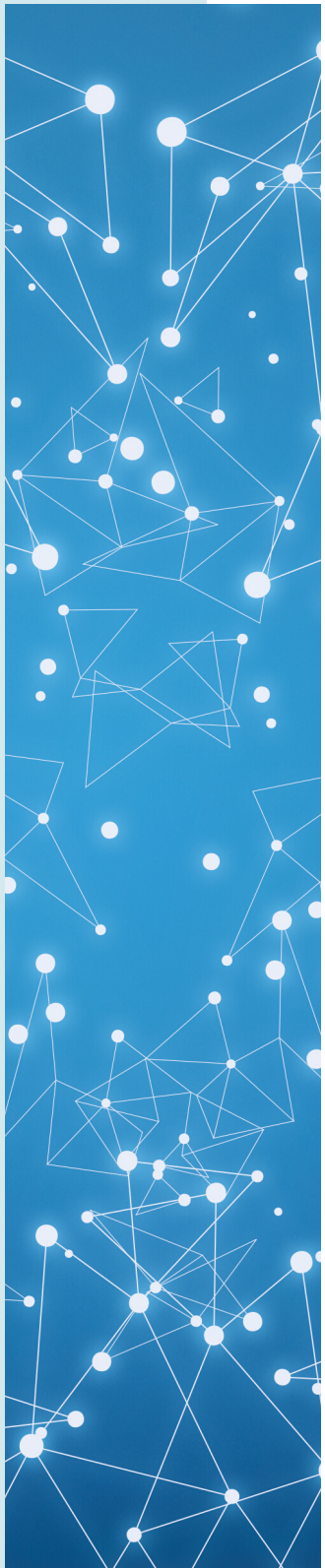
CYBERSECURITY RISK MANAGEMENT

DEPARTMENT OF BUSINESS REGULATION
INSURANCE DIVISION



INTRODUCTION:

We increasingly rely on the Internet to work, bank, shop and socialize. Our health and financial information is stored online and devices are connected to control everything from home security systems to thermostats and TVs. While convenient, these connections open the door for possible malicious activity. The Rhode Island Insurance Division offer these tips to help manage your cybersecurity risks.

03

UNDERSTANDING THE THREAT

Cybercrime is a criminal act involving a computer and a network. **Cyber risk** includes any risk associated with online activity, such as storing personal information online or completing online transactions. This includes damage to your or your business' reputation, financial loss or disruption to your life or your business operations.

Identity theft is the unauthorized use or attempted use of an existing account, use of your information to open a new account and misuse of your information to commit fraud. Identity theft insurance helps you pay the costs of restoring our identity if it is stolen.

Data thieves gain access to information from a variety of places including your mailbox, home and business trash, public dumps, public records and social media. Some criminals are after money, but some also seek public attention.

04

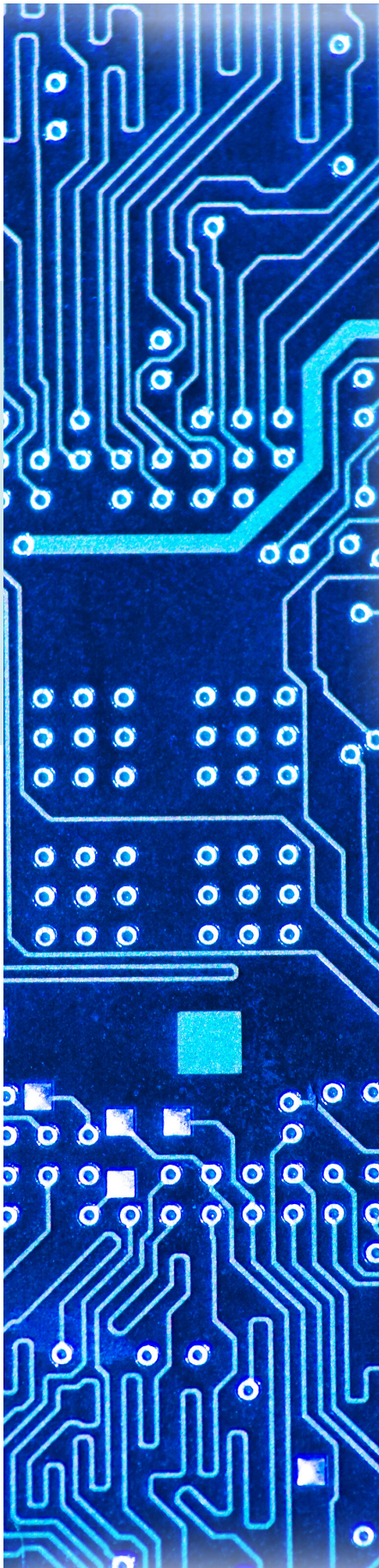
HOW DO I KNOW MY IDENTITY IS AT RISK?

You are at risk if you store personal information on a home or work computer, bank or shop online. Your data may have been compromised if you notice any of the following scenarios:

- You see unexpected withdrawals from your bank account
- You don't receive your bills or other mail
- You're billed for health services you didn't use or your health plan rejects a legitimate medical claim.

Regularly check your credit report to ensure you don't see:

- A new account you did not open
- Unfamiliar accounts listed
- Negative items



05

HOW CAN I KEEP MY INFORMATION SAFE ONLINE?

Security Starts at Home
Your Wi-Fi router is the first line of defense for your home's Internet network. To make sure no one is accessing your Wi-Fi, you should occasionally change the router's administrator login, enable encryption and change default passwords.

