From the desk of
Michael Aliperti
MS-ISAC Chair

Securing New Devices/ Data Privacy Day

The holiday season has sadly come to an end, but hopefully you were able to treat yourself to some of the latest gadgets! Just remember that, however impressive the latest iPhone or gaming computer might be, the ability and knowledge to properly secure these devices is more important than ever, as any device that connects to the internet is potentially vulnerable and could become compromised. In honor of Data Privacy Day (January 28), here are five great tips to keep in mind that can help you securely configure your new devices!

1. Multi-factor authentication

If presented the opportunity, always enable multi-factor authentication (MFA) on your devices. This will ensure that only the person who has access to your account is you! If MFA is an option, enable it by using a trusted mobile device such as your smartphone, an authenticator app, or a secure token. For instance, with an iPhone you can utilize your screen lock feature with a PIN or password. MFA can prevent hackers from accessing your accounts, computer, and mobile devices. The availability of MFA is becoming more and more widespread, and for good reason!

2. Disable your location and safeguard yourself from monitoring devices

Location services might allow someone to see where you are located, so make sure you consider disabling this feature when you aren't utilizing your device. Additionally, consider disabling your Bluetooth feature when not in use as well. Bluetooth can be used to connect to other devices or computers and disabling this feature when not using your device can help to further secure your private information.

Another form of device to always be cognizant of is your digital assistant. If you use an Amazon Alexa, baby monitor, audio recordable device, or anything of that nature, always be sure to limit your conversations when they are on, and cover any cameras on toys, laptops, and monitoring devices when they are not in use.

3. Consider installing firewalls and antivirus software

Installing a firewall on your home network can help defend it against outside threats. For instance, a firewall can block malicious traffic from entering your network, while also alerting you to potentially dangerous activity. Please note that some firewall features, including the firewall itself, may be turned off by default, so ensure that your firewall is on and all the settings are properly configured, as this will greatly strengthen your security!

In addition to a network firewall, antivirus software can be a very protective measure against malicious activity. This type of software possesses the ability to detect, quarantine, and remove malware. Fortunately, this software is typically very easy to install and adds another protective shield to your security arsenal.

4. Patch & Update!

Quite often, technology has settings that allow for automatic updates to occur, and this is very important! Updates to your devices aren't always about creating a smoother and slicker interface. Manufacturers will typically issue updates when vulnerabilities in their products are discovered. A perfect example of this would be the update notifications you receive on your iPhone! Whether you have an iPhone or not, make sure that your device is configured to receive automatic updates. If updating your device is something that you need to do yourself manually, it is important that you ensure you are making updates directly from the manufacturer (i.e. Apple), as third-party applications could very well compromise your device.

5. Secure your Wi-Fi Network

The good news is that it isn't too difficult to make your wireless network and your devices more secure, and this can be completed in a few simple steps:

a. The first thing you should do to secure your network is change your router's default password to something more secure. Using a password manager is a great idea, as it will ensure you are only using strong passwords, such as those with special characters, numbers, upper- and lower-case letters, etc. This will prevent others from accessing the router and allow you to maintain the security settings you desire.

b. In addition to changing your password, it is also worth changing your SSID (Service Set Identifier), otherwise known as your wireless network name. Although changing this name won't necessarily enhance your network security, it will make it clear which network you are connecting to. Make sure you do not use your name, home address or other personal information in your new SSID name.

c. To further improve your defenses, you should also use Wi-Fi Protected Access 3 (WPA3). WPA3 is currently the strongest form of encryption for Wi-Fi. Other methods are outdated and thus, more vulnerable to exploitation.

Conclusion

In today's world we are more connected than ever — not only to each other, but to our devices. In the same manner in which you protect your physical assets, such as your bike with a padlock, you need to similarly protect your internet-connected devices! This is how Data Privacy Day came to fruition. This international event occurs every year on January 28, with the purpose of raising security awareness as well as highlighting data protection best practices.

In addition to its educational initiative, Data Privacy Day also promotes events and activities that aim to enhance the development of technology devices which promote individual control over personal information. For further information on Data Privacy Day and how you can get involved, please copy and paste the following link into your browser: https://staysafeonline.org/data-privacy-day/

Here's to a very cyber-safe New Year!

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™