CS

CYBER SECURITY & YOU

JANUARY 2021

SECURING NEW DEVICES / DATA

In honor of Data Privacy Day (January 28), here are five great tips 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. MFA can prevent hackers from accessing your accounts, computer, and mobile devices.

2 DISABLE YOUR LOCATION & SAFEGUARD YOURSELF FROM MONITORING DEVICES

You should consider disabling location services when you are not utilizing your device. Additionally, consider disabling your Bluetooth feature when not in use. 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. Always be cognizant of your digital assistant, baby monitor, or anything of that nature. 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 & 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 the firewall itself may be turned off by default, so ensure that your firewall is on. In addition, antivirus software can be a protective measure against malicious activity. This type of software possesses the ability to detect, quarantine, and remove malware. This software is 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. Manufacturers will typically issue updates when vulnerabilities in their products are discovered. An example of this is the update notification you receive on your iPhone. Whether you have an iPhone or not, make sure that your device is configured to receive automatic updates. Ensure you are making updates directly from the manufacturer (i.e. Apple), as third-party applications could compromise your device.

5 SECURE YOUR WI-FI NETWORK

1. Change your router's default password to something more secure. This will prevent others from accessing the router and allow you to maintain the security settings you desire.

2. You should also change your Service Set Identifier (SSID), otherwise known as your wireless network name. Although changing this will not necessarily enhance your network security, it will make it clear which network you are connecting to. Do not use your name, home address or other personal information in your new SSID name.

3. You should also use Wi-Fi Protected Access 3 (WPA3). WPA3 is currently the strongest form of encryption for Wi-Fi. ■

LASERS IT
Making Digital Retirement a Reality