5 Simple Steps To Prevent Cyber Losses Today

Worldwide spending on cybersecurity is forecast to reach $133.7 billion in 2022. The average ransomware attack on a business now costs over $100,000! The statistics become more and more disturbing each year. Fortunately, you can avoid most issues by following so very simple safety procedures;

1) Don’t procrastinate- say ‘Yes’ to the Update!

Installing updates promptly is one of the best ways to help protect your system and keep it more cybersecure. The next time you see and app that is asking to update click ‘Yes’ instead of ‘remind me later’. Take a short break and let the system updater. In the long run you’ll save time.

2) Strengthen your passwords.

I have a slide I like to display when discussing passwords. It is a list of the most popular passwords (the word password is one of them) and combinations such as the name of your business, your pet, favorite sports team, child, or otherwise and year of birth, graduation, etc. If its been a while since you’ve updated your passwords consider doing it today. Oh, and get rid of the sticky note taped to your laptop or under your desk phone, it’s not fooling anyone any more than hiding your wallet in the toe of your shoe when you go swimming.

3) Stop clicking on stuff you don’t recognize.

Scammers are masters of making you second guess or worry something has gone wrong. Let’s say you get an email that says your bank account authorized several hundred be paid out and to click the link if you did not authorize. STOP! Unless you have reason to believe that your account has been compromised this type of email is usually a scam. Nearly 100% of all malware is sent via email. Commit to take a deep breath before clicking anything moving forward. This holds doubly true if the email indicates you must take immediate action or uses the word ‘urgent’. Think about it, if something was truly ‘urgent’ would sending an email be the most effective path of communication?

4) Move it or lose it!

Actually, a better way is *save it or lose it.* Become a fierce data backer upper. If you save all of your data on a secure cloud or hard drive that you then store off-site you can prevent the majority of all cyber losses. I like to think what would happen if my computer were to fall into a lake or get burned up in a fire. If that happened, would my data be available easily and quickly to be uploaded to a new system? If the answer is ‘yes’ you are in good shape. If not, its an easy fix- just back it up!

5) Lock Down

Secure your WI-FI account with a password and ensure each user has his or her own password to enter your server and log into their computer. Securing your WI-FI with a password protects you from an unauthorized system introducing whatever virus or issue it has into your network. Requiring each user to have his or her own password makes it easier to identify the people involved in the event of a cyber-attack. Sharing of passwords should be discouraged or outright forbidden.

6) Insure against cyber losses

Despite doing our best, a cyber crime can still find its way into the business and wreak havoc. This is the time where having a Cyber-Liability insurance policy will come in helpful. Such a policy provides coverage for investigation, rebuilding, reputation repair, identity theft, and more. Visit with your insurance agent about the options available for a cyber-liability policy.

Todd Shepard is the founder of Shepard & Shepard Insurance Solutions and regular contributor to the Front Row. For a review of your garage policy and a competitive quote or more information on cybercrimes and cyber insurance call 855-396-0488 or visit www.shepquote.com