The Cincinnati Insurance Companies

The **Personal Cyber Protection Playbook**

Understanding the risks and remedies of modern cyber crime.

Let’s get started

Contents

The state of personal cyber security.

We live in a complex and ever-changing world. It’s exciting, with new technologies coming to light every day designed to make our lives more interesting, efficient, enjoyable, and informed. But with new technologies come new threats. New technologies like artificial intelligence are great tools, but in the wrong hands, they can be deployed to enhance social engineering to guess passwords or break previously un-hackable systems. Cyber criminals don't have to target you specifically. You may be swept up in a company data breach where your personal information, log ins, and passwords are exposed. Once they have your credentials, it doesn't take a lot of work to target you. And cyber criminals are not just targeting older adults who may not be as tech savvy as other generations, or kids who have yet to develop the critical skills to spot fraud. The whole family is vulnerable, even those of us who have grown up with technology and understand how it works. No one is 100% safe.

The average annual payout for a personal cyber claim is around $10,000[1], which means not having coverage against a range of cyber threats can be financially devastating. This guide will help assess the level of vulnerability you may have to cyber threats and provide recommendations for improving cyber safety. Of course, cyber criminals can target even the safest people, so the sooner you update your homeowner's policy with comprehensive personal cyber coverage, the better.

[1] HSB Claims Data

Ways you may be vulnerable.

Weak passwords can be easy to crack.

This is perhaps the most common vulnerability that people face. In an effort to develop passwords we can all remember, we create passwords that others can guess with a little bit of research into our online lives. Your pets' names, birthdays, street names, and ZIP codes all provide clues that can give hackers a way to discover your passwords. The solution is simple, but not always easy, because many of us have dozens or hundreds of online accounts that are password protected. The best course of action is to change all your passwords (yes, all!) to unique strings, without duplicating the same password twice. Using a password manager from a company that you trust can make this process easier. This process can take days or weeks, but once it's complete, you will be much more secure.

As an added layer of security, when paired with multi-factor authentication — the practice of using two or more verification factors to authenticate your identity — passwords become even that much stronger against hackers.

Online/retail third-party data breach.

Most online retailers are diligent about keeping customer data secure because hackers are continually trying to break through security to get at all of our information. That being said, hacks do sometimes occur, and when they do, it's important to take steps right away to protect yourself. A password you may have used for decades could be available to anyone on the dark web. If you are contacted by a legitimate retailer, they will not ask you to give them your user information (see phishing and smishing below), but if they have experienced an actual data breach, they will alert you and provide some instructions on how to remain safe. It's a good idea to initiate multi-factor authentication and ensure your passwords are strong, and unique from other accounts. Most reputable retailers will ask you to do this as a matter of course.

Phishing and smishing (fraud through phone, email and texts).

Most people are aware of the various schemes hackers use to trick us into giving them our passwords, account numbers, or payment info. But some people still fall for these tricks because they continually change their tactics and deploy highly convincing methods. When you receive an alert through a phone call, email, or SMS that says there's a problem with your account, your service has been interrupted, or there has been a data breach and they ask you to update your information, do not give out any information or click any links. Instead, go to your search engine and enter the business's site, or call their legitimate customer service line to see if the alert was, in fact, real. Make sure anyone else with access to your accounts does the same thing.

Wi-Fi and IoT vulnerabilities.

