



Home Network Security

Martial MICHEL



Security & Privacy for your Internet access

A conversation initiated by the NSA's excellent ["Best Practices for Securing Your Home Network"](#)

Note: we will not cover telework, social network presence, or online behavior recommendations. Please refer to the above document for informative content on those topics.



Contents

Security & Privacy for your Internet access	2
Preamble	4
Network security is a problem for everyone:.....	4
Taking steps to secure your network is easier than you think. Here are some steps you can take:.....	5
“Best Practices for Securing Your Home Network”	6
ISP Provided router	6
Wireless Access Point	6
Internet of Things (IoT) devices.....	6
Devices security	7
Devices’ Operating System	7
Passwords	7
Securing Your Internet Access	8
ISP-Provided Router	8
Using a Second Router.....	9
Firewall capabilities	10
IoT-specific Wireless router	11
Browsing: Security & Privacy	12
Password Managers.....	13
Data backup	14
Closing.....	15
Disclaimer	16



Preamble

The digital age has woven technology into the fabric of our lives. From smartphones and laptops to smart appliances and digital assistants, our homes and businesses are increasingly connected to the internet. While convenient and transformative, this interconnectedness opens the door to many security risks. Network security is no longer a concern reserved for large corporations or tech-savvy individuals; it's an issue that affects everyone.

Cyber threats are evolving, and hackers target large organizations, individuals, and small businesses. The rise of the Internet of Things (IoT) has further expanded the attack surface. IoT devices, ranging from smart thermostats, home assistants, smart locks, and connected medical devices to security cameras, often lack robust security measures, making them targets for hackers. In general, anything in your network is a potential attack vector that needs to be dealt with.

Both home and commercial network security is a problem for everyone:



Financial Loss: Cyberattacks can lead to economic losses through identity theft, fraud, or extortion. Hackers can steal credit card information, bank account details including account credentials, or other sensitive financial data. They can also use ransomware to encrypt your files and demand payment for their release.



Data Loss: Cyberattacks can result in losing valuable personal or business data, including photos, documents, and financial records. This can be devastating for individuals and companies alike.











Privacy Breaches: Hackers can access and expose your personal information, such as browsing history, social media activity, or health records. IoT devices such as cameras can also be compromised. This can lead to identity theft, damage your reputation, and erode trust. This can be particularly devastating for businesses that rely on customer trust.



Operational Disruptions: Cyberattacks can disrupt your daily life or business operations. For example, a ransomware attack could encrypt your computer, preventing you from accessing your files or using your device. A DDoS attack could incapacitate your website, causing lost revenue and customer frustration.

Taking steps to secure your network is easier than you think. Here are some steps you can take:

	Use strong, unique passwords for all your online accounts and devices. Use a password manager to help you generate and store complex passwords.
	Secure your Wi-Fi network by changing its default name (SSID), using encryption (at minimum WPA2), and using a strong Wi-Fi password.
	Keep your operating systems (desktops, laptops, phones, tablets, ...), software (web browsers, email software, productivity tools, ...), and firmware (printers, NAS, smart watches, ...) up to date. <ul style="list-style-type: none">• If a device can no longer receive security updates, perform a backup of the required files, then isolate it from your primary network or disable networking for it. In some cases, you can find alternate operating system options.• Devices that are not current on security updates are vulnerable to compromise.
	Enable the firewall on your router and devices.
	Install reputable antivirus and anti-malware software on compatible devices. Keep those up-to-date and schedule regular checks.
	Be mindful of the security risks associated with IoT devices: change default passwords, disable unnecessary features, and update firmware regularly.
	Be careful about what information you share online and avoid clicking on suspicious links or attachments. Be wary of phishing emails that trick you into revealing sensitive information.
	Attempt to stay informed about cybersecurity threats and best practices.

In this document, we will present the different recommendations made by the NSA document and expand upon them by discussing the importance of securing your home network through your ISP-provided router and utilizing additional routers for added protection. We will also discuss the benefits of using a firewall, enhancing browser security, highlighting the significance of password managers, and highlighting the importance of data backups.

“Best Practices for Securing Your Home Network”

The following items from the NSA document are grouped by topics.

ISP Provided router

- “Your router is the gateway into your home network. Without proper security and patching, it is more likely to be compromised, which can lead to the compromise of other devices on the network as well.”
- “routing devices on your home network should be updated to the latest patches, preferably through automatic updates.”
- “should also be replaced when they reach end-of-life (EOL) for support.”
- “Enable strong authentication on your router.”
- “consider using a personally owned routing device that connects to the ISP-provided modem/router.”
- “Ensure that your personally owned routing device supports basic firewall capabilities. Verify that it includes network address translation (NAT) to prevent internal systems from being scanned through the network boundary.”
- “Disable the ability to perform remote administration on the routing device.”
- “Disable Universal Plug-n-Play (UPnP).”

Wireless Access Point

- “To keep your wireless communications confidential, ensure your personal or ISP-provided WAP is capable of Wi-Fi Protected Access 3 (WPA3).”
- “If you have devices on your network that do not support WPA3, you can select WPA2/3 instead.”
- “use a strong passphrase with a minimum length of twenty characters.”
- “protected management frames should also be enabled for added security.”
- “use modern router features to create a separate wireless network for guests.”
- “schedule weekly reboots.”
- “Change the default service set identifier (SSID) to something unique. Do not hide the SSID as this adds no additional security to the wireless network and may cause compatibility issues.”
- “your wireless network should be segmented between your primary Wi-Fi, guest Wi-Fi, and IoT network.”

Note: Protected Management Frames are used for maintaining and managing the network, such as association and disassociation requests, beacons, and probe requests. They are mandatory in WPA3, optional in WPA2.

Internet of Things (IoT) devices

- “IoT devices on a home network are often overlooked, but also require updates. Enable automatic update functionality when available. If automatic updates are not possible, download and install patches and updates from a trusted vendor on a monthly basis.”
- “use modern router features to create a separate wireless network [...] for network separation from your more trusted and private devices.”

Devices security

- “Electronic computing devices, including computers, laptops, printers, mobile phones, tablets, security cameras, home appliances, cars [...] must all be secured to reduce the risk of compromise.”
- “Minimize charging mobile devices with computers; use the power adapter instead [...] Avoid connecting devices to public charging stations.”

Devices’ Operating System

- “Upgrade to a modern operating system and keep it up-to-date.”
- “Utilize a non-privileged user account for everyday activities: [...] highly privileged administrator account can access and potentially overwrite all files and configurations on your system. [...] Only use the privileged account for maintenance, installations, and updates.”
- “Leverage security software that provides layered defense via anti-virus, anti-phishing, anti-malware, safe browsing, and firewall capabilities.”
- “Full disk encryption should be implemented where possible on laptops, tablets, and mobile phones.”
- “Regularly reboot computers to apply [...] updates.”

Passwords

- “Ensure that passwords and answers to challenge questions are properly protected.”
- “Passwords should be strong, unique for each account, and difficult to guess.”
- “Passwords and answers to challenge questions should not be stored in plain text form.”
- “Using a password manager is highly recommended.”
- “answer challenge questions [by] providing a false answer to a fact-based question, assuming the response is unique and memorable.”
- “Use multi-factor authentication (MFA) whenever possible.”

Securing Your Internet Access

ISP-Provided Router

Your home network's security hinges on the strength of your router(s)'s defenses. As the gateway to your internal network, a vulnerable router exposes every connected device to potential threats. Without proper security measures and timely patching, routers become a weak link that malicious actors can exploit to access sensitive information or launch attacks.

