6 CYBERSECURITY STEPS TO SECURE YOUR HOME WI-FI

Chatting online with friends, streaming movies, or banking online is convenient and easy. But cybercriminals look for vulnerabilities in almost any device connected to your home Wi-Fi network – from laptops and phones to security systems and thermostats – to infiltrate your home. Here are some key tips to help keep your home Wi-Fi network secure:

Review our 6 cybersecurity steps to help keep your personal information secure.

1 CHANGE THE DEFAULT NAME OF YOUR HOME WI-FI

First, change the SSID, (service set identifier), or the name of your home Wi-Fi network. Usually, manufacturers give all their wireless routers a default SSID—this gives hackers a better chance of breaking into your network. Consider your new SSID as something that does not disclose any personal information.

2 MAKE YOUR WIRELESS NETWORK PASSWORD UNIQUE AND STRONG

Most wireless routers come pre-set with a default password – making it easy to guess. Consider creating a password with at least 20 characters, including numbers, letters, and symbols.

3 ENABLE NETWORK ENCRYPTION

Almost all wireless routers come with an encryption feature, but most of them have it turned off. Turning on your wireless router's encryption setting helps secure your network, especially right after it is installed. Many types of encryptions are available, and the most recent and effective is "WPA2".

4 TURN OFF NETWORK NAME BROADCASTING

When using a wireless router in the privacy of your home, consider disabling the network name broadcasting to the general public. When nearby users try to find a Wi-Fi network, their device will show a list and your network name will not be included.

5 KEEP YOUR ROUTER'S SOFTWARE UP TO DATE

Sometimes a router's firmware, like any other software, contains flaws that have vulnerabilities, unless they're quickly fixed by the manufacturer. Always install the latest software available for your router and download the latest security patches immediately.

6 USE VPNS TO ACCESS YOUR NETWORK

A VPN (virtual private network) is a group of computers or networks that work together over the Internet. You can use VPNs to encrypt your communications and keep them secure. When you connect to a VPN and log in with your credentials, your computer exchanges keys with another server. Once both computers have verified each other as authentic, Internet activity is encrypted and hidden from outside prying.

Consider trying a few of the tips listed above even if you don't implement them all at this time.

Talk to our team about your options to help protect yourself online and offline.

INSGROUP
A BALDWIN RISK PARTNER