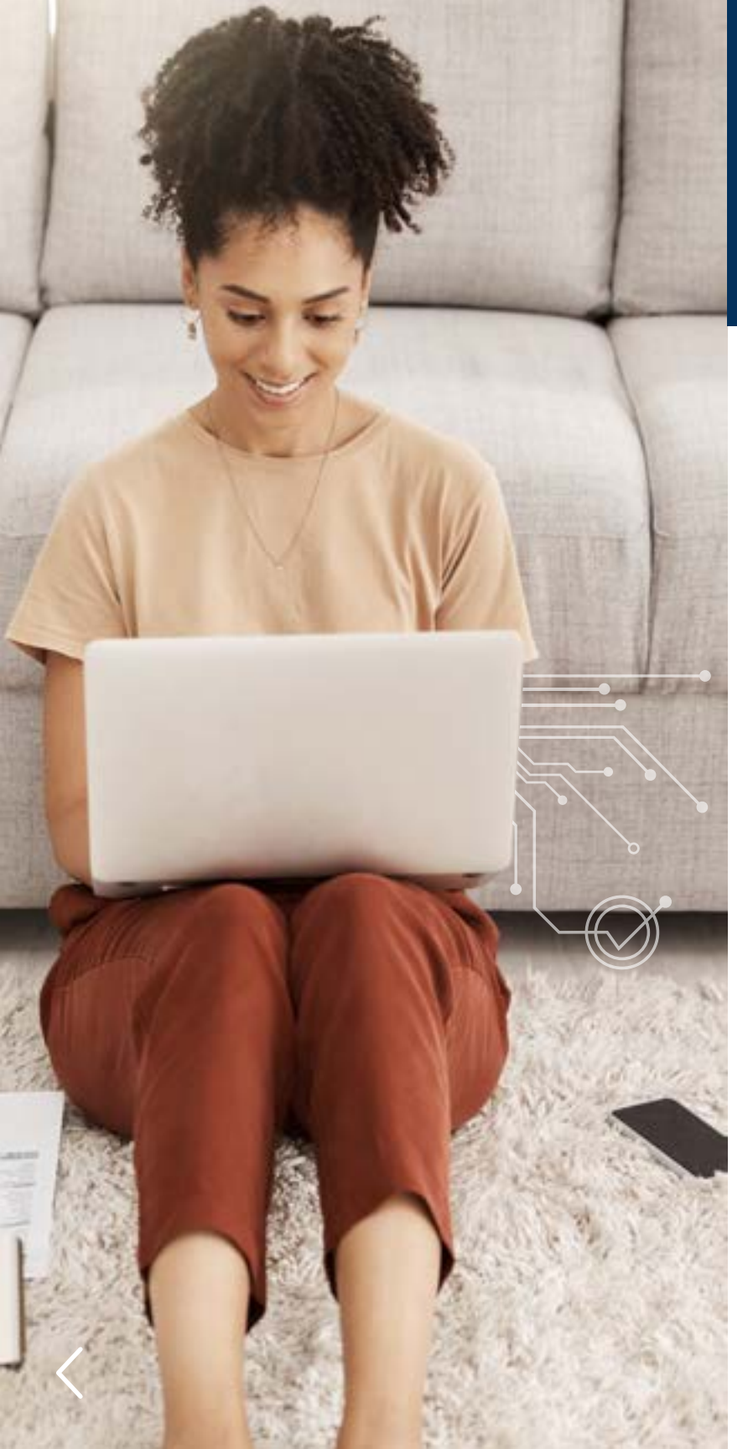
Gaining access to home WiFi or any device on your network like a doorbell, thermostat, baby monitor, phone or laptop can give hackers access to a treasure trove of personal information. The best thing to do is to maintain the password security protocols mentioned above, change your WiFi passwords and use the tools available from your cable provider to monitor activity on your WiFi network from time to time.

Phone hacks or SIM swapping.

It’s more common than you might think for a cyber criminal to pose as you with your phone company, and using some of the information they may have learned about you from social media, convince customer service that you’ve lost your phone and need a new SIM card to use in a replacement phone. Once they have the SIM card, they then have free phone service and access to your contacts list, apps, and payment info. At least until you figure it out and take steps to remedy the situation. It's best to talk to your phone company about a second step verification process (such as a secret pin) before they are allowed to initiate important changes, such as transferring your SIM card or related activities.

Social engineering.

Social engineering is the art of manipulating, influencing, or deceiving you in order to gain control over your computer system. These tactics can include tricking people into sharing information that they shouldn’t share, downloading software that they shouldn’t download, visiting websites they shouldn’t visit, sending money to criminals or making other mistakes that compromise their personal security. The best solution for this is to keep highly sensitive personal information offline. Be wary of cons on the phone, through email, and in texts involving people posing as friends or colleagues. And shred/destroy all sensitive documents before throwing them away.



Overview of coverages.

Computer Attack
Computer attack coverage removes malware and reprograms computers and tablets, Wi-Fi routers, or other internet access points.

Data Breach
Data breach coverage pays for notification costs and recovery services when private non-business data entrusted to an individual is lost, stolen, or published.

