SVG CONTENT SECURITY BEST PRACTICES

Work From Home? These Guidelines Can Help Keep Your Home Network Safe

Here are some basic steps in protecting your network from incursions and other threats.

BY

Tom Sahara
SVG Content Security Work Group Co-Chair

As "work from home" (WFH) continues to be important in a wide variety of industries, a reliable internet connection is more critical than ever. And, of course, there are the news headlines about hacked companies scrambling to recover from ransomware attacks and data leaks. WFH exposes company IT systems to a wide array of exposures and threats.

New electronic devices can open new vulnerabilities in work-from-home setups.

The company's IT department can help employees configure their home networks to improve security, but they are often overwhelmed with higher-priority tasks, leaving many employees to figure it out alone. This guide is intended to provide basic home-network security measures to reduce exposure to bad actors, such as gangs and loosely organized hacking groups, bored teens looking to finance their online gaming, and the nosy neighbor with nothing better to do.

Internet modems and gateways provided by internet service providers (ISPs) typically offer only minimal security options, including basic firewall functions. Regular network maintenance — virus and malware scans using latest profiles, updates to operating-system and application software on all connected devices — should be performed, and you should stay aware of latest phishing and malware attacks to avoid clicking on malicious links in texts and emails. But other steps can help in fortifying the home network from threats; here are a few suggestions.

HOME CONFIGURATIONS

WFH offers an opportunity to review the settings of the home router and network. There are two IP address settings in the router: the one provided by the internet service provider, and the address of the router in the home network. Home-network IP addresses are typically default Dynamic Host Configuration Protocol (DHCP) settings at 192.168.1.xxx, with the master administrator (admin) access address at 192.168.1.1. Changing the default range — for example, 192.168.20.xxx or 10.10.23.xxx — is good

start. Changing the admin address to an odd address can help prevent someone from accessing the admin page and trying to get in: for example, 192.168.20.52. Changing the router default login helps as well; admin/default is pretty easy to guess, and so is your email address.

Most home routers have firewall settings, which help stop external attempts to access the home network. Make sure that the firewall is enabled. Often, your employer will have you install software on your computer or place a router on your network. These often use a virtual-private-network (VPN) security protocol to connect your home to the company network.

A VPN is a quick and secure way to connect distant endpoints, allowing data to flow freely through an encrypted connection called a tunnel; a hacker can intercept the traffic but is unable to see what is inside. A VPN works great if you are connecting to only one remote network. If you must connect to several networks, ensure that you do not cascade or stack VPNs. Connect each VPN directly to your ISP router and, most important, do not install the VPN on the ISP router.

INTERNET SPEED

Although fast internet connections are often demanded, the reality is that you can likely be satisfied with less bandwidth than you think you need. As a guide, an internet connection with a minimum of 50Mb download and 25Mb upload speeds are required. There are different types of internet connections, and it is important to understand the type of service your provider offers so that you can set your expectations for performance.

Another consideration for advanced users is use of a “split-tunnel” VPN, which reduces the traffic flowing through by allowing it to flow directly to particular destinations, such as SaaS services like Office365, Webex, and Dropbox. One downside of a split tunnel is that the corporate IT department may not know what traffic is flowing from the home network to these destinations because the traffic no longer flows through corporate systems and monitoring.

Another factor that can affect the perceived speed of your connection is the DNS-server response time. Often, your ISP will default to its DNS server, which allows the provider to control what you are able to connect to, and your “speed” is dependent on the performance of the DNS server. You can often set a backup DNS server in case your ISP’s server experiences problems. Public DNS servers — such as OpenDNS (208.67.220.220/20 8.67.222.222), Google (8.8.8.8/8.8.4.4), Cloudflare (1.1.1.1/1.0.0.1), or Quad9 (9.9.9.9/149.112.112.112) — are freely available, and a paid DNS can provide phishing and malware filtering and other features.

WEB BROWSERS AND PASSWORDS

Many cloud products use a web browser for access, and all browsers have privacy and security settings. Though required by some services, pop-ups and cookies can be managed and set up to require permission. Here are some suggestions for basic settings that will not interfere with performance or accessibility:

- Use private browsing where possible. You can usually access this feature by clicking at the right end of the browser navigation bar.
- Use Do Not Track when possible. This setting is found in the Security or Privacy section.
- Use the browser Ask Before Saving feature for passwords and cookies.
- Disable automatic updates but be sure to get in the habit of checking for updates. The reason is that many browser-based applications are built for a specific browser version and you want to be sure that an automatic update does not cause unpredictable behavior of an app that is not compatible with the new browser version.

