NW Insurance Council

Consumer Alert

Contact:
Kenton Brine, President
Sandi Henke, Deputy Director
NW Insurance Council
Phone: (503) 465-6800 / (800) 664-4942

Release Date: 08-08-2024
kenton.brine@nwinsurance.org
sandi.henke@nwinsurance.org
Follow at Twitter/nwinsuranceinfo
Facebook/NWInsuranceCouncil

Is Personal Cyber Insurance worth the investment? Key factors to consider for digital protection

What to Know

- *The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) received a record number of 880,418 cybercrime complaints from Americans in 2023 with losses exceeding $12.5 billion.*
- *Oregon ranked 25th in the nation for cybercrime complaints last year with 6,724 complaints and $136 million in losses, according to IC3.*
- *More insurers are now offering Cyber Insurance Policies for homeowners and renters upon request as an endorsement or stand-alone policy.*

PORTLAND, OR, August 8, 2024 – A record number of Americans fell victim to cyber-attacks last year, according to the FBI, with more than 880,000 complaints and $12.5 billion in losses. As reliance on technology continues to grow, so does cybercrime. It's imperative to have robust cybersecurity measures to help prevent a cyber-attack. It's also worth considering Personal Cyber Insurance to help you recover after an attack.

Protecting ourselves from cybercriminals is crucial to maintaining personal and financial well-being. Even when users take safety measures, savvy cybercriminals may still find a way in through gaps in digital security strategies. If a cyber-attack occurs, having a Personal Cyber Insurance Policy can assist with a quicker recovery.

“These days, we lock our cars and we lock our front doors, but many people may not think about locking the electronic gateway to our personal finances – our bank accounts, credit cards and personal identities – that can be exploited by cybercriminals,” said NW Insurance Council President Kenton Brine. “It is critical to take simple steps to prevent access to your personal information online and through our devices, but it may also be time to consider a personal cyber insurance policy to help recover from financial loss.”

What is Personal Cyber Insurance?

Personal Cyber Insurance helps individuals and families recover financial losses due to cyber-crime, and assists with recovery from a wide variety of cyber-attacks, such as identity theft, cyberbullying and data breaches. While Cyber Insurance won’t keep an attack from happening, it can help you recover. Keep in mind that insurance typically only covers new events, so you can’t buy Personal Cyber Insurance after someone hacks your device and/or steals your identity or funds.

What does Personal Cyber Insurance cover?

It is important to note that many insurers underwrite personal cyber policies, and they may differ widely in what (and how much) they cover, what they exclude, what deductibles apply and how much they cost (the premium). Consumers interested in this coverage should reach out to a reputable homeowners or renters insurance provider, or contact an experienced professional insurance agent or broker to find out more.

Cyber-attack coverage: This pays for the removal of a virus or to reprogram laptops, smartphones, wi-fi routers, smart home devices and security systems, for example.

Cyber Extortion and Ransomware coverage: Cyber extortion involves illegally gaining access to sensitive data and demanding money in return for stopping the attack. Ransomware is a type of malware that locks down a computer until the victim pays to have the device unlocked. This coverage may include assistance to help you regain control of your files and data and may provide reimbursement for any ransom paid, if approved by your insurance company.

Identity Theft: Offers financial protection for victims of identity theft and helps cover the costs of restoring your identity, repair your credit and retrieve stolen data. It may be offered as an add-on to your homeowners or renters policy.

Financial or Deceptive Transfer Fraud: This coverage can help reimburse lost funds if you mistakenly send money to a criminal.

Data Breaches: If someone steals your personal information and publishes it online or posts false information about you, this coverage can pay for legal fees, lost wages and a review from experts on how your personal information was accessed.

Cyberbullying: If you or your child is a victim of online bullying, Personal Cyber Insurance may reimburse you for counseling expenses, the cost of temporary relocation, private tutoring and social media monitoring.

How do I get Personal Cyber Insurance? And what does it cost?

More insurers now offer 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.

According to Security.org, a Personal Cyber Insurance policy that is not part of an existing policy can cost up to $1,000 a year, or $3 a day, depending on the insurer and the coverage limits chosen. However, there are companies in the Washington market that may offer personal cyber insurance policies as an endorsement to an existing

Homeowners' or Renters' policy for a flat fee as low as $25 per year for up to $50,000 in coverage and a $500 deductible.

Having strong digital security already in place may help lower your premiums. Contact your insurance company representative to discuss what cyber coverage options are available to you.

In the meantime, implementing a cybersecurity plan will help reduce the risk of a cyber-attack. Here are a few tips to implement digital security for you and your family:

Personal Cybersecurity Tips

- 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.
- Use strong passwords and practice good password management. Consider storing your passwords in a secure location using a password manager. 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.
- 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.
- Make sure your software is up to date before online shopping. Turn on automatic updates for your operating system and make sure browser plug-ins (such as

Adobe Flash) are up to date. Keeping your software updated minimizes threats from malware, hackers and other cyber risks

- Avoid free public wi-fi for online shopping. If you plan to go to your favorite coffee shop to do some online shopping, using the shop's free wi-fi could make you vulnerable to cybercriminals. Use a virtual private network or your phone as a hotspot instead.
- Monitor your bank accounts on a regular basis so you catch and put a stop to suspicious activity/fraudulent purchases right away.
- Always verify the legitimacy of a vendor before supplying any information. Some attackers try to trick you by creating fake websites that appear legitimate to try and steal your information.
- Recognize and avoid phishing scams. If a link looks "off," CISA recommends you "think before you click." Cybercriminals 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.

For more information about how to protect yourself online, visit the U.S. Department of Homeland Security's CISA website.

If you believe you or another person has been a victim of a cybercrime, visit the Internet Crime Complaint Center (IC3) for more information and to file a complaint. For information about identify theft and how to file a complaint, visit the Federal Trade Commission's Identity Theft website.

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.

###