Cyber Extortion
This coverage pays to provide professional assistance to respond to a ransomware attack and payment of the ransom (when it has been pre-approved).

Social Media Income Interruption
This covers the victims of social media income loss resulting from a cyber attack or account takeover.

Online Fraud
This pays for financial losses resulting from identity theft, phishing schemes, illegal bank and credit card transfers, and other deceptions and scams.

Frequently asked questions.

How does this differ from the coverage I have with my credit card or bank?

Off-the-shelf policies commonly offered by banks and credit card companies often cover limited damages from online or credit card fraud, which can be helpful, but they typically do not cover things like online scams and fraud, cyber attacks against your devices, ransomware/extortion, data breaches, as well as several other types of cyber crime. As our world becomes more complex,cyber criminals are finding new ways to exploit our vulnerability, which is why personal cyber protection is the most comprehensive coverage to keep you protected from a wide variety of modern threats.

Does this provide coverage for any work from home exposures?

Generally speaking, personal cyber protection only covers personal cyber related exposures.

There may be some situations in which business cyber liability coverage held by the insured's employer comes into play. Some personal cyber protection policies do have the option to remove the business exclusion – but it is important consult your policy to confirm if this is the case.

What about my online business, is it covered or not?

It is recommended that commercial entities secure cyber coverage that is separate and distinct from homeowner's cyber coverage. That said, there may be situations in which a home based business's cyber loss is covered under homeowner's cyber coverage. See policy for details.

Is a borrowed laptop/tablet covered or not?

The personal cyber policy generally does not cover borrowed devices — it would only apply to owned property.

Is there typically coverage for this in my homeowner's policy?

Often not. This is why homeowner's cyber coverage has been developed. To augment the coverage that most homeowner's policies provide as technology becomes more complex and risks associated with technology use increase.

Common objections to personal cyber coverage.

It won’t happen to me.

Most people think this. Until it happens. In the most recent Internet Crime Report produced by the FBI’s Internet Crime Complaint Center (IC3), the FBI receives an average of 2,175 reports of serious cyber crime every day of the year. (The number of crimes reported to the FBI are a fraction of the total crimes experienced nationwide.) As the technology in our lives becomes more sophisticated, so do the kinds of cyber attacks we all face. The truth is, it’s not a matter of if one will be affected by cyber crime, but when.

I don’t have any devices at risk.

If you own a phone or a laptop and a cyber criminal wants to access your sensitive data, no preventative measure is 100% effective. Cyber criminals are that good. Not being covered could cost you $10,000 or more in lost time, data, and money.

I’m already covered for this elsewhere.

Are you? The coverage offered by credit card companies and banks only goes so far. Also, identity theft coverage does not cover all the exposures that would be found in a typical personal cyber insurance policy. Comprehensive personal cyber insurance allows you the peace of mind that limited, off-the-shelf coverage offerings by third parties cannot hope to match.

It’s too expensive.

When you consider that the average annual payout for a personal cyber claim is $10,000, not having this coverage can turn out to be far more expensive.

Cyber vulnerability checklist.

How vulnerable to cyber crime are you?
If you check one or more of these, you may be vulnerable.
Personal cyber protection could be a valuable addition to
your insurance portfolio.

- [ ] You have a home Wi-Fi network and connected devices.
- [ ] You use the same password for multiple services on the web and/or your phone.
- [ ] You do not use complex passwords for all of your important accounts.
- [ ] You are active on social media and maintain a moderate social media presence.
- [ ] You have been exposed to a phishing or smishing scheme in the past.
- [ ] You have a short, memorable social media handle that others may desire.
- [ ] You shop online at least once a week, occasionally using publicly available WiFi networks.
- [ ] You occasionally share personal information about your home, family, or work online.
- [ ] You spend five or more days each week connected to some form of technology.

Claims stories.

The following are real stories of actual claims filed by consumers with personal cyber protection coverage.

Fake IRS agent.

An individual was contacted by phone by someone posing as a representative of the IRS. The fraudster claimed he needed to make a payment to prevent his home from being taken away. Over the next several days, the victim sent one $500 Target gift card and several wire transfers totaling $119,024. Later that week, he visited his bank because he received a notification of the low account balance and became aware of the scam.

The victim was reimbursed for the loss within policy limits.

