Best Practices for Keeping Your Home Network Secure



September 2016

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.

Electronic Computing Device Recommendations

Electronic computing devices include computers, laptops, printers, mobile phones, tablets, security cameras, home appliances, cars, and "Internet of Things" devices. Take special care to secure them and prevent misuse.

1. Migrate to a Modern Operating System

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. Utilizing the latest available and supported 64-bit OS for desktops and laptops increases difficulty of gaining privileged access to a computer by an adversary. Employ the OS auto-update feature to keep computers updated. Alternatively, download patches and updates from a trusted vendor on a monthly basis at a minimum.

2. Install a Security Suite

Install a comprehensive security suite that provides layered defense via anti-virus, anti-phishing, safe browsing, host-based intrusion prevention, and firewall capabilities. Several security suites also provide access to a 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.

3. Protect Passwords

Ensure that passwords and challenge responses are properly protected since they provide access to personal information. Passwords should be strong[1], unique for each account, and difficult to guess.

4. Limit Use of the Administrator Account

In every OS the highly-privileged administrator account has the ability to access all files and configurations on your system. Malware can more effectively compromise your system if executed while you are logged on as an administrator. 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.

5. Update Software from Trusted Sources

Attackers often exploit vulnerabilities in unpatched, outdated software applications running on your computing device. Enable the auto-update feature for applications that offer this option and promptly install patches. If automated updates are not available within an application, seek out products that can quickly survey the product health/status. For mobile devices, disable third-party software installations, don't jailbreak/root the device, and disable developer mode.

Network Recommendations

Home network devices include modems, routers, and wireless access points (WAP). These devices control the flow of information into and out of your network and should be carefully secured.

1. Improve Administrator Control

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. Use modern router features to create a separate wireless network for guests.

2. Employ Firewall Capabilities

Ensure 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. WAPs

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.

3. 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. Note that some computers may not support WPA2 and require a software or hardware upgrade. When identifying a suitable replacement, ensure the device is WPA2-Personal certified. Change the default SSID to something unique.

4. Limit Administration to the Internal Network

Disable the ability to perform remote/external 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.

5. Implement Strong Passwords on all Network Devices

For any network device that can be managed through a web interface, such as routers and printers, use a strong[1] and unique password. Devices with a missing, weak, or default passwords may allow attackers to infiltrate these devices and gain access to other internal systems.

Home Entertainment Device Recommendations

Most home entertainment devices, such as Blu-Ray players, streaming video players, and video game consoles, can access the Internet. Implement security measures to ensure these devices don't become a weak link in your network.

1. Protect the Device within the Network

Ensure the device is behind the home router/firewall to protect it from unfettered access from the Internet. In the case of a device that supports wireless, follow the Wireless LAN security guidance in this document.

2. Use Strong Passwords for Service Accounts

Home entertainment devices typically require you to sign up for additional service accounts or link with other social media accounts. Ensure that each account is protected with a strong[1], unique, and difficult to guess password.

Internet Behavior Recommendations

In order to avoid revealing sensitive information, abide by the following guidelines while accessing the Internet.

1. Authentication Safeguards

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 that pair with password login include secondary confirmation phone/email, security questions, and trusted device identification.

2. 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.

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.

Best Practices for Keeping Your Home Network Secure

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.

3. 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, it's preferable to attach to a remote desktop or terminal server inside the corporate network. 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.

4. Device Isolation

Establish a level of trust based on a device's security features and its usage. Consider segregating devices dedicated to different purposes. For example, one device may be for financial/PII use and another for games/children activities.

5. Enable the Use of TLS Encryption

Application encryption (TLS) over the Internet protects the confidentiality of sensitive information while in transit when logging into web based applications such as webmail, banking, and social networking sites. This prevents others from intercepting, reading, and potentially altering your data while in transit between you and the site.

When conducting activities such as account logins and financial transactions, ensure the web site supports TLS. Many browsers enable TLS by default; if an older browser must be used, select TLS over other encryption (SSL). Most web browsers provide some indication that TLS is enabled and is shown as "https:" in the URL or displayed as a lock icon for instance.

6. Follow Email Best Practices

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

- 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).
- Avoid opening attachments or links from unsolicited emails. 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.
- Never open emails that make outlandish claims or offers that seem "too good to be true."

7. 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.
- Limit access of your information to "friends only" and verify any new requests by phone.
- Review the security policies and settings available from your social network provider quarterly or when the site's Terms of Use changes. Opt-out of exposing personal information to search engines.
- Refer to email best practices about precautions concerning unsolicited requests and links.

Best Practices for Keeping Your Home Network Secure

References

[1] A strong password contains a mix of lower and uppercase characters, numbers, and symbols. It has a minimum length of 12 characters and does not use dictionary words or keyboard patterns.

Additional Guidance

IAD Mitigations (Top Ten, Identity Theft, Social Media, Operating Systems, Biometrics, Wireless)
https://www.nsa.gov

DISA STIGs A thru Z subjects
http://iase.disa.mil/stigs/Pages/a-z.aspx

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

Mobile Access Capability Package
https://www.nsa.gov

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

NIST
http://csrc.nist.gov/publications/PubsSPs.html#800-124

Protecting Personally Identifiable Information
http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

Contact Information

Industry Inquiries

410-854-6091
bao@nsa.gov

Client Requirements and General Information Assurance Inquiries

Client Contact Center
410-854-4200
IAD_CCC@nsa.gov