Best Practices for Securing Your Home Network

Executive summary

Don't be a victim! Malicious cyber actors may leverage your home network to gain access to personal, private, and confidential information. Help protect yourself, your family, and your work by practicing cybersecurity-aware behaviors, observing some basic configuration guidelines, and implementing the following mitigations on your home network, including:

- Upgrade and update all equipment and software regularly, including routing devices
- Exercise secure habits by backing up your data and disconnecting devices when connections are not needed
- Limit administration to the internal network only

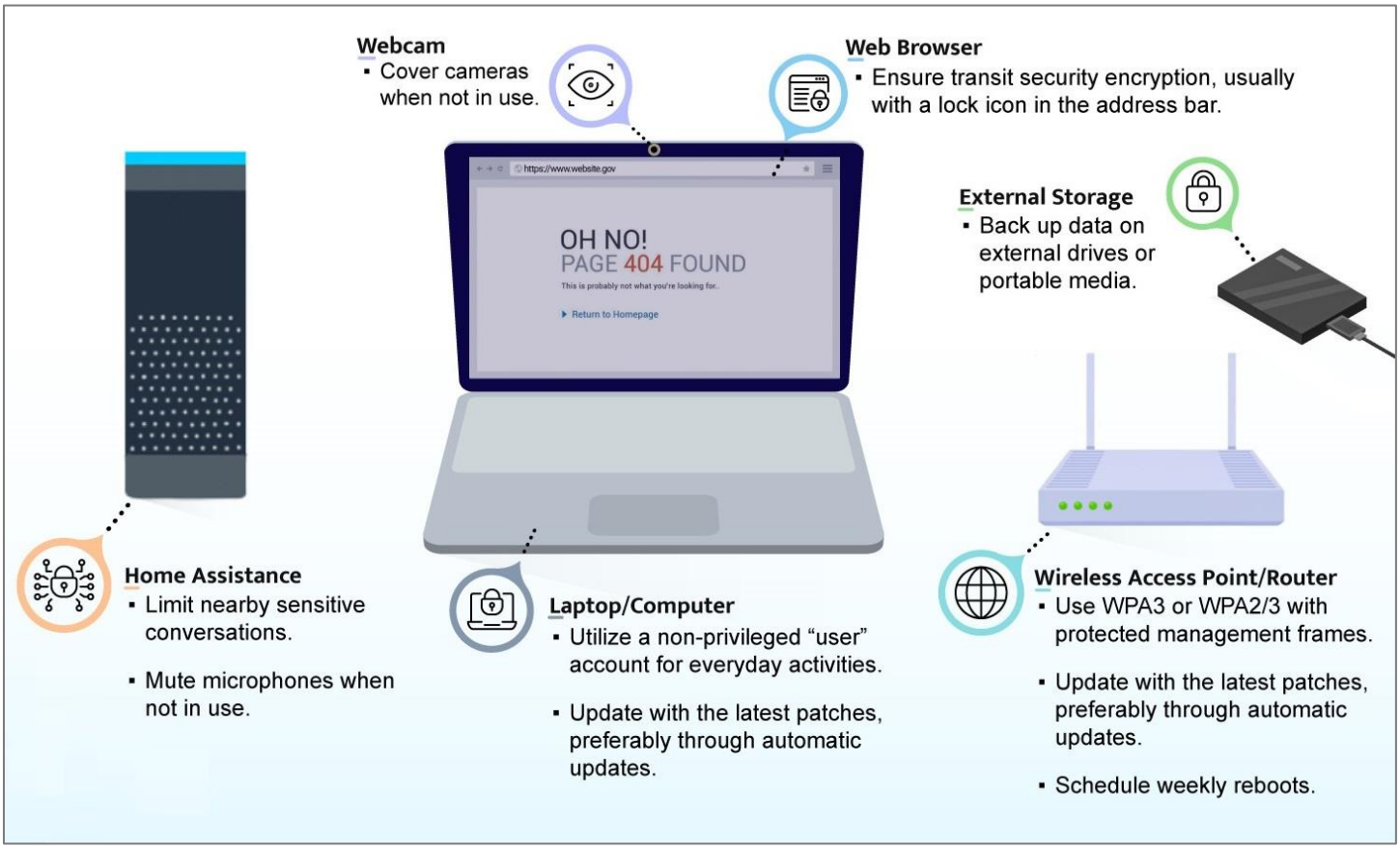

Figure: Several best practices for securing your home network

Recommendations for device security

Electronic computing devices, including computers, laptops, printers, mobile phones, tablets, security cameras, home appliances, cars, and other “Internet of Things” (IoT) devices must all be secured to reduce the risk of compromise. Most home entertainment and utility devices, such as home monitoring systems, baby monitors, IoT devices, smart devices, Blu-ray™ players, streaming video players, and video game consoles, are capable of accessing the Internet, recording audio, and/or capturing video. Implementing security measures can ensure these devices don’t become the weak link in your home protection.

Upgrade to a modern operating system and keep it up-to-date

The most recent version of any operating system (OS) contains security features not found in previous versions. Many of these security features are enabled by default and help prevent common attack vectors. Increase the difficulty for an adversary to gain privileged access by using the latest available and supported OS for desktops, laptops, and smart 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.

Secure routing devices and keep them up-to-date

Your Internet Service Provider (ISP) may provide a modem/router as part of your service contract. To maximize administrative control over the routing and wireless features of your home network, consider using a personally owned routing device that connects to the ISP-provided modem/router. In addition, use modern router features to create a separate wireless network for guests, for network separation from your more trusted and private devices.

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. To minimize vulnerabilities and improve security, the routing devices on your home network should be updated to the latest patches, preferably through automatic updates. These devices should also be replaced when they reach end-of-life (EOL) for support. This ensures that all devices can continue to be updated and patched as vulnerabilities are discovered.

Implement WPA3 or WPA2 on the wireless network