[Attackers can exploit remote administration features](#) or [Universal Plug-n-Play \(UPnP\)](#), which allows devices to configure port forwarding automatically) to create remotely controllable minions. Those “Zombie computers” are infected with malware and are controlled remotely by attackers, often as part of a botnet network. They can launch [Distributed Denial of Service \(DDoS\)](#) attacks by flooding websites/servers with traffic from multiple sources and overwhelming them. An example of a DDoS system was the [Mirai botnet](#) in late 2016, which leveraged UPnP to compromise many Internet of Things (IoT) devices like security cameras and routers and launched massive attacks. Regularly updating the router's firmware is crucial to address known vulnerabilities and protect against emerging threats. Enable automatic updates to ensure you receive the latest patches promptly. If an automatic option is unavailable, a weekly update check and mandatory reboot can help mitigate certain types of in-memory attacks or malware infections by clearing the router's memory and resetting it to a clean state. Rebooting will not remove *persistent* malware installed on the router's firmware or non-volatile storage.

Routers provide [Network Address Translation \(NAT\)](#) to [enable multiple devices on a private network to share a single public IP address for accessing the Internet](#) or other public networks:

- Devices on the [Local Area Network \(LAN\)](#) are assigned [private IP addresses](#) from reserved non-routable ranges (like 192.168.x.x or 10.x.x.x), which masks your devices' internal IP addresses from the outside world.
- The [Internet Service Provider \(ISP\)](#) assigns the router a single public and routable IP address on its [Wide Area Network \(WAN\)](#) port.
- When a device on the LAN wants to access the internet, the router creates an entry in its NAT table, mapping the device's private IP and source port to the router's public IP and a new port number. As packets go out from the LAN to the internet, the router modifies the source IP in the packet headers, replacing the private IP with its public IP and translating the source port.
- When response packets come back from the internet, the router refers to the NAT table, replaces the destination public IP and port with the original private IP and port of the LAN device, and forwards the packets to the originating device.

