Consumer Alert

Contact:
Kenton Brine, President
Sandi Henke, Deputy Director
NW Insurance Council
Phone: (800) 664-4942

Release Date: 11-24-2020
kenton.brine@nwinsurance.org
sandi.henke@nwinsurance.org
Follow at Twitter/nwinsuranceinfo
Facebook/NWInsuranceCouncil

Shopping Black Friday from home this year? Make sure you are cyber-secure

What to Know

- *The frequency of cyber-attacks is expected to increase 70 percent over the next five years, according to a study.*

- *Implementing a cybersecurity strategy will help reduce your risk of a cyber-attack.*

- *More insurers are now offering Cyber Insurance Policies for homeowners and renters upon request as an endorsement or stand-alone policy.*

BOISE, November 24, 2020 – First comes Black Friday, then Cyber Monday. If the COVID-19 pandemic has you shopping online from home this year to get all the great deals, consider taking cyber-safety measures and adding cyber coverage to your insurance policy to help protect yourself or your business from a cyber-attack.

Cyber-attacks have become a constant threat in our daily lives, which means protecting ourselves and our businesses from cybercriminals is crucial to maintaining personal and financial well-being. Despite taking safety measures, savvy cybercriminals may still find a

way in, however. If a cyberattack occurs, having a Cyber Insurance Policy can assist with a quicker recovery.

"Whether we realize it or not, most of us are a single mouse-click or finger-tap away from giving criminals the keys that lock our online accounts," said Kenton Brine, NW Insurance Council President. "There are steps all consumers should take today to protect your personal and business finances online, including simple security measures as well as adding cyber-coverage to your insurance policies.

According to the [Insurance Information Institute](#) (I.I.I.), the cost of data breaches worldwide was approximately $3 trillion last year, and the frequency of cybersecurity breaches is expected to increase nearly 70 percent over the next five years.

More insurers are now offering cyber insurance policies for businesses, homeowners and renters. Policies may be available through a stand-alone policy or endorsement for homeowners and renters upon request but can differ by company. A policy may include coverage for identity restoration, attorney's fees and lost wages and may cover fees for a fraud specialist to manage the restoration process.

Some standard business insurance policies may already provide coverage for certain types of cyber incidents, such as recovery of data due to a computer virus. To extend coverage to a full range of cyber liability risks, however, a stand-alone cyber liability policy customized for your business will need to be purchased, according to [I.I.I.](#)

If you are concerned about a cyber-attack on your personal or business devices, contact your insurance company representative to discuss what cyber coverage options are available.

In the meantime, implementing a cybersecurity strategy will help reduce the risk of a cyber-attack. The NW Insurance Council and I.I.I. offer the following tips:

Personal Cybersecurity Tips

- **Keep software up to date.** Turn on automatic updates for your operating system and make sure browser plug-ins (such as Adobe Flash and Java) are up to date. Keeping your software updated minimizes threats from malware, hackers and other cyber risks.

- **Use anti-virus and firewall protection** to help block malware and viruses from entering your device. Be sure to use antivirus software only from trusted vendors. Also, utilizing a firewall will determine what internet traffic can enter your device and will screen out hackers, malware and viruses.

- **Use strong passwords and practice good password management.** Consider storing your passwords in a secure location using a password manager, such as LastPass.com, for example. Change your password every six months and make sure your passwords are strong and contain more the six digits, use special characters and include uppercase and lowercase letters.

- **Use multifactor authentication,** a security protocol that uses a secondary device to verify that you are who you say you are. Typically, verification codes are texted or emailed to you to enter when you sign-in.

- **Avoid phishing scams.** Cyber-criminals often use phone calls and email scams to trick email recipients into giving away personal information, such as banking or credit card information, or clicking a link that installs harmful software on a computer. Be suspicious of any email, text or phone call that asks for personal or financial information.

- **Keep your mobile devices secure** by creating a difficult password, only install apps from trusted sources and keep all apps updated. Also, avoid texting sensitive information and perform regular mobile backups to a cloud service.

- **Never leave your devices unattended.** If you need to leave your laptop, phone or tablet be sure to put them away in a secure place. If you are using a desktop computer, lock your screen.

Business Cybersecurity Tips

- **All businesses are vulnerable to cyber-attacks** through hacking, malware, phishing and more. Implement a cybersecurity strategy to help protect your business, employees and your customers.

- **Provide firewall security.** Make sure your business's operating system's firewall is enabled or install free firewall software from a trusted vendor. This will prevent cyber-criminals from accessing data on a private network.

- **Train your staff.** Enforce a computer password policy for employees and provide security awareness training. If you have employee's working remotely or from home, make sure their system is protected by a firewall, for example. If your employees use mobile devices for work, require and provide training on how to prevent business information from being stolen from those devices.

- **Keep computer software and hardware up to date.** Routinely check and upgrade your business's software, including operating systems, security software and web browsers. You may want to consider investing in an IT security services vendor. Make sure your systems have antivirus and firewall technology.

- **Back up your files and store them off-site** on an external hard drive or on a separate cloud account.

For more information about how to protect yourself and your business from a cyberattack, visit the U.S. Department of Homeland Security's [CISA](#) website. Also, read Mutual of Enumclaw's [Cybersecurity Checklist](#) for more details.

NW Insurance Council is a nonprofit, insurer-supported organization providing information about home, auto and business insurance to consumers, media and public policymakers in Washington, Oregon and Idaho.

###