One important note is that, when multiple browsers tabs are open, they can communicate with each other. If a shopping site is open, the social-media site sees the browsing history and offers product.

When any browser or application is used, the first measure is to change default user accounts to unique names and default passwords to “strong” versions that can’t be guessed from user information. Avoid using common login information for every account. You may also use a password manager app but be sure that multi-factor authentication (MFA) is active to ensure that, if the password app is hacked, the infiltrators cannot access your account without the second authentication step, which is typically a short-message-service (SMS) text message, email, or phone call with a code that expires within a short period.

Single sign-on (SSO) — using FaceBook, Google, or LinkedIn accounts, for example — is convenient but also exposes more points of entry for hacking or theft. If you choose to use SSO, be sure to activate MFA features in those applications. Microsoft reports that more than 99% of its accounts that were compromised did not use MFA.

Microsoft recently posted a blog contending that “secure” passwords and SMS are not secure. Yes, it is true that SMS messages and phone calls are not encrypted, but that does not mean that you should abandon using “secure” passwords and MFA, which discourage the majority of attempts to infiltrate your network. Authentication apps and security-key managers do provide a higher level of security than SMS and voice-calling MFA, but they introduce their own limitations and management challenges.

WI-FI NETWORKS

The first step in protecting your home wireless network is to enable Wi-Fi security on your Wi-Fi access point (AP) and select the most secure protocol available. WEP, WPA, or WPA2 protocols are commonly offered in home-network routers.

Wired Equivalent Privacy (WEP), a legacy protocol, uses a static security key. It is the least secure and should be avoided, but, if that is all your equipment supports, it is better than no security.

Wi-Fi Protected Access (WPA) was introduced in 2003 to replace WEP but had its own set of weaknesses. Wi-Fi Protected Access II (WPA2) replaced WPA and incorporates AES encryption, making it more secure than WPA. Both WPA and WPA2 were found to have a vulnerability when the Wi-Fi Protected Setup (WPS) standard is used. It is recommended that WPS be turned off and the router firmware updated to versions that have removed WPS.

If you live in an apartment building and don't want others to see your network, you can disable the service-set ID (SSID), but this means that you need to remember and enter your Wi-Fi network name whenever you access it. Choose a strong password for your network to keep others from snooping on your Wi-Fi.

VIRTUAL LOCAL AREA NETWORKS (VLANS)

If your work requires access to secure corporate systems, it is advised that your network be split into separate virtual local-area networks (VLANs) to keep unauthorized parties out of the corporate network. A number of low-cost home routers and gateways provide VLAN capabilities that are simple to set up and maintain.

Home appliances, smart lights, doorbell cameras, baby cameras, and other internet-of-things (IOT) devices have been found to be easily compromised. Separating these devices on a separate VLAN can isolate the IOT traffic from your private home and work needs.

Using VPN within VLAN requires a bit more care than previously discussed, and it is best to consult with the company IT department or network administrators if you are using multiple VPN connections. Some routers feature Quality of Service (QoS), where certain VLANs and destinations can be prioritized ahead of other network traffic, ensuring that your gamer child does not bump you off your important Zoom presentation

with a new client. As with the use of VLANs, this requires a more advanced network topology, and you should consult your network administrator.

BACKUP OPTIONS

Besides basic access prevention, firewalls and gateways can also incorporate alternative connections in case of ISP outages. The ideal solution is to have a secondary high-speed connection from another service provider. As much as broadband is thought to be universally available, fast broadband is, in fact, limited to densely populated areas, such as large cities and their suburbs. Rural communities are often served by a single provider offering a limited number of services.

Several firewall and gateway systems have wireless-modem options that can be configured to automatically switch if your internet goes down. The backup wireless modems require a monthly data plan, and their speeds are typically only a fraction of those of the wired connection, but, in emergencies and mission-critical applications, they could keep you working.