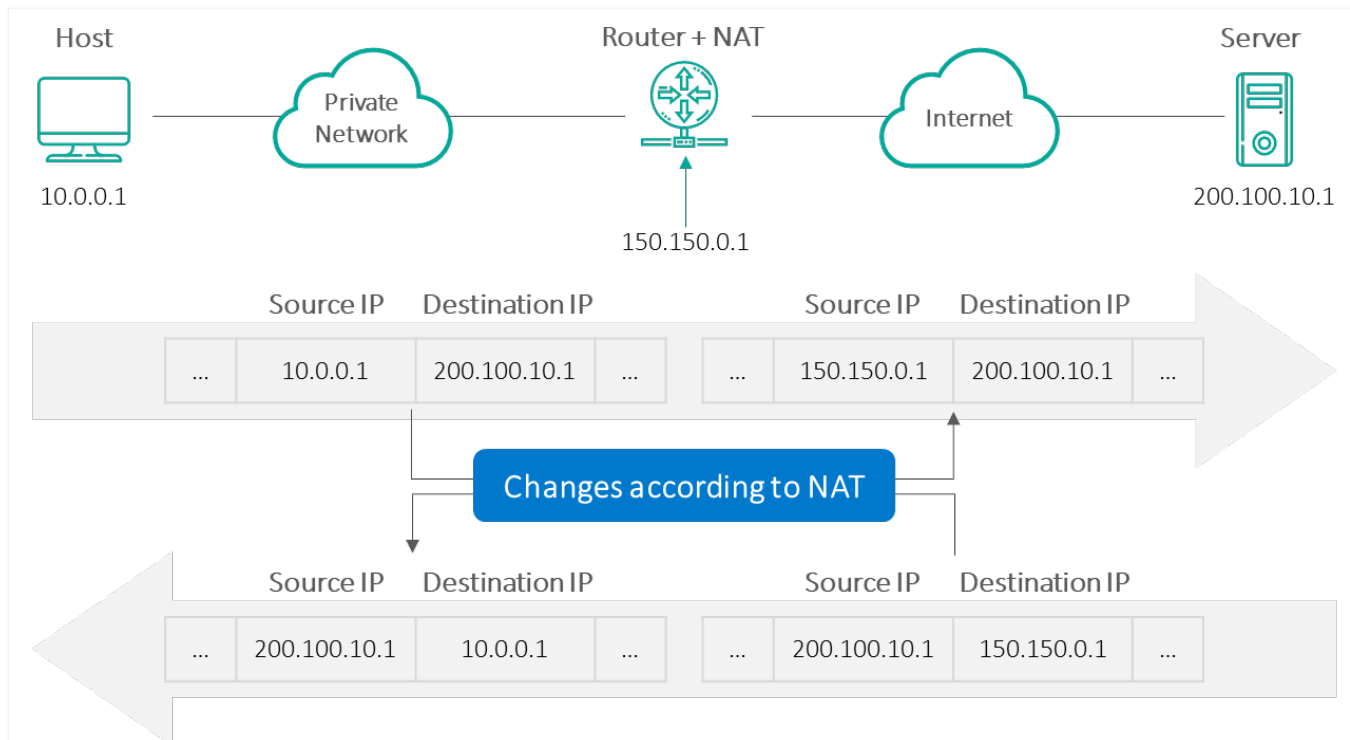


Figure 1: NAT -- Michel Bakni, CC BY-SA 4.0 <https://creativecommons.org/licenses/by-sa/4.0>, via Wikimedia Commons

The router's [Stateful Packet Inspection \(SPI\) firewall](#) monitors active network connections and filters incoming and outgoing data packets based on predetermined security rules and the context of each connection. For example, a data packet in the WAN without a matching NAT entry from the LAN will be blocked.

Using a Second Router

While ISPs often offer their customers a router device with wireless capabilities, using a second router to act as your devices' router and [Wireless Access Point \(WAP\)](#) adds some protection. The ISP device might be required to be used by some other services, such as cable boxes. However, disabling its Wifi capabilities or only using that Wifi setup for the ISP devices gives more control over your security setup.

Utilizing this second router as a dedicated Wifi access for your devices can significantly enhance your network's security.

- It enforces [network segmentation](#) for your devices, which acts as a barrier, isolating potential threats that may originate from the internet or the ISP-provided device from reaching your devices.
- Many dedicated routers offer enhanced security features compared to the functionalities provided by ISP-issued devices, which may include advanced firewalls, intrusion detection systems, and content filtering options, allowing you to customize security measures to your specific needs.
- It allows you to control firmware update frequency and apply patches and updates promptly, ensuring your network is protected against the latest vulnerabilities without relying on the ISP's update schedule.
- Most support Guest Network isolation and provide internet access to visitors and IoT devices without granting them access to your primary network or shared resources, adding another layer of protection for your sensitive data.
- By isolating your wireless devices on a separate network segment, you effectively reduce the attack surface exposed to potential threats from vulnerabilities in the ISP-provided router.

Firewall capabilities

Adding a (hardware) firewall to this setup is also an option if your secondary router does not provide some of the features you might want from the list below. Because it handles traffic filtering and security functions, the hardware firewall offloads most of the processing burden from your router, potentially improving its performance and stability.

Among those potential added features:

- [IDS or IPS](#): An Intrusion Detection System (IDS) passively monitors network traffic and alerts administrators when it detects potential security breaches or malicious activity but does not take any action to block or mitigate the detected activity. An Intrusion Prevention System (IPS) actively monitors network traffic and immediately blocks or mitigates detected threats.
- *Network scanning* scans your network for vulnerabilities and potential threats, simulating attacks to identify weaknesses before malicious actors can exploit them. Some of those can also identify software and attempt to report known vulnerabilities for given versions.
 - Similar to this concept, devices' open port detection uses *port scanning* to send packets to various ports on a target device and analyze the responses to determine whether the ports are open or closed.
- For users with limited bandwidth or those concerned about excessive data consumption, *data usage monitoring* tracks how much data is being transferred over the network, identifies which devices (or applications) are consuming the most data, and detect any unusual patterns that may indicate security breaches or unauthorized access.
 - It can also run periodic tests on the bandwidth throughput of your ISP and local wireless network.
 - When combined with per-device analytics, it is possible to follow the data flow for a given device to a destination.
- Getting your devices' LAN IPs using [Dynamic Host Configuration Protocol \(DHCP\)](#) or *static IP assignment* simplifies tracking device behavior. DHCP automatically assigns devices LAN IP addresses, subnet masks, default gateways, and other network configuration parameters. For some devices, you might prefer to use static IP assignment to manually assign a predictable fixed LAN IP address to a device (useful for printers, servers, NAS devices, ...)
- *New device quarantine* automatically isolates devices that connect to your network with a not-before-seen [MAC address](#), preventing them from accessing other devices or the internet until you explicitly authorize them.
 - "Private Wi-Fi addresses" on some of your devices might trigger this, so it is recommended that you disable this feature on your Wi-Fi networks.
- *Content and service filtering* controls and restricts access to certain types of content or services on the internet. These filtering mechanisms can be implemented at various levels, including for individual devices.
 - Content filtering involves analyzing web traffic and blocking or allowing access to websites or web pages based on their content. This can be done using various methods, such as keyword, category, URL, or reputation-based filtering.
 - Service filtering involves blocking or allowing access to specific internet services or protocols. This can be done based on port numbers, application signatures, or other criteria to block access to things such as Peer-to-Peer (P2P) or restricting Social Media access.

