INSURANCE *Identity Thieves*

Tips to Keep Identity Thieves Out of Your Home and Small Business

We have become dependent on the convenience of having our financial accounts, healthcare information and personal profiles just a click or two away. Whether you use a desktop, laptop, tablet or a smartphone to access the Internet, this convenience comes with a responsibility to be vigilant with regards to basic cybersecurity. The Wyoming Department of Insurance offers the following tips to help keep your identity safe and your business secure.

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. If you want to share your Wi-Fi with guests, you can do that safely by providing them with guest network access.

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.

Cyber thieves have created information-skimming devices that are attached to ATMs, gas pumps and other Point of Sale (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.

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 use 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.

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. 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.

More Information

The National Association of Insurance Commissioners (NAIC) has published a Roadmap for Cybersecurity Consumer Protection at: https://www.naic.org/documents/committees_ex_cybersecurity_tf_related_roadmap_cybersecurity_consumer_protections.pdf.

Also, the Federal Deposit Insurance Corporation (FDIC) 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.

Wyoming Department of Insurance
http://doi.wyo.gov / 1 (800) 438-5768