Microsoft customer service scam.

Posing as a Microsoft employee, an individual gained remote access to a couple's computer and advised them that their devices and bank accounts were compromised. This criminal then told the couple to transfer the funds into his account which, he assured the victims, was secure and provided wire transfer details. The couple sent two wire transfers to the criminal, and only after going to their bank to attempt to transfer more were they made aware that this was a scam. The bank was able to recover a portion of one wire transfer.

A claim of $40,000 was paid to cover the remaining loss.

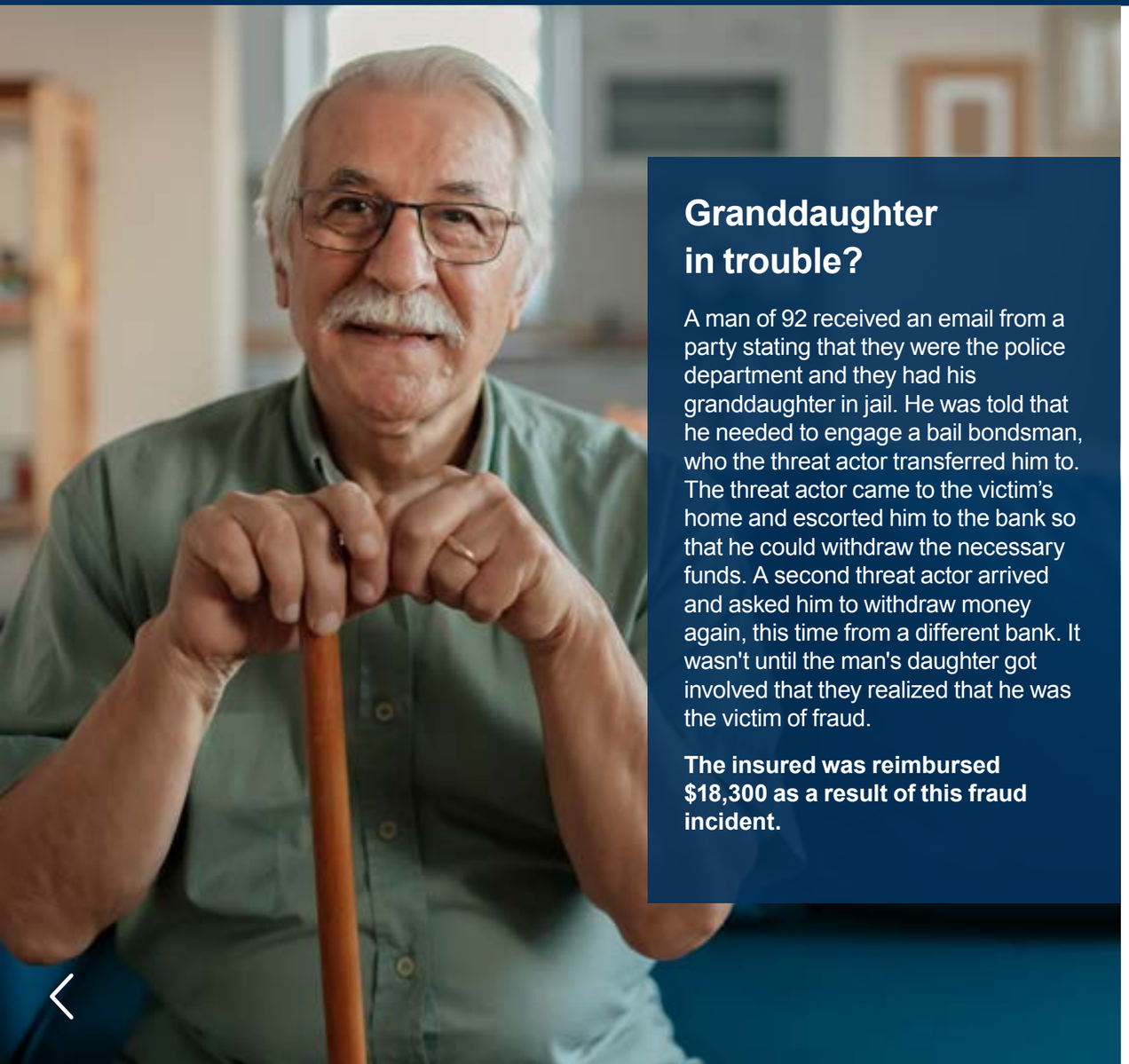
Mistaken refund.

