Best Practices for Keeping Your Home Network Secure

As a user with access to sensitive corporate or government information at work, you are at risk at home. In order to gain access to information typically housed on protected work networks, cyber adversaries may target you while you are operating on your less secure home network.

Don't be a victim. You can help protect yourself, your family, and your organization by following some common sense guidelines and implementing a few simple mitigations on your home network.

Personal Computing Device Recommendations

Personal computing devices include desktop computers, laptops, smartphones, and tablets. Because the bulk of your information is stored and accessed via these devices, you need to take special care in securing them.

1. Migrate to a Modern Operating System and Hardware Platform

The latest 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. In addition, using a 64-bit OS on a 64-bit hardware platform substantially increases the effort for an adversary to obtain privileged access on your computer.

2. Install A Comprehensive 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. In addition, several security suites, such as those from McAfee®[1], Norton®[2], and Symantec®[3], provide access to a cloud-based reputation service for leveraging corporate malware knowledge and history. Be sure to enable the suite's automatic update service to keep signatures up to date.

3. Limit Use of the Administrator Account

In your operating system, the highly-privileged administrator (or root) account has the ability to access any information and change any configuration on your system. Therefore, web or email delivered malware can more effectively compromise your system if executed while you are logged on as an administrator. Create a nonprivileged "user" account for the bulk of your activities including web browsing, e-mail access, and document creation/editing. Only use the privileged administrator account for system reconfigurations and software installations/ updates.

4. Use a Web Browser with Sandboxing Capabilities

Visiting compromised or malicious web servers is a common attack vector. Consider

using one of several currently available web browsers (e.g. Chrome™[4], Safari®[5]) that provide a sandboxing capability. Sandboxing contains malware during execution, thereby insulating the underlying operating system from exploitation.

5. Use a PDF Reader with Sandboxing Capabilities

PDF documents are a popular mechanism for delivering malware. Use one of several commercial or open source PDF readers (e.g. Adobe®[6], Foxit®[7]) that provide sandboxing capabilities and block execution of malicious embedded URLs (website links) within documents.

6. Update Application Software

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 or a new version when pop-up notifications indicate an update is available. Since many applications do not have an automated update feature, use one of several third-party products, such as those from Secunia and eEye Digital Security®[8], which can quickly survey installed software and report which applications are end-of-life or need patches or updates.

7. Implement Full Disk Encryption (FDE) on Laptops

To prevent data disclosure in the event that a laptop is lost or stolen, implement FDE. Most modern operating systems offer a built-in FDE capability, for example Microsoft's BitLocker®[9], Apple's Filevault®[10], or LUKS for Linux. If your OS does not offer FDE, use a third party product.

8. Download Software Only from Trusted Sources

To minimize the risk of inadvertently downloading malware, only download software and mobile device apps from reputable sources. On mobile devices, grant apps only those permissions necessary to function, and disable location services when not needed.

9. Secure Mobile Devices

Mobile devices such as laptops, smartphones, and tablets pose additional concerns due to their ease of use and portability. To protect against theft of the device and the information on the device, maintain physical control when possible, enable automatic screen locking after a period of inactivity, and use a hard-to-guess password or PIN. If a laptop must be left behind in a hotel room while travelling, power it down and use FDE as discussed above.

Network Recommendations

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

1. Configure a Flexible Home Network

Your Internet Service Provider (ISP) likely provides 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. Figure 1 depicts a typical small office/home office (SOHO) network configuration that provides the home user with a network that supports multiple systems as well as wireless networking and IP telephony services.

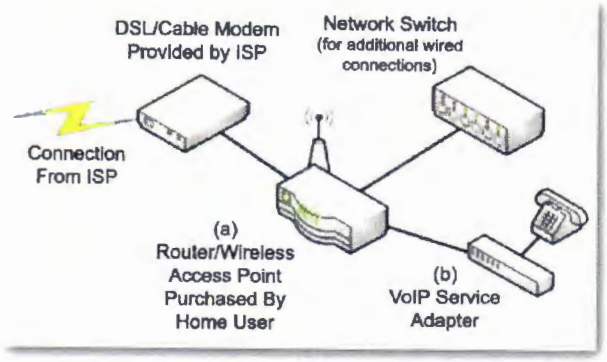

Figure 1: Typical SOHO Configuration

2. Disable Internet Protocol Version 6 (IPv6) Tunneling

Both IPv6 and its predecessor, IPv4, are used to transfer communications on the Internet. Most modern operating systems use IPv6 by default. If IPv6 is enabled on your device, but not supported by other systems/networks to which you are communicating, some OSes will attempt to pass IPv6 traffic in an IPv4 wrapper using tunneling capabilities such as Teredo, 6to4, or ISATAP (Intra-Site Automatic Tunnel Addressing Protocol). Because attackers could use these tunnels to create a hidden channel of communication to and from your system, you should disable tunneling mechanisms. In Windows, you can disable these through Device Manager (be sure to select "View hidden devices" under the View menu).

