What is home network security and why should I care?

Home network security refers to the protection of a network that connects devices—such as routers, computers, smartphones, and Wi-Fi-enabled baby monitors and cameras—to each other and to the internet within a home.

Many home users share two common misconceptions about the security of their networks:

1. Their home network is too small to be at risk of a cyberattack.
2. Their devices are “secure enough” right out of the box.

Most attacks are not personal in nature and can occur on any type of network—big or small, home or business. If a network connects to the internet, it is inherently more vulnerable and susceptible to outside threats.

How do I improve the security of my home network?

By following some of the simple but effective mitigation techniques below, you can significantly reduce the attack surface of your home network and make it more difficult for a malicious cyber actor to launch a successful attack.

- **Update your software regularly.** Regular software updates are one of the most effective steps you can take to improve the overall cybersecurity posture of your home networks and systems. Besides adding new features and functionality, software updates often include critical patches and security fixes for newly discovered threats and vulnerabilities. Most modern software applications will automatically check for newly released updates. If automated updates are not available, consider purchasing a software program that identifies and centrally manages all installed software updates.
- **Remove unnecessary services and software.** Disable all unnecessary services to reduce the attack surface of your network and devices, including your router. Unused or unwanted services and software can create security holes on a device’s system, which could lead to an increased attack surface of your network environment. This is especially true with new computer systems on which vendors will often pre-install a large number of trial software and applications—referred to as “bloatware”—that users may not find useful. The Cybersecurity and Infrastructure Security Agency (CISA) recommends that you research and remove any software or services that are not being used regularly.
- **Adjust factory-default configurations on software and hardware.** Many software and hardware products come “out of the box” with overly permissive factory-default configurations intended to make them user-friendly and reduce the troubleshooting time for customer service. Unfortunately, these default configurations are not geared

towards security. Leaving them enabled after the installation may create more avenues for an attacker to exploit. Users should take steps to harden the default configuration parameters to reduce vulnerabilities and protect against intrusions.

- **Change default log-in passwords and usernames.** Most network devices are pre-configured with default administrator passwords to simplify setup. These default credentials are not secure—they may be readily available on the internet, or may even be physically labeled on the device itself. Leaving these unchanged creates opportunities for malicious cyber actors to gain unauthorized access to information, install malicious software, and cause other problems.
- **Use strong and unique passwords.** Choose strong passwords to help secure your devices. Additionally, do not use the same password with multiple accounts. This way, if one of your accounts is compromised, the attacker will not be able to breach any other of your accounts.
- **Run up-to-date antivirus software.** A reputable antivirus software application is an important protective measure against known malicious threats. It can automatically detect, quarantine, and remove various types of malware, such as viruses, worms, and ransomware. Many antivirus solutions are extremely easy to install and intuitive to use. CISA recommends that all computers and mobile devices on your home network run antivirus software. Additionally, be sure to enable automatic virus definition updates to ensure maximum protection against the latest threats. **Note:** because detection relies on signatures—known patterns that can identify code as malware—even the best antivirus will not provide adequate protections against new and advanced threats, such as zero-day exploits and polymorphic viruses.
- **Install a network firewall.** Install a firewall at the boundary of your home network to defend against external threats. A firewall can block malicious traffic from entering your home network and alert you to potentially dangerous activity. When properly configured, it can also serve as a barrier for internal threats, preventing unwanted or malicious software from reaching out to the internet. Most wireless routers come with a configurable, built-in network firewall that includes additional features—such as access controls, web-filtering, and denial-of-service (DoS) defense—that you can tailor to fit your networking environment. Keep in mind that some firewall features, including the firewall itself, may be turned off by default. Ensuring that your firewall is on and all the settings are properly configured will strengthen the network security of your network. **Note:** your internet service provider (ISP) may be able to help you determine whether your firewall has the most appropriate settings for your particular equipment and environment.
- **Install firewalls on network devices.** In addition to a network firewall, consider installing a firewall on all computers connected to your network. Often referred to as host- or software-based, these firewalls inspect and filter a computer’s inbound and outbound network traffic based on a predetermined policy or set of rules. Most modern Windows and Linux operating systems come with a built-in, customizable, and feature-rich firewall. Additionally, most vendors bundle their antivirus software

with additional security features such as parental controls, email protection, and malicious websites blocking.