A woman received an email regarding the renewal of a security subscription. She called the number in the email and spoke with someone posing as a representative of Norton Security. After gaining remote access to the victim's computer, he had her fill out a form she believed was to request a refund. The woman was then informed that she input the wrong amount and needed to send back $27,500 using the wiring instructions provided. She sent the funds and only became aware that this was a scam when she reviewed her account balance.

Fortunately, the victim was covered, and was paid $27,500 for this loss.

Claims stories.

The following are real stories of actual claims filed by consumers with personal cyber protection coverage.



Granddaughter in trouble?

A man of 92 received an email from a party stating that they were the police department and they had his granddaughter in jail. He was told that he needed to engage a bail bondsman, who the threat actor transferred him to. The threat actor came to the victim's home and escorted him to the bank so that he could withdraw the necessary funds. A second threat actor arrived and asked him to withdraw money again, this time from a different bank. It wasn't until the man's daughter got involved that they realized that he was the victim of fraud.

The insured was reimbursed $18,300 as a result of this fraud incident.

Ransomware demand.

A woman was a victim of online fraud after a cyber criminal had infected her computer and then advised her that her computer and online banking had been compromised. Wire transfers were requested in order to restore the computer and accounts.

When the fraud was finally discovered, a claim was made, the computer was cleaned up, and the insured was reimbursed $37,400.

Dating site scam.

A woman met an individual on a popular dating site. As part of a systematic confidence scheme, the conversation turned to investments in cryptocurrency. The victim received instructions from the individual advising her she could make money easily by wiring funds to an account that seemed legitimate. In an elaborate scheme that involved several kinds of transfers, the victim provided routing numbers and even copies of the front and back of her driver's license in order to create and verify crypto accounts.

After she realized she was the victim of fraud and that her bank was unable to recover her funds, she turned to her insurance provider, and after providing the verifying documents, was reimbursed $34,000 for her loss.

Glossary of cyber security terms.

The following are terms you may hear or read in the process of learning more about cyber crime.

- **Algorithm** — Code written to instruct hardware/software assets to follow a specific set of complex instructions.
- **Anti-virus (anti-malware)** — Any software that works to identify malware and remove it from a given system or network.
- **Authentication** — The process of proving a user is who they say they are by using various tools and systems.
- **Backing up (backup)** — A way to duplicate an infected or un-ransomed system in order to restore it at a later date if needed.
- **Behavior monitoring** — The process hackers use to keep a record of a victim's behavior in order to use the gathered information to steal their identity or attack their social media connections.
- **Blacklist** — A list that exists on a server or computer that blocks unwanted connections for specific IP addresses. (See whitelist.)
- **Bug** — An error or mistake in software or hardware that may be exploited by hackers.
- **Clickjacking** — A malicious process in which a victim is tricked into clicking on a URL, button, or other screen object.
- **Cloud computing** — A process by which computer files and resources are stored and accessed in a location other than the user's phone or computer.
- **Cracker** — The industry term for “hacker.” (See hacker.)
- **Critical infrastructure** — The computer hardware and networks needed for daily operations.
- **Cryptography** — The mathematical security strategies used to protect data and provide security, confidentiality, and authentication.
- **Cyber attack** — Any attempt to gain access or exploit a computer system or phone.
- **Cyber security** — The process of protecting digital assets on any kind of network.
- **Data breach** — A breach occurs when hackers are able to access data that had previously been stored in protected and anonymous ways.
- **DDoS (Distributed denial of service) attack** — An attack that attempts to halt access to any resource by using multiple computers to overload a computer, server, or network.
- **Decrypt** — To remove/deactivate encryption.
- **Digital certificate** — A digital assurance by a third party that a digital property or identity is legitimate.
- **Digital forensics** — The process of uncovering the history within server logs and other digital records to expose potential unseen vulnerabilities and exploits within a system.
- **Eavesdropping** — The act of listening in on a transaction, communication, data transfer, or conversation.
- **Encryption key** — The secret number value used by a symmetric encryption algorithm to control the encryption and decryption process.
- **Firewall** — A security tool, which may be a hardware or software solution, that is used to filter network traffic.
- **Hacker** — A person who has knowledge and skill in analyzing program code or a computer system, modifying its functions or operations, and altering its abilities and capabilities.
- **Identity cloning** — A form of identity theft in which the attacker takes on the identity of a victim and then attempts to live and act as the stolen identity.
- **Identity fraud** — A form of identity theft in which a transaction, typically financial, is performed using the stolen identity of another individual. The fraud is due to the attacker impersonating someone else.
- **ISP (internet service provider)** — The organization that provides connectivity to the Internet for individuals or companies.
- **Key-logger** — Software or other eavesdropping measures used to record the keystrokes of a victim as they are typed.