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. This allows newer devices to use the more secure method while still allowing older devices to connect to the network over WPA2.

When configuring WPA3 or WPA2/3, use a strong passphrase with a minimum length of twenty characters. When available, protected management frames should also be enabled for added security. Most computers and mobile devices now support WPA3 or WPA2. If you are planning to purchase a new device, ensure it is WPA3-Personal certified. 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.

Implement wireless network segmentation

Leverage network segmentation on your home network to keep your wireless communication secure. At a minimum, your wireless network should be segmented between your primary Wi-Fi, guest Wi-Fi, and IoT network. This segmentation keeps less secure devices from directly communicating with your more secure devices.

Employ firewall capabilities

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. Wireless access points (WAP) generally do not provide these capabilities so it may be necessary to purchase a router. If your ISP supports IPv6, ensure your router supports IPv6 firewall capabilities.

Leverage security software

Leverage security software that provides layered defense via anti-virus, anti-phishing, anti-malware, safe browsing, and firewall capabilities. The security suite may be built into the operating system or available to install as a separate product on computers, laptops, and tablets. However, some devices, such as home assistants, smart devices, and other IoT devices, may not support installing security suites. Modern endpoint detection and response software use cloud-based reputation services for detecting and

preventing execution of malware. Full disk encryption should be implemented where possible on laptops, tablets, and mobile phones to prevent data disclosure if that device is lost or stolen—many mobile devices enable disk encryption by default and security software can make it as easy as pushing a button.

Protect passwords

Ensure that passwords and answers to challenge questions are properly protected since they provide access to personal information. 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 on the system or anywhere a malicious actor might have access. Using a password manager is highly recommended because it allows you to use unique, complex passwords without needing to remember them.

Limit use of the administrator account

The highly privileged administrator account can access and potentially overwrite all files and configurations on your system. Because it can access more files, malware can more effectively compromise your system if it is executed while you are logged on as an administrator. To prevent this, create a non-privileged “user” account for normal, everyday activities, such as web browsing, email access, and file creation/editing. Only use the privileged account for maintenance, installations, and updates.

