Risk Management Services

ARE YOU PROTECTED?

Cybersecurity Tips for Your Business

The Internet, broadband, and information technology are powerful tools to help businesses reach new markets and increase sales and productivity. Cybersecurity threats are real, and businesses must implement the best tools and tactics to protect themselves, their customers, and their data. Theft of digital information has become the most commonly reported fraud, surpassing physical theft.

No matter the size of your business or the extent of your computing, cybersecurity should be a crucial part of every business's risk management process. Use the following cybersecurity tips to help protect your business:

- **Train employees in security principles –** Establish security practices and policies for employees. These should include how to develop and use strong passwords, appropriate Internet usage guidelines that detail penalties for violating company cybersecurity policies, and rules of behavior describing how to handle and protect customer information and other vital data.

- **Protect information, computers, and networks from cyber attacks –** Ensure you have the latest updates to your security software, web browser, and operating systems. These are the best defenses against viruses, malware, and other online threats.

  Be aware that operating systems do have end-of-life dates after which you will no longer be able to obtain software updates to address vulnerabilities. In 2020, for example, Microsoft Windows 7 and Windows Server 2008 operating systems reached their end of life and are no longer supported.

  In addition, set anti-virus software to run a scan after each update. Install other key software updates as soon as they are available.

- **Provide firewall security for your Internet connection –** A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure your operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home systems are protected by a firewall and consider the use of a virtual private network, commonly known as a VPN.

- **Create a mobile device action plan –** Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access your corporate network. If mobile devices access your corporate network, require users to password-protect their devices, encrypt their data, and install security apps. This will prevent criminals from stealing information while the device is connected to public networks or if the device is lost or stolen. Be sure you have procedures in place for reporting lost or stolen equipment.

- **Back up important business data and information –** Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. The backup should be done automatically, at least weekly, and be stored either offsite or in the cloud.

Continues

- **Secure your Wi-Fi networks –** If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password-protect access to the router.

- **Employ best practices on payment cards –** Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations pursuant to agreements with your bank or processor. Isolate payment systems from other, less secure programs, and don't use the same computer to process payments and surf the Internet.

- **Passwords and authentication –** Require employees to use unique passwords and change passwords regularly – at least every three months is recommended. Multi-factor authentication (MFA) that requires additional information beyond a password to gain entry is also recommended. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer MFA for your account.

Visit the Federal Communications Commission (FCC) at **www.fcc.gov/cyberplanner** to create a free customized Cyber Security Planning guide for your business. Visit the Cybersecurity & Infrastructure Security Agency (CISA) at **www.dhs.gov/stopthinkconnect** to download resources on cybersecurity awareness.

Contact your local Risk Management Representative to assist with cyber tools and other loss prevention tools which can help you minimize the frequency and cost of cyber-related losses.

Source: Federal Communications Commission – **https://www.fcc.gov/general/cybersecurity-small-business**

This information is provided solely as an insurance risk management tool. It is provided with the understanding that the member insurance companies of the Utica National Insurance Group are not providing legal advice, or any other professional services or advice. Utica shall have no liability to any person or entity with respect to any loss or damages alleged to have been caused, directly or indirectly, by the use of this information. You are encouraged to consult an attorney or other professional for advice on these issues.