POWER-LINE ETHERNET ADAPTERS AND WIRELESS EXTENDERS

Often, the home office may be in an unused room, attic, or basement where the Wi-Fi signal may be weak and getting a wire directly from the network router may be difficult. This is where power-line Ethernet adapters can help. Although the adapters advertise gigabit speeds, the typical installation achieves only about half the advertised speed, which, in many cases, is still much faster than the Wi-Fi. Power-line extenders are immune to interference from other Wi-Fi devices and can provide interruption-free connections for bandwidth-hungry uses.

Wireless-network extenders typically deploy mesh-network technology, which uses repeaters and a part of your Wi-Fi bandwidth to relay communications between distant devices and the main base unit. Though convenient to deploy and set up, mesh networks have inherent tradeoffs, such as reduced bandwidth and increased latency across the network. Bandwidth and low-latency needs are best satisfied by wired connections. Checking email and casual web browsing and viewing of Tik Tok and YouTube will work fine on a wireless network; online gaming may not.

POWER CONDITIONING AND UPS

In general, power utilities in major cities are good, but weather can cause problems. And what if you live in rural areas, where power glitches occur frequently? Uninterruptible power supplies (UPSs) have dropped in price and can easily remedy momentary dips and short outages. Fortunately, you aren't building a data center in your home; you need only enough capacity to keep the modem and computer running for a few minutes, enough time to let others know about the problem, save your work, and shut down your computer. UPSs of this size are readily available for under $200.

If your modem, router, and Wi-Fi access point are in different locations from your computer, you will need a UPS in each location. If you are using power-line Ethernet extenders, you will have to revert to Wi-Fi because they use power from the home electrical wiring.

SUMMARY

As WFH becomes a normal part of daily work lives and creating and maintaining a safe and cost-effective home internet network is a necessity. By following a few guidelines, you will be able to rest easier, knowing that you have done your best to ensure that your home network is secure and you are getting the most from your internet service.

If these steps and your fear of making a mistake seem imposing, there are consultants who can assist you. As with financial planners, don't pick the first one you meet; check references and do some research. You don't want to hand over sensitive personal and company information to someone you don't know.

Network technology is changing at a rapid pace, and hackers are adapting their attacks even more quickly. It's imperative, therefore, that you keep your virus and malware scanning up-to-date and regularly check for firmware and product updates to minimize your exposure to what is called the "threat attack surface." The basic steps discussed here barely scratch at the edges of the threat but will discourage the majority of intrusion attempts.

Hackers pursue easy targets, typically using malware introduced through phishing and click-baiting techniques. To entice people to click on a link, they deploy social-engineering principles, such as an email that looks like it comes from someone you know or from an "official" source. Corporate IT departments expend tremendous efforts in this area because it poses the greatest threat to their networks. Security reports note that as many

as 90% of corporate hacks have been the result of someone's clicking on a malicious link.

Each of the steps discussed here will individually contribute to improving the security and usability of your home network. In an increasingly technology-dependent world, getting the most out of your home network while keeping your family and employer safe is paramount. There is no 100%-secure method for protecting a network, but placing obstacles between the hacker and your network will eliminate the vast majority of intruders.

If you determine that an intrusion has occurred, there are resources available to help guide your next step. First is to immediately inform your company IT department and network administrator. Then, depending upon the severity of the breach, you can seek additional resources from FBI Internet Crime Complaint Center and FBI Cyber Crime (https://www.ic3.gov).

ABOUT SVG CONTENT SECURITY WORK GROUP

As network and content security continue to be a growing concern across the industry, the SVG Content Security Work Group has been created to strengthen the processes by which content is protected throughout the lifecycle of production, distribution, and archiving. Based on the input of SVG's membership — including broadcasters, rights owners, and production service providers — this Work Group is developing an ongoing series of Recommendations and Best Practices that outline suggested controls for individual consideration within the sports-production industry.

The SVG Content Security Best Practices documents provide rights owners, rights holders, and third-party vendors a clear and consistent understanding of general security expectations and current industry Best Practices. Decisions regarding use of individual vendors or the use of these Best Practices by any company are voluntary and agreed to between individual business partners.

Note: This is not an accreditation program, nor should any company promote that they have been assessed or accredited by SVG Content Security Work Group regarding their adherence or compliance with these Best Practices. Each suggested control is labeled with a prominent version number and date since they are subject to change periodically.