Viruses and malware are a constant threat. Investing in antivirus and anti-malware software is a necessary expense to protect your identity and personal information.

Sensitive information, such as your social security number, confidential business, bank information, medical records and tax returns should never be sent over email or other communication channels without encryption.

Be Aware of Your Surroundings
Whether you are sitting in a coffee shop, a shared workspace, or on public transportation for your daily commute, keep in mind there are individuals who may be listening to your conversations or are able to see your screens. Do not read your credit card number or discuss your bank account or other personal information in a public setting.

Cyberthieves have created information-skimming devices that are attached to ATMs, gas pumps and other POS devices. Once you enter your PIN, thieves have access to everything they need to clean out your bank account. Watch out for any card-swiping devices that look suspicious.

Password Protection
Along with the convenience of our online lifestyle comes the need for an endless number of passwords. Security experts suggest you memorize the most important ones and write the rest down, keeping them in a safe place. Keep this data secure, and do not keep your account numbers and passwords in the same place. If you keep a list of passwords on your phone, laptop or even in the cloud, avoid naming that file "Passwords."

Experts recommend passwords with a combination of upper and lowercase letters, numbers and symbols. Two-factor authentication offers an extra layer of security by requiring a password, a username, as well as something only the user has access to when logging in. This might include a specific piece of information only they should know — or a physical token, a fingerprint or facial recognition. Two-factor authentication can be added to your social media accounts, mobile phones, email and bank accounts.

06

HOW CAN I KEEP MY INFORMATION SAFE ONLINE?

Think Before you Click
If you see an email from an address you do not recognize, proceed with caution and never click on attachments or links in emails that seem suspicious. With one click, you could infect your computer with viruses or malware that may not be detected for months. In the meantime, your data has been compromised and you may have invited an identity thief into your system.

Hackers have begun using fake web addresses (URLs) that seem completely normal to break into systems. One way to stay safe online is to look for spelling or grammatical errors in domain names and email addresses.

There are additional steps you can take to secure your information and data:

- Be alert to impersonators by being careful about who you trust online
- Safely dispose of personal information by shredding documents using a cross-cut shredder
- Use strict privacy settings on your computer, devices and browsers
- Be careful when sharing personal information on social media
- Be cautious of what you download from the Internet
- If your social security number is requested by a vendor, ask why it's needed and how it will be used and protected

Keeping your information safe also means ensuring your devices, including smart phones, laptops, desktops, iPads and other devices are secure:

- Update your software regularly
- Use antivirus or anti-malware software to protect against malicious software that disrupts computer operations, gathers sensitive information, gains access to private computers or displays unwanted advertising
- Back up your files to an encrypted flash drive or external hard drive

The Federal Deposit Insurance Corporation (FDIC) offers a **Cybersecurity Checklist** to help you protect your computer and money from online criminals.

07

IDENTITY THEFT INSURANCE

The cybersecurity insurance and identity theft insurance market is growing and may be useful to you or your business depending on the types of information you collect and store.

Some homeowners' or auto policies now offer identity theft protection, which includes access to credit monitoring and repair services in the event of a breach. Note that this coverage only refunds the costs associated with restoring your identity. It does not cover loss if you used your credit/debit card to make purchases or get cash. Restoring other losses would depend on the coverage policies of your credit card company and bank.

Your insurance agent may be able to help provide more information about assessing your risks and whether additional coverage is needed on home or auto policies.

08

CYBERSECURITY INSURANCE BUSINESS COVERAGE

Despite high profile data breaches of large companies, small companies are also targets for hackers as they possess sensitive information but typically have less security than larger companies. Cybersecurity insurance provides coverage for compromised security or privacy breaches at work. Business cybersecurity policies tend to be highly customized and therefore, costly.

Securing a Small Business
About half of all small businesses experience a cyberattack because they generally have a moderate amount of data and usually have minimal cybersecurity.

Small businesses should secure their Wi-Fi networks, train employees on cyber security, and consider using third-party security companies to protect their data. If you want to share your Wi-Fi with guests, you can do that safely by providing them with guest network access. Cyber liability insurance can help a small business survive cyber-attacks by paying for customer notification, credit monitoring, legal fees and fines after a data breach.

There are additional steps you can take to help secure your business:

- Start by conducting a security and self-risk assessment. Determine what to protect, what protection exists and where the gaps exist. This also means developing a plan to protect your property and data, operational information and client data.
- Finally, identify the tools you need to protect this information.
- Implement sound cybersecurity procedures and training for employees. Educate employees on smart use of social media, how to spot suspicious emails and not connecting to public Wi-Fi on a company device.
- If your small business has a disaster recovery plan, consider cybersecurity insurance as part of it. If you don't have such a plan, consider creating one. Developing procedures and identifying threats is important but you also must understand your vulnerabilities. You might consider testing such as an internal phishing campaign against employees to check your company's vulnerably.
- Always back up important business systems and data. Implement settings encouraging regular password changes, restrictions on the websites employees can access as well as strong security software.

MORE INFORMATION

The Federal Deposit Insurance Corporation (FDIC) also hosts a wealth of information on **cybersecurity**. The Federal Trade Commission (FTC) has an **identity theft website** to report incidents and develop a recovery plan after a cybersecurity attack.

Rhode Island Insurance Division
1511 Pontiac Avenue, Bldg 69-2
Cranston, Rhode Island 02920
Telephone: (401) 462-9520
Website: www.dbr.ri.gov
Email: dbr.insurance@dbr.ri.gov
Follow us on Social Media!Twitter
@RIDBRFinancial