- Upgrading [Domain Name Services \(DNS\)](#) queries to use [DNS-over-HTTPS \(DoH\)](#) (or over [TLS](#) or [QUIC](#)). DNS queries are sent over plain text, making them susceptible to eavesdropping and manipulation. DoH encrypts DNS queries and responses, enhancing privacy and security.
 - It is also possible to use cloud-based DNS services that offer enhanced security, privacy, and customization features compared to traditional DNS providers, such as Content Filtering (ads, trackers, malware,...), Security (phishing attacks and DNS-based threats), Location-Based Filtering (bypass geo-restrictions, block specific countries' [TLD](#), ...), IP Blocklists (entire ranges of IP including [DNS-rebinding](#)), Service-Specific Blocking (e.g., social media, streaming platforms, ...), online tracking blocking (embedded trackers) and perform analytics.
- Using Dynamic DNS (DDNS) to access your home network or devices with a fixed hostname, even if your ISP assigns you a dynamic IP address that changes periodically.
 - A reachable port on your ISP router allows you to access your network devices remotely through an encrypted tunnel, a [Virtual Private Network](#). [WireGuard](#) is a modern, open-source VPN protocol with a fast, secure (and easy-to-use alternative to traditional VPN protocols like OpenVPN and IPsec). It uses state-of-the-art cryptography for robust security and is known for its speed compared to other VPN protocols. To use it, you must open a port on the ISP-provided router and set port forwarding to the device providing the Wireguard server (within your network).
 - Alternate no-open-port solutions exist that provide modern, secure network services. These services allow you to connect devices and resources across different networks as if on a single private network (a [mesh](#) VPN built on top of WireGuard), enabling secure and direct peer-to-peer connections between devices.

IoT-specific Wireless router

Adding another Wireless router at the end of your ISP-provided one can create another layer of separation specifically for your Internet of Things (IoT) devices, isolating them from your primary network. This limits the potential damage if an IoT device is compromised, preventing attackers from attempting to access (and potentially install [ransomware](#) on) your computers, phones, or other sensitive data. Because this IoT-specific router is behind the ISP-provided router, it is behind a first layer of separation from the internet and completely separated from your main router's network (and blocked by the SPI rules of that router).

