National Security Agency | Cybersecurity Information

Best Practices for Securing Your Home Network

Don't be a victim; cyber criminals may leverage your home network to gain access to personal, private, and confidential information. Help protect yourself and your family by observing some basic guidelines and implementing the following mitigations on your home network.

Computing and Entertainment Device Recommendations

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 in order to prevent attack. Most home entertainment and utility devices, such as home monitoring systems, baby monitors, IoT devices, Smart Devices, Blu-ray™[1] 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.

1. Upgrade to a Modern Operating System and Keep it Up-To-Date

The most recent version of any operating system (OS) inevitably 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 utilizing the latest available and supported OS for desktops, laptops, and other devices. Enable automatic update functionality inside the OS. If automatic updates are not possible, download and install patches and updates from a trusted vendor minimally on a monthly basis.

2. Exercise Secure User Habits

To minimize ransomware threat, backup data on external drives and portable media. Disconnect external storage when not in use. Disable or disconnect printer and fax wireless and phone lines when not in use. Power down access points overnight or when not in use. Minimize charging mobile with desktop; use the power adapter instead. Turn off desktop, instead of leaving in sleep mode. Disconnect a desktop’s internet connect when not in use.

3. 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 as a separate product. Modern endpoint detection and response software uses cloud-based reputation service for detecting and preventing execution of malware. To prevent data disclosure in the event that a laptop is lost or stolen, implement full disk encryption.

4. Safeguard against Eavesdropping

Disconnect digital assistants when not in use. Limit conversation near baby monitors, audio recordable toys, and digital assistants. For toys, laptops, and monitoring devices, cover cameras unless in direct use. Disable wireless for entertainment devices unless in use. Disconnect internet access if a device is not commonly used.

5. Protect Passwords

Ensure that passwords and challenge responses 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 an adversary might have access. Use passphrases and multi-factor authentication if available. Phrases should include multiple words and be unique per account.

[1] Blu-ray is a trademark of Blu-ray Disc Association.

6. Limit Use of the Administrator Account

The highly-privileged administrator account has the ability to access and potentially overwrite all files and configurations on your system. Malware can more effectively compromise your system if executed while you are logged on as an administrator, since it can access more files. 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 update. 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, use a personally-owned routing device that connects to the ISP-provided modem/router. Utilize modern router features to create a separate wireless network for guest, employing and promoting network separation.

7. 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 at 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.

8. Implement WPA2 on the Wireless Network

To keep your wireless communication confidential, ensure your personal or ISP-provided WAP is using Wi-Fi Protected Access 2 (WPA2). When configuring WPA2, use a strong passphrase of 20 characters or more. Most computers and mobile devices should now support WPA2. When identifying a suitable replacement, ensure the device is WPA2-Personal certified. Change the default SSID to something unique. Do not hide the SSID as this adds no additional security to the wireless network and may cause compatibility issues.

9. Limit Administration to the Internal Network

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.

Recommendations for Online Behavior

Spear Phishing, malicious ads, email attachments, and untrusted applications can present concern for home internet users. In order to avoid revealing sensitive information, abide by the following guidelines while accessing the Internet.

1. 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 and don’t 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 reuse of any compromised passwords, use a different password for each account. Periodically change your password.
- Avoid using the out-of-office message feature unless absolutely 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 TLS option (Secure IMAP or Secure POP3).
- Never open emails that make outlandish claims or offers “too good to be true.”

2. 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, do the following:

- Avoid posting information such as address, phone number, place of employment, and other personal information that can be used to target or harass you. Some scam artists make use of 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.
- 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.
- Refer to email best practices about precautions concerning unsolicited requests and links.

3. Authentication Safeguards

- Enable strong authentication on the router. Protect your login passwords and take steps to minimize misuse of password recovery options.
- Disable the feature that allows web sites or programs to remember passwords.
- Many online sites make use of 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 whenever possible. Examples of multi-factor authentication include secondary confirmation phone/email, security questions, and trusted device identification.

4. 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 is often weak, these hotspots are susceptible to adversarial activity. If you have a need to access the Internet while away from home, avoid direct use of public access. Avoid logging into any personal accounts.

- If possible, use the cellular network (that is, mobile Wi-Fi, 3G or 4G services) to connect to the Internet instead of public hotspots. This option generally requires a service plan with a cellular provider.
- If public Wi-Fi must be used, make use of a trusted virtual private network (VPN). This option can protect your connection from malicious activities and monitoring.
- Exercise physical security in the public place. Don’t leave devices unattended.

5. 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. It’s preferable to attach 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 to connect to corporate networks to ensure your data is secured through encryption.

6. 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.

7. 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 will show indication that transit security is in place.

Additional Guidance

Cybersecurity:

- https://www.nsa.gov

General topics:

- https://www.niap-ccevs.org/pp

Standards:

- http://csrc.nist.gov/publications/PubsSPs.html#800-124
- https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd

Disclaimer of Warranties and Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

This information was developed in the course of NSA's cybersecurity mission including its responsibilities to identify and disseminate information on threats to national security systems and Department of Defense information technologies, develop and issue security implementation specifications for cybersecurity-enabled products, and to assist Executive departments and agencies with operational security programs. The information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov