works even if internet is down
- No dependency on manufacturer's servers
- Devices still work if company goes out of business
- More privacy, data stays in your home

**Tradeoff:** More complex to set up and requires ongoing maintenance. Only recommended for technically comfortable users.

## Use VLANs for Advanced Network Segmentation

VLANs provide the strongest isolation between IoT devices and your trusted devices.

**VLAN segmentation example:**

- VLAN 10: Trusted devices (computers, phones)
- VLAN 20: IoT devices (smart bulbs, thermostats)
- VLAN 30: Security cameras (complete isolation)
- VLAN 40: Guest network

**Firewall rules:**

- IoT devices can access internet but not trusted devices
- Trusted devices can initiate connections to IoT (for control)
- Security cameras can't initiate any connections

**Requirements:**

- Managed router/firewall (OPNSense, UniFi, etc.)
- Managed network switch (if using wired devices)
- Technical knowledge to configure VLANs and firewall rules

See the Home WiFi section for more on VLANs, of TheDen Home Network Guide.

# 4.4 Virtual Private Networks (VPNs)

*Core Concepts: Protect Yourself, Protect Your Data*

VPNs are one of the most misunderstood security tools. They're marketed as making you "invisible online" which isn't true, but they do have legitimate, specific uses that can protect your privacy and security.

This section cuts through the marketing hype to explain what VPNs actually do, when you need one, when you don't, and how to choose and use one effectively.

## 4.4.1. Understanding VPNs

### What is a VPN?

A Virtual Private Network creates an encrypted tunnel between your device and a VPN server. All your internet traffic goes through this tunnel before reaching its destination. A VPN protects your network traffic from local snooping on public WiFi, but it does not make you anonymous or protect you from phishing or malware.

Think of regular internet traffic like sending a postcard. Anyone handling it can read the message and see where it's going. A VPN puts your postcards in sealed envelopes and sends them to a trusted friend (the VPN server) who opens them and sends them to their final destination. The recipient sees the message as coming from your friend, not you.

### What VPNs DO:

- **Encrypts your traffic:** Prevents people between you and the VPN server from seeing what you're doing
- **Hides your IP address:** Websites see the VPN server's IP, not yours
- **Hides activity from your ISP:** Your internet provider sees you're using a VPN but not what you're doing
- **Bypasses geographic restrictions:** Access content blocked in your location
- **Protection on public WiFi:** Secure your connection on untrusted networks

### What VPNs DON'T DO:

- **Make you anonymous:** Websites can still identify you through logins, cookies, and device fingerprinting
- **Protect against malware:** You can still download viruses or visit phishing sites
- **Prevent tracking:** Facebook, Google, etc. still track you when you're logged in

**The trade-off:** VPNs add an extra step to your internet connection, which usually means slower speeds. You're trading some speed for privacy and security in specific situations.

# When You Should Use a VPN

## On Public or Untrusted WiFi

This is the real reason for using a VPN. Use a VPN when connected to any open (unencrypted) WiFi network. An open WiFi network is any network you do not have to enter a network key to connect to.

Note that captive portal sign-in is not the same thing. If you have ever connected to a network, then had to open a browser and sign in to get internet access, you were probably on an open network with a captive portal. A captive portal is a web page that appears when you connect to some WiFi networks (like at hotels or airports) requiring you to agree to terms or enter a password before accessing the internet. These do not offer any protection!

When you connect to an open WiFi network, all other people on the network can potentially see what you are doing. This means a malicious person could also tamper with the data coming from or going to your device. A VPN encrypts all your traffic so they cannot.

## For Privacy from Your ISP

Your internet service provider can see all the websites you visit. A VPN hides this.

### Why you might want this:

- ISPs can sell your browsing history to advertisers (legal in the US)
- ISPs may throttle certain types of traffic (streaming, gaming)
- You don't trust your ISP with your browsing data

**Keep in mind:** You're shifting trust from your ISP to your VPN provider. Choose your VPN provider carefully.

# When You DON'T Need a VPN

## To "Stay Anonymous Online"

VPNs don't make you anonymous, this is marketing hype. You are still tracked based on the accounts you log into, browser and device fingerprinting, tracking cookies, and payment information.

If you want more anonymity (for journalism, activism, etc.), you need specialized tools like Tor, not just a VPN.

## 4.4.2. The Basics

### Choose a Reputable VPN Provider

**This is the most important decision.** A bad VPN provider is worse than no VPN as they can see and log everything you do. Avoid free tiers, as they make money by selling ads to you or your data to someone else. In fact, avoid any VPN that offers a free tier.

#### What to look for:

- **No-logs policy:** Provider doesn't keep records of your activity
- **Independent audit:** Third-party verification of no-logs claims
- **Strong encryption:** AES-256 or equivalent
- **Kill switch:** Blocks internet if VPN disconnects so you don't accidentally disclose unencrypted internet traffic
- **Based in privacy-friendly jurisdiction:** Not subject to invasive data retention laws
- **Good reputation:** Positive reviews from independent tech sites

My recommendation is Mullvad <https://mullvad.net/en>.