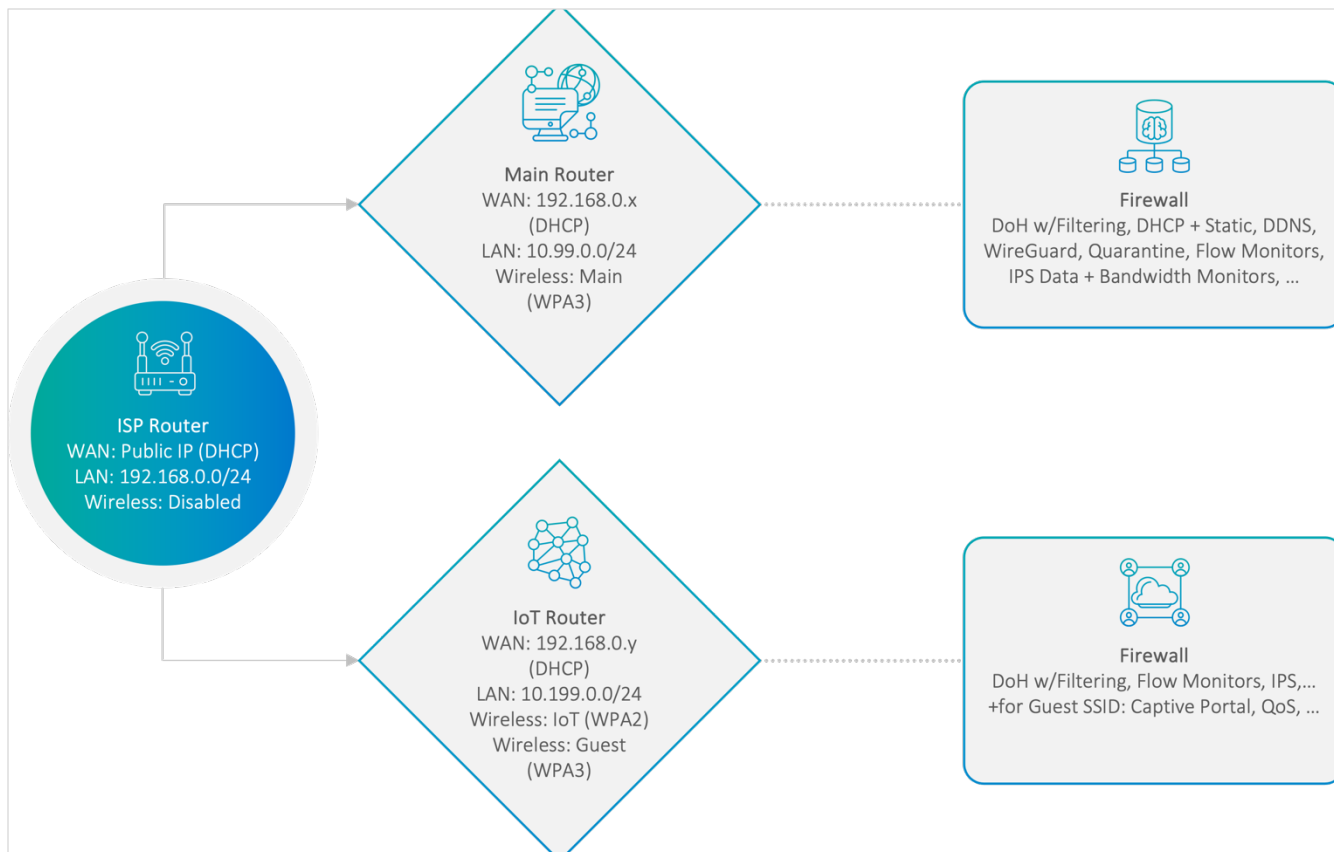


Figure 2: Example setup (using [Captive Portal](#) and [Quality of Service \(QoS\)](#) for the Guest Wifi)

Browsing: Security & Privacy

[Ad blockers](#) greatly enhance browser security and privacy. While their primary function is removing unwanted advertisements, their benefits are multiple:

- Malicious, [malvertising](#) ads are a significant threat that can infect your system with malware through drive-by downloads, even without clicking on them. Ad blockers prevent these malicious ads from loading, drastically reducing your risk of infection.
- Many ads track your online activity, collecting data about browsing habits, interests, and personal information, which some [filter lists](#) in ad blockers prevent.
- Ads consume bandwidth and processing power, slowing your browsing experience (sometimes up to over 40 additional sites to reach: ads and promotional elements like social media sharing buttons, email subscription prompts, related article recommendations, ...).