Glossary of cyber security terms.

The following are terms you may hear or read in the process of learning more about cyber crime.

- **LAN (local area network)** — An interconnection of devices (i.e. a network) that is contained within a limited geographic area.
- **Link jacking** — A potentially unethical practice of redirecting a link to a middleman or aggregator site or location rather than the original site the link seemed to indicate it was directed towards.
- **Malware (malicious software)** — Code written for the purpose of causing harm, disclosing information, or violating security. The following are examples of malware: virus, worm, T rojan horse, logic bomb, backdoor, remote-access Trojan (RAT), rootkit, ransomware, and spyware/adware.
- **MFA (multi-factor authentication)** — A security measure that protects individuals by requiring users to provide two or more authentication factors to access an application, account, or virtual private network (VPN). This adds extra layers of security to combat more sophisticated cyber attacks, since credentials can be stolen, exposed, or sold by third parties.
- **Pen testing** — Short for penetration testing. This is the act of intentionally attempting to gain access to hardware, software, or physical security measures to test the robustness of a security measure.
- **Phishing** — A social engineering attack that attempts to collect information from victims. Phishing attacks can take place over email, text messages, through social networks, or via smartphone apps.
- **POS (point of sale) intrusions** — An attack that gains access to the POS (point of sale) devices at a retail outlet, usually aimed at copying legitimate credit card numbers.
- **Ransomware** — A form of malware that holds a victim's data hostage on their computer, typically through robust encryption.
- **Restore** — To bring a system back to an originally clean and safe backed-up state.
- **Social engineering** — A hack focusing on people rather than technology. Social engineering seeks to use knowledge of one's life and habits to gain trust or exploit vulnerabilities.
- **Spam** — Unsolicited messages or communications received in an e-mail or text messaging, social networks, or VoIP.
- **Spear phishing** — A form of social engineering attack that is targeted to victims who have an existing digital relationship with an online entity such as a bank or retail website.
- **Spoof (spoofing)** — The act of falsifying the identity of the source of a communication or interaction. It is possible to spoof IP addresses, MAC addresses, and email addresses.
- **Spyware** — Malware that spies — or monitors online activities — and reports them to a cybercriminal.
- **Trojan horse (Trojan)** — Malware unknowingly embedded within a benign host file that a user downloads or installs.
- **Two-factor authentication** — The means of proving identity using two authentication factors which is considered stronger than any single-factor authentication. A form of multi-factor authentication.
- **VPN (virtual private network)** — A communication link between systems or networks that is typically encrypted to provide a secured, private, isolated pathway of communications.
- **Virus** — A form of malware that often attaches itself to a file or system as a parasite. When activated, the virus can infect other systems connected to the infected computer.
- **Vishing** — A form of phishing attack taking place over VoIP. In this attack, the cybercriminal uses VoIP systems to be able to call any phone number toll-free.
- **Vulnerability** — Any weakness in an asset or security protection that would allow for a threat to cause harm.
- **Whitelist** — A list of approved resources that a system uses to grant access. The opposite of a blacklist.
- **Wi-Fi** — Network communication in the home, at work or in retail businesses using radio waves rather than cables.

These examples are for educational purposes only. Every claim is adjusted according to its own specific set of facts. Whether or not insurance coverage would apply to any claim is dependent on the facts and circumstances of each individual claim and the language of the insurance policy.

The Hartford Steam Boiler Inspection and Insurance Company provides The Cincinnati Insurance Companies with a variety of support services, including call center assistance, collaborative claims service and risk mitigation materials.