- **Regularly back up your data.** Make and store—using either external media or a cloud-based service—regular backup copies of all valuable information residing on your device. Consider using a third-party backup application, which can simplify and automate the process. Be sure to encrypt your backup to protect the confidentiality and integrity of your information. Data backups are crucial to minimize the impact if that data is lost, corrupted, infected, or stolen.
- **Increase wireless security.** Follow the steps below to increase the security of your wireless router. **Note:** consult your router's instruction manual or contact your ISP for specific instructions on how to change a particular setting on your device.
    - *Use the strongest encryption protocol available.* CISA recommends using the Wi-Fi Protected Access 3 (WPA3) Personal Advanced Encryption Standard (AES) and Temporary Key Integrity Protocol (TKIP), which is currently the most secure router configuration available for home use. It incorporates AES and is capable of using cryptographic keys of 128, 192, and 256 bits. This standard has been approved by the National Institute of Standards and Technology (NIST).
    - *Change the router's default administrator password.* Change your router's administrator password to help protect it from an attack using default credentials.
    - *Change the default service set identifier (SSID).* Sometimes referred to as the "network name," an SSID is a unique name that identifies a particular wireless local area network (WLAN). All wireless devices on a Wireless Local Area Network (WLAN) must use the same SSID to communicate with each other. Because the device's default SSID typically identifies the manufacturer or the actual device, an attacker can use this to identify the device and exploit any of its known vulnerabilities. Make your SSID unique and not tied to your identity or location, which would make it easier for the attacker to identify your home network.
    - *Disable Wi-Fi Protected Setup (WPS).* WPS provides simplified mechanisms for a wireless device to join a Wi-Fi network without the need to enter the wireless network password. However, a design flaw in the WPS specification for PIN authentication significantly reduces the time required for a cyberattacker to brute force an entire PIN, because it informs them when the first half of the eight-digit PIN is correct. Many routers lack a proper lockout policy after a certain number of failed attempts to guess the PIN, making a brute-force attack much more likely to occur.
    - *Reduce wireless signal strength.* Your Wi-Fi signal frequently propagates beyond the perimeters of your home. This extended emission allows eavesdropping by intruders outside your network perimeter. Therefore, carefully consider antenna placement, antenna type, and transmission power levels. By experimenting with your router placement and signal strength levels, you can

    decrease the transmitting coverage of your Wi-Fi network, thus reducing this risk of compromise. **Note:** while this reduces your risk, a motivated attacker may still be able to intercept a signal that has limited coverage.

    - *Turn the network off when not in use.* While it may be impractical to turn the Wi-Fi signal off and on frequently, consider disabling it during travel or extended periods when you will not need to be online. Additionally, many routers offer the option to configure a wireless schedule that will automatically disable the Wi-Fi at specified times. When your Wi-Fi is disabled, you prevent outside attackers from being able to exploit your home network.
    - *Disable Universal Plug and Play (UPnP) when not needed.* UPnP is a handy feature that allows networked devices to seamlessly discover and establish communication with each other on the network. However, though the UPnP feature eases initial network configuration, it is also a security risk. Recent large-scale network attacks prove that malware within your network can use UPnP to bypass your router's firewall, allow attackers to take control of your devices remotely, and spread malware to other devices. You should therefore disable UPnP unless you have a specific need for it.
    - *Upgrade firmware.* Check your router manufacturer's website to ensure you are running the latest firmware version. Firmware updates enhance product performance, fix flaws, and address security vulnerabilities. **Note:** some routers have the option to turn on automatic updates.
    - *Disable remote management.* Most routers offer the option to view and modify their settings over the internet. Turn this feature off to guard against unauthorized individuals accessing and changing your router's configuration.
    - *Monitor for unknown device connections.* Use your router manufacturer's website to monitor for unauthorized devices joining or attempting to join your network. Also see the manufacturer's website for tips on how to prevent unauthorized devices from connecting to your network.

- **Mitigate Email Threats**. Phishing emails continue to be one of the most common initial attack vectors employed by for malware delivery and credential harvesting. Attacking the human element—considered the weakest component in every network—continues to be extremely effective. To infect a system, the attacker simply has to persuade a user to click on a link or open an attachment. The good news is that there are many indicators that you can use to quickly identify a phishing email. The best defense against these attacks is to become an educated and cautious user and familiarize yourself with the most common elements of a phishing attack.

Authors

CISA