Safeguard against eavesdropping

Be aware that home assistants and smart devices have microphones and are listening to conversations, even when you are not actively engaging with the device. If compromised, the adversary can eavesdrop on conversations. Limit sensitive conversations when you are near baby monitors, audio recording toys, home assistants, and smart devices. Consider muting their microphones when not in use. For devices with cameras (e.g., laptops, monitoring devices and toys) cover cameras when you are not using them. Disconnect Internet access if a device is not commonly used, but be sure to update it when you do use it.

Exercise secure user habits

To minimize ransomware risks, back up data on external drives or portable media. Disconnect and securely store external storage when not in use. Minimize charging mobile devices with computers; use the power adapter instead. Avoid connecting

devices to public charging stations. Leave computers in sleep mode to enable downloading and installing updates automatically. Regularly reboot computers to apply the updates. Turn off devices or disconnect their Internet connections when they will not be used for an extended time, such as when going on vacation.

Limit administration to the internal network only

Disable the ability to perform remote administration on the routing device. Only make network configuration changes from within your internal network. Disable Universal Plug-n-Play (UPnP). These measures help close holes that may enable an attacker to compromise your network.

Schedule frequent device reboots

To minimize the threat of non-persistent malicious code on your personally owned device, reboot the device periodically. Malicious implants have been reported to infect home routers without persistence. At a minimum, you should schedule weekly reboots of your routing device, smartphones, and computers. Regular reboots help to remove implants and ensure security. For more guidance on better protecting your smartphone, refer to the "Mobile Device Best Practices" CSI.

Ensure confidentiality during telework

The security of your home network can directly affect not only your personal information, but also your work information and networks when teleworking. Using a virtual private network (VPN) to remotely connect to your internal corporate network via a secure tunnel is one solution for securely accessing work information. This provides an added layer of security while allowing you to take advantage of services normally offered to on-site users. For more guidance on securing your VPN, refer to the "Selecting and Hardening Remote Access VPN Solutions" cybersecurity information guidance (CSI).

When connecting to other work services, such as websites and cloud-based office apps, be sure that it is also through a secure tunnel by checking for a lock icon on the web browser's address bar. If you utilize commercial collaboration services, choose one that provides strong encryption, preferably end-to-end encryption. For an in-depth look at some commercial collaboration platforms refer to the "Selecting and Safely Using Collaboration Services for Telework" CSI.

Recommendations for online behavior

Spearphishing, malicious ads, email attachments, and untrusted applications can present concerns for home Internet users. To avoid revealing sensitive information, abide by the following guidelines while accessing the Internet.

Follow email best practices

Email is a potential attack vector for hackers. The following recommendations help reduce exposure to threats:

- Avoid opening attachments or links from unsolicited emails. Exercise cyber hygiene; do not open unknown emails or click on their attachments or web links. Check the identity of the sender via secondary methods (phone call, in-person) and delete the email if verification fails. For those emails with embedded links, open a browser and navigate to the web site directly by its well-known web address or search for the site using an Internet search engine.
- To prevent reusing any compromised passwords, use a different password for each account. Consider using a password manager to create and remember strong, unique passwords.
- Avoid using the out-of-office message feature unless it is necessary. Make it harder for unknown parties to learn about your activities or status.
- Always use secure email protocols, particularly if using a wireless network. Configure your email client to use the transport layer security (TLS) option (Secure IMAP or Secure POP3) to encrypt your email in transit between the mail server and your device.
- Never open emails that make outlandish claims or offers that are “too good to be true.”

Upgrade to a modern browser and keep it up-to-date

Modern browsers are much better at prompting users when security features are not enabled or used. Modern browsers help protect the confidentiality of sensitive information in transit over the Internet. The browser should be kept up-to-date. When conducting activities such as account logins and financial transactions, the browser’s URL tab indicates that transit security is in place, usually with a lock icon.

