Cybersecurity: Five Tips on How to Work Remotely Safely

By Karl Susman

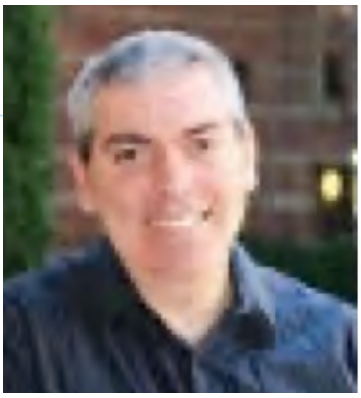
The Coronavirus pandemic (Covid-19) has reshaped the business community. "Remote work" by electronic means, including computers, is here, and here to stay. There are both advantages and disadvantages of Remote work. In 2020 there was an 80% increase in cyber attacks. This translates into an attempted attack every 39 seconds. It is estimated that cybercrime will cost a projected 6 trillion dollars this year alone. Since we are working remotely, by definition we are online or otherwise away from home base, and therefore exposed. More and more stories are emerging about hacking, data breaches, theft, virus, ransomware attacks, phishing, or other disruptions, which have caused business interruption and other damage. Standalone insurance policies are being formulated for this new market. Here are five tips on how to stay safe while working online remotely. While these might be very basic tips, they bear repeating.

Tip Number One – Update Your Computer

If you are working on a Windows computer, you should have an option to have your computer automatically update when updates become available. Be sure this option is enabled. In addition, be certain that you have your privacy and security settings enabled. You will find all these settings in Windows under "Settings". If you are running on a MAC, it may be less vulnerable to a virus or ransomware attack, however that is primarily because there are less of them to attack. Follow the same guidelines and be sure that your MAC is set to auto-update the software and apps. Also select all privacy and security settings to ensure you have the best protection your operating system can offer.

Tip Number Two – Think Before You Click

Read and think before you click. When you receive an email, before you open it or click on any links in it, read the email, and think about it prior to taking any action. Ask yourself if you know the person emailing you or the company that is emailing you. Ask if the email purports to be from a questionable sender from whom you would never expect to receive a communication. Whenever in doubt, call the sender and verify they sent the email before doing anything.



Susman

Karl Susman, CPCU, CIC, LUTCF
Susman Insurance Agency

Karl D. Susman Is the President of Susman Insurance Agency, Los Angeles, California. He is a frequent contributor to the IRC Newsletter on issues of interest to the IRC and TIPS. He can be reached at (310) 820-5200 or (424) 744-9761.

Cybercrime will cost a projected $6 trillion this year alone; these five basic tips on cybersecurity bear repeating.

Tip Number Three – Text Messages Can Be Dangerous

The well used the Text Message has now been invaded by deceptive hackers trying to get at you and your data. If you get a text message from an unknown person, you should immediately be skeptical. Even though you may use your cell phone for work, do not assume an unknown number is from a co-worker. Keep in mind that over 80% of the US population send and receive text messages! Be cautious about providing any personal information over text message and do not click on any links in a text message unless you are sure the sender is trustworthy.

Tip Number Four – Remote Connections Also Means Unwanted Eyes

Watch who is watching your screen. Working remotely means just that, you are remotely connected to your business and you could be literally anywhere. If you are sitting in the local coffee shop or in an airport while working on your laptop, be conscious of who else can see your screen.

Tip Number Five – Create Complex Passwords For Each Website

Never use the same password twice. Would you like to know the most used password in all of 2020? It is “123456”. A close runner-up is simply the word “password”. If you think using one good and complex password is the right way to go, think again. If your password is stolen from one of the websites you use it on, it most likely will be used on other websites but without you even being aware. Use one specific password for one website and nowhere else. Ever.

Standalone Insurance Is Emerging To Cover Network Security, Computer Replacement, Ransomware Protection, Financial Scam Coverage, ID Theft, Credit Monitoring, and Other Risks

The Standalone Cybersecurity policy market is emerging. Several insurers have stepped up with products and services available to cover many of these risks. One of the comprehensive products currently out there is a program called Cyberman 365. This product offers home network security, hacked computer replacement, ransomware protection, financial scam coverage and id theft and credit monitoring. There are policies available from other companies as well. An insurance agent or broker will be familiar with companies that offer the most comprehensive and most reasonably priced cybersecurity policies.

The Standalone Cybersecurity Policy Market Is Emerging; The Product Could Offer Home Network Security, Hacked Computer Replacement, Ransomware Protection, Financial Scam Coverage And Id Theft And Credit Monitoring.