From the desk of
**Mendee L. Wyenandt**
Vice President of Operations
Chief Information Officer
EAGLE.bank

# Beware of Uninvited Holiday Guests (On your Network)

Whether you are finishing your holiday shopping or celebrating early, this is the time when you will likely be adding new devices to your home. While you may be taking a holiday vacation, hackers don't rest and are eagerly waiting for you to plug in your new devices so they can gain control.

This holiday season, stay one step ahead by securing your network and devices before cyber criminals get their chance.

## 1 Secure your Home Network.

With a few configuration changes you can greatly enhance the security of your home network. If you are unsure of how to perform the following steps, please consult the product support documentation for your router.

- **Change your router's password from the default to a secure password.** This will prevent others from accessing the router's configuration, changing settings, and gaining visibility into your network.
- **Enable automatic updates and install the latest router firmware.** Keeping your router up to date with the latest firmware helps protect it as new vulnerabilities are discovered.
- **Enable the router's firewall.** The firewall helps prevent the devices on your network from accessing malicious sites, as well as keeping outsiders on the outside of your network.
- **Change the Wireless Network Name (SSID).** The default wireless network name is typically the brand of the router, which can provide clues to outsiders as to what you are using and what vulnerabilities exist. Make sure you do not use your name, home address, or other personal information in your new SSID name. For added protection, disable broadcast of the wireless network name.
- **Enable Wireless Encryption.** Use Wi-Fi Protected Access 3 (WPA3) if supported by your device and choose a strong passphrase to connect devices to your network. When feasible, choose wired connections over wireless for enhanced security.
- **Enable a Wireless Guest Network.** A security best practice is to segregate network devices. Connect your computers, mobile devices, printers, and other trusted devices on your primary wireless network, while restricting devices such as Smart TVs, Personal Digital Assistants, and your refrigerator to the guest network.

## 2 Secure your Work-at-Home Devices.

Here are tips when working remotely both over the holidays and at any time.

- **Keep devices physically secured.** Always keep your devices with you and store them in a secure location when not in use. Set an idle timeout such as a password protected screen saver to automatically lock the device when you are not using it.
- **Keep devices up to date.** Enable automatic updates and install the newest updates for the operating system, antivirus software, and other software when available.

- **Secure data.** Save your work files, e-mails, and other data to authorized locations in your organization's network. Do not store your organization's data in your personal e-mail, cloud storage, or USB devices.
- **Use Secure Networks.** Never connect your work-at-home devices to untrusted networks such as public Wi-Fi. Instead, use your cell phone connection or a personal mobile hotspot when you are working outside of your home. If using an untrusted network is absolutely required and supported by your organization, use a virtual private network (VPN) to keep your network communications encrypted.

## 3 Secure your Personal Devices.

You may be tempted to plug in your new device and start to use it right away. Be sure to take a few minutes to configure security settings before you get started.

- **Change Default Passwords.** Some devices are configured with default passwords to simplify setup. If the password is not changed, these passwords are well-known and can give attackers full access to your device. Use strong and unique passwords for all your devices.
- **Deactivate features that you don't need.** Many devices are equipped with features such as location services, remote connectivity, Wi-Fi, and bluetooth. Each feature that is turned on is a potential opening for an attacker to access your device and gain control. Only use the features that you need and turn them off when not in use. If you don't need to connect a device to the internet, keep it offline and out of reach of hackers.
- **Update and Patch Regularly.** Manufacturers will issue updates as they discover vulnerabilities in their products. Configuring your device to receive automatic updates makes this easier for devices. However, if you need to manually update your device, make sure you are only applying updates directly from the manufacturer, as third-party sites and applications may be unreliable and can result in an infected device.
- **Secure Accounts.** Some personal devices such as gaming consoles require you to establish an account and maintain a subscription to access services. Pay close attention to the information being collected about you and the data that is visible to others. For gaming accounts, the default option may be to share the games that you play, when you are online, the number of hours played, and your contacts list to anyone who is subscribed to the same service. Change your privacy settings to only share data with people that you trust.

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™

The information provided in the MS-ISAC Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.