3. Provide Firewall Capabilities

To prevent attackers from scanning your network, ensure your personally-owned routing device supports basic firewall capabilities. Also verify that it supports Network Address Translation (NAT) to prevent internal systems from being accessed directly from the Internet. Wireless Access Points (WAPs) generally do not provide these capabilities so it may be necessary to purchase a wireless router, or a wired router in addition to the WAP. If your ISP supports IPv6, ensure your router supports IPv6 firewall capabilities in addition to IPv4.

4. 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) instead of the much weaker, and easily broken Wired Equivalent Privacy (WEP) or the original WPA. When configuring WPA2, change the default key to a complex, hard-to-guess passphrase. Note that older client systems and access points may not support WPA2 and will require a software or hardware upgrade. When identifying a suitable replacement, ensure the device is WPA2-Personal certified.

5. Limit Administration to the Internal Network

To close holes that would allow an attacker to access and make changes to your network, on your network devices, disable the ability to perform remote/external administration. Always make network configuration changes from within your internal network.

6. Implement an Alternate DNS Provider

The Domain Name System (DNS) associates domain names (e.g. www.example.com) with their numerical IP addresses. The ISP DNS provider likely does not provide enhanced security services such as the blocking and blacklisting of dangerous web sites. Consider using either open source or commercial DNS providers to enhance web browsing security.

7. Implement Strong Passwords on all Network Devices

In addition to a strong and complex password on your WAP, use a strong password on any network device that can be managed via a web interface, including routers and printers. For instance, many network printers on the market today can be managed via a web

interface to configure services, determine job status, and enable features such as e-mail alerts and logging. Without a password, or with a weak or default password, attackers could leverage these devices to gain access to your other internal systems.

Home Entertainment Device Recommendations

Home entertainment devices, such as blu-ray players, set-top video players (e.g. Apple TV®[11]), and video game controllers, are capable of accessing the Internet via wireless or wired connection. Although connecting these types of devices to a home network generally poses a low security risk, you can implement security measures to ensure these 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

Most home entertainment devices require you to sign up for additional services (e.g. Playstation®[12] Network, Xbox Live®[13], Netflix®[14], Amazon Prime®[15], iTunes®[16]). Follow the password guidance later in this document when creating and maintaining service accounts.

3. Disconnect When Not in Use

To prevent attackers from probing the network via home entertainment devices, if possible, disconnect these systems from the Internet when not in use. Some ISP modems/routers have a standby button you can use to disable the Internet connection.

Internet Behavior Recommendations

In order to avoid revealing sensitive information about your organization or personal life, abide by the following guidelines while accessing the Internet.

1. 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, follow these recommendations:

- If possible, use the cellular network (that is, mobile Wi-Fi, 3G or 4G services) to connect to the Internet instead of wireless hotspots. This option often requires a service plan with a cellular provider.

- Set up a confidential tunnel to a trusted virtual private network (VPN) service provider (for example, StrongSwan's StrongVPN). This option can protect your traffic from malicious activities such as monitoring. However, use of a VPN carries some inconvenience, overhead, and often cost. Additionally, you are still vulnerable during initial connection to the public network before establishing the VPN.

- If using a hotspot is the only option for accessing the Internet, limit activities to web browsing. Avoid accessing services such as banking websites that require user credentials or entering personal information.

2. Do Not Exchange Home and Work Content

The exchange of information (e.g. e-mails, documents) between less-secure home systems and work systems via e-mail or removable media may put work systems at an increased risk of compromise. If possible, use organization-provided laptops to conduct all work business from home. For those business interactions that are solicited and expected, have the contact send work-related correspondence to your work, rather than personal, e-mail account.

3. Be Cognizant of Device Trust Levels

Home networks consist of various combinations of wired and wireless devices and computers. Establish a level of trust based not only on a device's security features, but also its usage. For example, children typically are less savvy about security than adults and may be more likely to have malicious software on their devices. Avoid using a less savvy user's computer for online banking, stock trading, family photograph storage, and other sensitive functions.

4. Be Wary of Storing Personal Information on the Internet

Personal information historically stored on a local computing device is steadily moving to on-demand Internet storage called the cloud. Information in the cloud can be difficult to permanently remove. Before posting information to these cloud-based services, ask yourself who will have access to your information and what controls do you have over how the information is stored and displayed. In addition, be aware of personal information already published online by periodically performing a search using an Internet search engine.

5. Take Precaustions 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:

- Think twice about posting information such as address, phone number, place of employment, and other personal information that can be used to target or harass you.
- If available, limit access of your information to "friends only" and attempt to verify any new sharing requests either by phone or in person.
- Take care when receiving content (such as third-party applications) from friends because many recent attacks deliver malware by taking advantage of the ease with which content is generally accepted within the social network community.
- Periodically review the security policies and settings available from your social network provider to determine if new features are available to protect your personal information. For example, some social networking sites now allow you to opt-out of exposing your personal information to Internet search engines.
- Follow friends' profiles to see whether information posted about you might be a problem.

6. Enable the Use of SSL Encryption

Application encryption (SSL or TLS) over the Internet protects the confidentiality of sensitive information while in transit when logging into web based applications such as webmail and social networking sites. Fortunately, most web browsers enable SSL support by default.

