# Know Your Insurance

## Home

Courtesy of NXG Insurance Group LLC

## Personal Cyber Coverage Explained

Today's society has grown increasingly digital in nature, with many individuals leveraging smart devices within their daily lives. Although this technology can offer various benefits, it can also make individuals more susceptible to cybercrime. Such incidents have steadily become more common and costly. In fact, the FBI reported receiving more than 800,000 complaints regarding cybercrimes in the past year, totaling $4.2 billion in overall expenses.

These findings emphasize how critical it is for individuals to safeguard themselves and their families from cyber events. That's where personal cyber insurance can help. Typically offered as an endorsement to a homeowners policy, this form of coverage can provide financial protection for losses resulting from a range of cyber incidents—including fraud, identity theft and data breaches. Keep reading to learn more about the growing need for this coverage and the key types of personal cyber insurance available.

### The Growing Need for Personal Cyber Coverage

Technology has continued to advance in the past decade, playing a larger role in how individuals live, work, and entertain. A variety of online platforms have given individuals the ability to stream content, communicate with others, shop for goods and make electronic payments at the click of a button. Additionally, smart devices have allowed individuals to upgrade a number of household appliances (e.g., thermostats, fridges, doorbells and security systems). Altogether, this technology has contributed to the growing adoption of the Internet of Things (IoT), which refers to any devices that connect or send information to the internet. Looking ahead, insurance experts anticipate that the average household will possess as many as 50 IoT-capable gadgets by 2023.

While these devices certainly offer several advantages, increased technology utilization also comes with greater cyber vulnerabilities. As technology advances, so do the tactics of cybercriminals—resulting in more frequent and severe cyber events. Here are some of the most common cyber incident scenarios that individuals and their families may encounter:

- **Bank fraud**—This form of fraud entails a cybercriminal gaining unauthorized access to an individual's electronic bank credentials, allowing them to transfer and steal funds from the individual's account. According to a recent report from NortonLifeLock, cybercriminals steal over $170 billion each year via bank fraud.
- **Identity theft**—Such theft refers to a cybercriminal accessing an individual's personal information (e.g., Social Security number or credit card number) and using it to commit fraud or other crimes under the individual's name. The Federal Trade Commission confirmed that nearly 1.4 million complaints related to identity theft were filed last year, up 113% from the previous year.
- **Data loss**—In the event that an individual's device gets infected with a virus or other malicious software (also called malware), they face the risk of losing any valuable data stored on that device. Viruses and malware can come from numerous avenues, including harmful websites, dangerous email attachments or infected USB flash drives—thus making data loss a major threat.
- **Extortion**—Ransomware incidents have contributed to a substantial rise in cyber extortion over the last few years. These incidents stem from a cybercriminal using malware to compromise an individual's device (and any data stored on it) and

demanding a ransom payment in exchange for restoration. In some cases, the cybercriminal may even threaten to publicly share the individual's data if they don't receive payment. According to cybersecurity experts, ransomware incidents have increased 500% since 2018, with the average ransom payment totaling over $300,000.

- **Cyberbullying**—While social media platforms allow individuals to connect with others, these platforms can also, unfortunately, be used for negative purposes, such as cyberbullying. This type of bullying includes refers to harassment, threats or other intimidating language that occurs via electronic means. Although anyone can be a victim of cyberbullying, kids and teenagers are particularly vulnerable. The latest data from Pew Research revealed that 59% of teens have experienced cyberbullying.

Considering these risks, it's clear that individuals can't afford to ignore cybercrime. In addition to implementing effective cybersecurity practices (e.g., using trusted devices, browsing secure websites, conducting software updates, backing up data, creating unique passwords and knowing how to identify potential scams), having adequate insurance in place is crucial. By investing in personal cyber coverage, individuals can properly protect themselves and their families amid cyber-related losses.

**Types of Personal Cyber Coverage**

Personal cyber insurance varies between insurers. However, there are a number of key coverage offerings available:

- **Online fraud coverage**—This coverage can offer reimbursement for financial losses that may result from the various types of online fraud, such as phishing scams, identity theft or unauthorized banking.
- **Online shopping coverage**—Such coverage can help pay for the cost of any goods that were purchased online but arrived damaged upon delivery or didn't get delivered whatsoever.
- **Identity recovery coverage**—This coverage can provide reimbursement for the expenses associated with recovering from an identity theft incident (e.g., rectifying records with banks or other authorities, hiring a consultant to assist with credit restoration and taking unpaid time off from work to recover from the incident).
- **Data restoration coverage**—Such coverage can help compensate the cost of having an IT specialist recover a device and restore any data stored on it if the device gets infected with a virus or malware.
- **Data breach coverage**—This coverage can offer reimbursement for the necessary notification and recovery services in the event that private, nonbusiness data entrusted to the policyholder becomes lost, stolen or published.
- **Cyber extortion coverage**—Such coverage can help pay for the expenses associated with responding to a ransomware event (e.g., consulting an IT specialist to mitigate the extortion attempt and restoring compromised devices or data).
- **Cyberbullying coverage**—This coverage can provide reimbursement for the costs that come with recovering from a cyberbullying incident resulting in unlawful harassment or defamation of character. These costs may include psychological counseling services, legal advice, temporary relocation expenses and social media monitoring software. This coverage can also offer protection if an individual or their child faces engages in cyberbullying and faces subsequent legal action from the victim.

Because personal cyber insurance is still a relatively new type of coverage, it is usually only available as an add-on to an existing homeowners policy. Further, certain insurers only provide this coverage as an endorsement for high-value homeowners policies. Yet, some insurers may offer standalone personal cyber coverage. Moving forward, insurance experts expect the personal cyber coverage market to continue growing, allowing for more widely available policy options. In any case, individuals should consult trusted insurance professionals to discuss their specific coverage capabilities.

For further risk management resources and insurance solutions, contact us today.