

FOR IMMEDIATE RELEASE: April 8, 2016

Contact: Danielle Barrick, director of communications, (603) 271-7973, ext. 336, danielle.barrick@ins.nh.gov.

Cybersecurity Risk Management: Lock Down Your Assets, Secure Your Data

Concord, NH – The New Hampshire Insurance Department offers the following tips to help you manage your cybersecurity risks:

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 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 your 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.

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 your 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

How can I keep my information safe online?

There are basic 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
- Keep passwords private and complex
- 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.
- Password-protect your laptop to prevent unknown users from accessing it.
- Avoid opening emails or attachments from unknown senders.
- 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:

<https://www.fdic.gov/consumers/consumer/news/cnwin16/checklist.html>

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 offer identity theft protection, which includes access to credit monitoring and repair services. Note that this refunds just the costs associated with restoring your identity and 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.

Cybersecurity insurance business coverage

Small companies are 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 costly.

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

- Conducting a security and self-risk assessment. Determine what to protect, what protection exists and where the gaps exist. Develop a plan to protect your property and data.
- 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. You might consider testing such as an internal phishing campaign against employees to check your vulnerability.
- Always back up important business systems and data. Encourage regular password changes, restrictions on the websites employees can access as well as strong security software.

More Information

The FDIC hosts a wealth of information on cybersecurity:

https://www.fdic.gov/consumers/consumer/news/cnwin16/?source=govdelivery&utm_medium=email&utm_source=govdelivery

The Federal Trade Commission has an identity theft website to report incidents and develop a recovery plan: <https://www.identitytheft.gov/>

The New Hampshire Insurance Department's mission is to promote and protect the public good by ensuring the existence of a safe and competitive insurance marketplace through the development and enforcement of the insurance laws of the State of New Hampshire. For more information, visit www.nh.gov/insurance.

#