Cookies are a method used to track users [when visiting a site](#). While some cookies are essential for website functionality, others, known as tracking cookies, are used to monitor your online activity. When you visit a website, it may place a tracking cookie that contains a unique identifier that can be used to recognize your device across different websites and over time. As you browse the web, the tracking cookie collects information about your activity, often shared with or sold to third-party companies. These companies can then aggregate data from multiple websites to create detailed profiles of your interests, preferences, and online behavior.

Google has introduced the [Privacy Sandbox](#), which intends to phase out support for third-party cookies in Chrome. “Topics” aims to enable interest-based advertising while protecting user privacy by replacing third-party cookies with a taxonomy of around 350 topics or interest categories (like "Sports," "Travel," "Cooking," etc.). Chrome tracks the websites a user visits over a week and maps them to the corresponding topics. Three of those topics are then shared with websites, allowing for more private and less invasive targeted advertising. Topics are stored on the user's device for only 3 weeks before being deleted and refreshed. During [Google I/O in May 2024](#), it was discussed that Chrome plans to begin rolling out third-party cookie phaseout and the Tracking Protection UI to all Chrome clients in early 2025.

Beyond those, there are several other essential considerations for enhancing browser security and protecting yourself online:

- Keep your browser (and Operating System) updated to the latest version, as those often include security patches that fix vulnerabilities that attackers could exploit.
- Only install *necessary* extensions and plugins from reputable sources.
- Use a password manager to generate and store *strong, unique* passwords for your online accounts. Avoid password reuse to help protect from [credential stuffing](#) attacks.
 - Enable [Multi-Factor Authentication \(MFA\)](#) whenever possible. Avoid [SMS codes](#) in favor of [Time-based one-time passwords \(TOTP\)](#).
 - If your password manager does not offer a password for a site it knows, be wary of [typo-squatting](#) attacks.
- Some browsers offer [sandboxing](#) features that isolate web pages from the rest of your system (Chrome, Firefox, and Edge utilize various sandboxing methods such as process isolation, restricted access tokens, filtering of system calls and API usage, validating inputs, and sanitizing data passing between processes).

Password Managers

In general, when looking for a password manager (PM), look for one that:

- Prompt you automatically to fill in details for the site visited. This is important if you got to a [typo-squatting](#) website by mistake (ex: [google](#) vs. [goooogle](#)) and were to type your login information.
- Record your [Time-based One Time Passwords \(TOTP\)](#). Many prominent websites will offer “2-factor authentication” (2-FA) or “multi-factor authentication” (MFA). Some of those will prompt you to scan a QR code. Some PMs will store that information by scanning the QR code from the website. Some will even tell you if some of your sites offer the service and you are not using it. In general, it is strongly recommended that MFA be used. If your username/password gets compromised, this will prevent malicious actors from accessing your account if they get this information. Some PMs will offer to protect your account with MFA; do not store the MFA inside the PM itself to avoid locking yourself out of your account.
- Check if any of your passwords have been [compromised in a data breach](#) and inform you so you can change it before your account is used by malicious actors (especially true if no MFA was added to that account).
- Inform you if you are reusing passwords. If you reuse passwords, when one is compromised (email/password pair), malicious actors will try this combination for many popular sites, putting you at risk.
- Allow you to generate passphrases. [Passphrases are more challenging to break than passwords](#). Some PMs will allow you to create passphrases and specify word separators, the number of words, capitalization, and include numbers. For example: “Machinist-Finalist.Outbreak9!Tidings”. Do not use a simple word as your password (ex: “[password](#)”); malicious actors use standard word dictionaries (and reverse, [l33t](#), foreign, ...) to attack websites.

- Have a note section with the account details to store, for example, the TOTP secret and backup codes, and answers to security questions (do not use the honest answer to “mother’s middle name”; use a two-word generated passphrase instead).
- **Never** store your information unencrypted on your device or in the cloud they use for synchronization. Data must be kept as encrypted blobs at rest and in transit. Those blobs only make sense once decrypted with your master password (and other augmentations to their encryption, such as [Password-Based Key Derivation Functions \(PBKDF\)](#)). The corollary is that if you lose your master password, the PM vendor cannot help you recover your data.