## 4.4.3. Better Protection

### Install On Your Phone Too

(Tested with Mullvad, should be a similar process for others)

#### Android Setup:

- Install & Log In
  - Download from the Play Store
  - Log in or activate using your subscription code
- Enable Always-on VPN + Kill Switch

- Go to: Settings > Network & internet > VPN > [Your VPN] > Gear Icon
- Toggle: Always-on VPN
- Block connections without VPN (kill switch)
  - This ensures traffic only flows through the VPN when it's meant to.
- Configure Auto-Connect
  - In your VPN app: Settings > Auto-connect > On WiFi
  - Choose "Untrusted networks only".
  - Add your home/work SSIDs to the Trusted Network List.
- Use WireGuard
  - If offered, select WireGuard protocol for faster performance and quicker reconnections on unstable public WiFi.

### **iOS Setup:**

- Install & Log In
  - Download from the App Store
  - Sign in or activate your account
- Enable Kill Switch
  - In the VPN app, toggle "Kill switch" or "Permanent VPN" (name varies)
  - This is critical on iOS because background app behavior can otherwise leak traffic
- Set Auto-Connect for Untrusted Networks
  - In the VPN app: Settings → Auto-connect → On WiFi
  - Choose "When joining unsecured networks" or "Untrusted networks only"
  - Add your safe networks (home/work) to the Trusted list
- Allow VPN Configurations
  - First time you enable Auto-connect, iOS will prompt to install a VPN profile; approve it

## 4.4.4. Extra Credit

### Run Your Own VPN Server

Advanced users can set up their own VPN server.

#### **Options:**

- Cloud VPS (DigitalOcean, Linode, Vultr) - ~\$5/month
- Home server (Raspberry Pi, old computer)
- Use WireGuard or OpenVPN software

#### **Benefits:**

- Complete control; you're the VPN provider

- No third party to trust
- Access your home network from anywhere (if you host on your network)

**Drawbacks:**

- Doesn't hide activity from ISP (traffic still goes through your connection)
- Single server location (wherever you host it)
- Requires technical knowledge
- You're responsible for security and maintenance

Best for encrypting your traffic on a public WiFi or accessing your home network remotely, not for privacy from ISP or geographical restrictions.

# 4.5 Travel Guide

*Core Concepts: All Four*

Travel introduces unique risks. Prepare before you go and stay vigilant while away.

## 4.5.1. Before You Leave

- **Back Up Everything:** Full backup, test restore (see Backups topic)
- **Enable and Test Find My Device:** Verify location tracking works (see Mobile Device Hardening and OS Hardening topics)
- **Update All Devices:** OS, apps, firmware (see OS Hardening and Mobile Device Hardening topics)
- **Know How to Remotely Wipe:** Review the process (see Mobile Device Hardening topic)
- **Install and Test VPN:** Essential for public WiFi (see VPN topic)
- **Enable Strong Lock Screens:** Not just biometrics (see Authentication and Mobile Device Hardening topics)
- **Pack Cable Locks:** Physical security essentials (see Physical Security topic)
- **Use RFID Blocking Sleeves:** for credit cards and passport
- **Create Emergency Contacts List:** Nearest embassy if international, bank fraud numbers; print and store in luggage

## 4.5.2. During Travel

- **Use VPN on All Public WiFi:** Hotels, airports, cafes (see VPN topic)
- **Don't Use Public USB Charging:** Use AC outlets with your charger (see Physical Security topic)
- **Keep Devices With You:** Never in checked luggage (see Physical Security topic)
- **Lock Screen Every Time:** Even for a moment (see Physical Security topic)
- **Disable Auto-Connect WiFi and Bluetooth:** Prevent automatic connections to malicious networks (see Mobile Device Hardening topic)
- **Be Aware of Shoulder Surfers:** Shield screen and keyboard (see Physical Security topic)
- **Don't Use Hotel Business Center Computers For Sensitive Tasks**

## 4.5.3. At Border Crossings

- **Power Off Devices Before Crossing:** Cold boot required to access encrypted storage (see OS Hardening topic)
- **Consider Disabling Biometrics Temporarily:** Can be compelled to use (see Authentication topic)
- **Know Your Rights:** Varies by country, research in advance

## Plan for Border Crossings

International border agents can legally search devices in many countries.

### Standard precautions:

- Turn off devices before border crossing (cold boot required to access encrypted drives)
- Log out of all services and set back up after crossing
- Uninstall social media apps, delete potentially sensitive text messages
- Clear your browser's cache
- Consider changing important passwords after crossing if device was searched
- Don't volunteer passwords or unlock devices unless legally required

### High-security approach:

- Travel with a "clean" device containing minimal data
- Access sensitive data through cloud services after crossing the border
- Use a burner phone for international travel
- Wipe device before travel, restore from backup after arrival