When conducting sensitive personal activities such as account logins and financial transactions, ensure the web site uses SSL. Most web browsers provide some indication that SSL is enabled, typically a lock symbol either next to the URL for the web page or within the status bar along the bottom of the browser. Additionally, many popular web applications such as Facebook®[17] and Gmail®[18] have options to force all communication to use SSL by default.

7. Follow E-mail Best Practices

Personal e-mail accounts, either web-based or local to the computer, are common attack targets. The following recommendations will help reduce exposure to e-mail-based threats:

- Use different usernames for home and work e-mail addresses. Unique usernames make it more difficult for someone targeting your work account to also target you via your personal accounts.
- To prevent reuse of compromised passwords, use different passwords for each of your e-mail accounts.
- Do not set out-of-office messages on personal e-mail accounts, as this can confirm to spammers that your e-mail address is legitimate and can provide information to unknown parties about your activities.
- To prevent others from reading e-mail while in transit between your computer and the mail server, always use secure e-mail protocols (Secure IMAP or Secure POP3), particularly if using a wireless network. You can configure these on most e-mail clients, or select the option to "always use SSL" for web-based e-mail.
- Consider unsolicited e-mails containing attachments or links to be suspicious. If the identity of the sender cannot be verified, delete the e-mail without opening. For those e-mails 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.
- Be wary of any e-mail requesting personal information such as a password or social security number as any web service with which you currently conduct business should already have this information.

8. 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. Consider using a passphrase that you can easily remember, but which is long enough to make password cracking more difficult.
- Disable the feature that allows web sites or programs to remember passwords.
- Many online sites make use of password recovery or challenge questions. Your answers to these questions should be something that no one else would know or find from Internet searches or public records. To prevent an attacker from leveraging personal information about yourself to answer challenge questions, consider providing a false answer to a fact-based question, assuming the response is unique and memorable.
- Use two-factor authentication when available for accessing webmail, social networking, and other accounts. Examples of two-factor authentication include a one-time password verification code sent to your phone, or a login based on both a password and identification of a trusted device.

9. Avoid Posting Photos with GPS Coordinates

Many phones and newer point-and-shoot cameras embed GPS location coordinates when a photo is taken. An attacker can use these coordinates to profile your habits/pattern of life and current location. Limit the exposure of these photos on the Internet to be viewable only by a trusted audience or use a third-party tool to remove the coordinates before uploading to the Internet. Some services such as Facebook automatically strip out the GPS coordinates in order to protect the privacy of their users.

Additional Guidance

Social Networking:
http://www.nsa.gov/ia/_files/factsheets/I73-021R-2009.pdf

Mitigation Monday –
Defense Against Malicious E-mail Attachments:
http://www.nsa.gov/ia/_files/factsheets/MitigationMonday.pdf

Mitigation Monday #2 –
Defense Against Drive By Downloads:
http://www.nsa.gov/ia/_files/factsheets/I733-011R-2009.pdf

Hardening Tips

Mac OSX 10.6 Hardening Tips:
http://www.nsa.gov/ia/_files/factsheets/macosx_10_6_hardeningtips.pdf

Enforcing No Internet or E-mail from Privileged Accounts:
http://www.nsa.gov/ia/_files/factsheets/Final_49635NonInternetsheet91.pdf

Hardening Tips for the Default Installation of Red Hat Enterprise Linux 5:
http://www.nsa.gov/ia/_files/factsheets/rhel5-pamphlet-i731.pdf

Internet Protocol Version 6:
http://www.nsa.gov/ia/_files/factsheets/Factsheet-IPv6.pdf

Security Tips for Personally-Managed Apple iPhones and iPads:
http://www.nsa.gov/ia/_files/factsheets/iphonetips-image.pdf

Security Highlights of Windows 7:
http://www.nsa.gov/ia/_files/os/win7/win7_security_highlights.pdf

References

[1] McAfee® is a registered trademark of McAfee, Inc.

[2] Norton® is a registered trademark of Symantec

[3] Symantec® is a registered trademark of Symantec

[4] ChromeTM is a trademark of Google

[5] Safari® is a registered trademark of Apple

[6] Adobe® is a registered trademark of Adobe Systems, Inc.

[7] Foxit® is a registered trademark of Foxit Corp.

[8] eEye Digital Security® is a registered trademark of eEye, Inc.

[9] BitLocker® is a registered trademark of Microsoft

[10] Filevault® is a registered trademark of Apple

[11] Apple TV® is a registered trademark of Apple

[12] Playstation® is a registered trademark of Sony

[13] Xbox Live® is a registered trademark of Microsoft

[14] Netflix® is a registered trademark of Netflix.com, Inc.

[15] Amazon Prime® is a registered trademark of Amazon Technologies, Inc.

[16] iTunes® is a registered trademark of Apple

[17] Facebook® is a registered trademark of Facebook

[18] Gmail® is a registered trademark of Google

Contact Information

Industry Inquiries
410-854-6091
bao@nsa.gov

USG/IC Customer Inquiries
410-854-4790

DoD/Military/COCOM Customer Inquiries
410-854-4200

General Inquiries
NSA Information Assurance Service Center
niasc@nsa.gov