New solutions to traditional passwords have emerged, and first-party support is being provided on modern devices. [Passkeys](#), from the [Fast Identity Online \(FIDO\)](#) alliance, are cryptographic key pairs (public and private) stored on devices and used to verify that you are who you claim to be. As the solutions expand, those are becoming more integrated into new devices and password managers. Not all websites support the FIDO protocols, and any key-pair generated is stored by default on the device or application that joined the site. So, for example, if you use [passkeys](#) in [Chrome](#), those will not be available to you in Firefox unless you store them in a compatible PM that you can use on multiple devices ([Mac/Linux/Win/iOS/Android](#)).

Data backup

Regularly back up your important data to an external hard drive or cloud storage service (prefer an “and” here). This ensures you can recover your data in case of a ransomware attack or other data loss incident. A robust backup strategy should incorporate a combination of on-site, off-site, and cloud backups to ensure maximum data protection and recovery options. This multi-layered approach follows the [3-2-1 backup rule](#), which recommends having:

- 3 copies of your data: Your original data plus two backups.
- 2 different media types: Store your backups on different media types (e.g., external hard drive, network-attached storage, cloud storage).
- 1 off-site location: Keep one backup copy in a separate physical location to protect against local disasters like fire, flood, or theft.



Closing

This document guides securing your home network and protecting your digital assets. By following the recommended best practices, you can significantly reduce the risk of cyber threats and ensure the privacy and integrity of your sensitive information. Implementing these proactive security measures can give you greater peace of mind and help you navigate the evolving landscape of cyber risks.

If you seek content to share with friends and family, PBS recently released "[Secrets in Your Data](#)" on YouTube. This video discusses how personal data is being extensively collected and tracked through our digital activities, often without our full awareness or consent. Encourage family members and friends to educate themselves on basic cybersecurity hygiene. A shared understanding can strengthen your household's overall security posture.

Several reputable cybersecurity newsletters provide the latest industry news, analysis, and insights. To get started, you can pick one of SysAdmin, Audit, Network, and Security (SANS)'s [three newsletters](#): the "NewsBites" is a "semiweekly executive summary of the most important cyber security news articles published recently," "@RISK" is a "weekly summary of newly discovered attack vectors, vulnerabilities with active new exploits, insightful explanations of how recent attacks worked, and other valuable data," and the "OUCH! Newsletters" aims to educate and inform ordinary computer users on how to use the internet and practice good cybersecurity habits safely.

Cybersecurity is a complex process that is not just for IT people; it's a shared responsibility to protect our homes and businesses. Everyone plays a role in digital defense, from securing your smart fridge to safeguarding company secrets.

Soon, consumers will be able to make better-informed choices and contribute to a safer digital landscape when purchasing new smart devices. In late 2024, some IoT devices will bear the "[U.S. Cyber Trust Mark](#)," a voluntary cybersecurity certification and labeling program introduced by the Biden-Harris Administration and the Federal Communications Commission (FCC) for consumer IoT devices. The program intends to adopt the cybersecurity criteria outlined by the National Institute of Standards and Technology (NIST) in [NIST IR 8259 "Foundational Cybersecurity Activities for IoT Device Manufacturers,"](#) which covers areas like asset identification, data protection, software updates, access control, security monitoring, etc. IoT device manufacturers can voluntarily submit their products for cybersecurity testing by accredited third-party labs. Products that meet the specified security benchmarks will be authorized to bear the U.S. Cyber Trust Mark label and QR code.

Finally, look at the "Software Update" on your different devices. At the time of the initial writeup of this document (mid-May 2024), iOS, Windows, Chrome, and some router vendors have updated their OS versions with security updates known to be exploited.

Disclaimer

Certain equipment or software, commercial or non-commercial, might be identified in this document. Such identification does not imply recommendation or endorsement of any product or service, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

The opinions, recommendations, findings, and conclusions in this document do not necessarily reflect the views or policies of Infotrend Inc.