Take precautions on social networking sites

Social networking sites are a convenient means for sharing personal information with family and friends. However, this convenience also brings a level of risk. To protect yourself, refer to the "Keeping Safe on Social Media" CSI guidance and do the following:

- Avoid posting information, such as addresses, phone numbers, places of employment, and other personal information, that can be used to target or harass you. Some scam artists use this information, along with pet names, first car make or model, and streets you have lived on, to figure out answers to account security questions.
- Limit access of your information to "friends only" and verify any new friend requests outside of social networking.
- Be cautious of duplicate or copycat profiles of current friends, family, or coworkers. Malicious actors may use impersonated accounts to query you for privileged information or target you for spearphishing.
- Review the security policies and settings available from your social network provider quarterly or when the site's Terms of Use policy changes, as the defaults can change. Opt-out of exposing personal information to search engines.
- Take precautions concerning unsolicited requests and links. Adversaries may attempt to get you to click on a link or download an attachment that may contain malicious software.

Authentication safeguards

- Enable strong authentication on your router. Protect your login passwords and take steps to minimize misuse of password recovery options.
- Disable features that allow web sites or programs to remember passwords. Use a password manager instead.
- Many online sites use password recovery or challenge questions. To prevent an attacker from leveraging personal information to answer challenge questions, consider providing a false answer to a fact-based question, assuming the response is unique and memorable.

- Use multi-factor authentication (MFA) whenever possible. Examples of multi-factor authentication include secondary confirmation phone/email, security questions, and app/device-based identification. Some forms of MFA, such as app/device-based identification, are more secure and should be used over less secure methods, such as confirmation phone/email. When available, prefer using phishing-resistant MFA options.

Exercise caution when accessing public hotspots

Many establishments, such as coffee shops, hotels, and airports, offer wireless hotspots or kiosks for customers to access the Internet. Because the underlying infrastructure of these is unknown and security may be weak, public hotspots are more susceptible to malicious activity. If you must access the Internet while away from home, avoid direct use of public wireless. When possible, use a corporate or personal Wi-Fi hotspot with strong authentication and encryption. If public access is necessary, refer to "Securing Wireless Devices in Public Settings" CSI for guidance and do the following:

- If possible, use the cellular network (that is, mobile Wi-Fi, 4G, or 5G services) to connect to the Internet instead of public hotspots. This option generally requires a service plan with a cellular provider.
- If you must use public Wi-Fi, use a trusted VPN. This option can protect your connection from malicious activities and monitoring.
- Exercise physical security in the public place. Do not leave devices unattended.

Do not exchange home and work content

The exchange of information between home systems and work systems via email or removable media may put work systems at an increased risk of compromise. Ideally, use organization-provided equipment and accounts to conduct work while away from the office. If using a personal device, such as through a Bring Your Own Device (BYOD) program, use corporate-mandated security products and guidance for accessing corporate resources and networks. Try to connect to a remote desktop or terminal server inside the corporate network rather than make copies of files and transport them between devices. Avoid using personal accounts and resources for business interactions. Always use a VPN or other secure channel to connect to corporate networks and services to ensure your data is secured through encryption.

Use separate devices for different activities

Establish a level of trust based on a device's security features and its usage. Consider segregating tasks by dividing them between devices dedicated to different purposes. For example, one device may be for financial/personally identifiable information (PII) use and another for games or entertainment for children.

Additional guidance

NSA cybersecurity guidance:

- Mobile Device Best Practices
- Secure Collaboration Platforms
- Compromised Personal Network Indicators and Mitigations
- NSA's Top Ten Cybersecurity Mitigation Strategies
- Phishing resistant MFA
- Keeping Safe on Social Media
- Securing Wireless Devices in Public

General topics:

- National Information Assurance Partnership

Standards:

- NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-63 Digital Identity Guidelines

Disclaimer of endorsement

Trademarks

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

General cybersecurity inquiries: CybersecurityReports@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov