Avoiding the Cybercrooks

How can you protect yourself against ransomware, phishing, and other tactics?

Provided by John Ruzza, CFP®

Imagine finding out that your computer has been hacked. The hackers leave you a message: if you want your data back, you must pay them $300 in bitcoin. This was what happened to hundreds of thousands of PC users in May 2017 when they were attacked by the WannaCry malware, which exploited security flaws in Windows.

How can you plan to avoid cyberattacks and other attempts to take your money over the Internet? Be wary, and if attacked, respond quickly.

Phishing. This is when a cybercriminal throws you a hook, line, and sinker in the form of a fake, but convincing, email from a bank, law enforcement agency, or corporation, complete with accurate logos and graphics. The goal is to get you to disclose your personal information – the crooks will either use it or sell it. The best way to avoid phishing emails: stick to a virtual private network (VPN) or extremely reliable Wi-Fi networks when you are online.[1]

Ransomware. In this scam, online thieves create a mock virus, with an announcement that freezes your monitor. Their message: your files have been kidnapped, and you will need a decryption key to get them back, which you will pay handsomely to receive. In 2016, the FBI fielded 2,673 ransomware attack complaints, by companies and individuals who lost a total of $2.4 million. How can you avoid joining their ranks? Keep your security software and operating system as state of the art as you can. Your anti-virus programs should have the latest set of virus definitions. Your Internet browser and its plug-ins should also be up to date.[2]

Advance fee scams. A crook contacts you via text message or email, posing as a charity, a handyman, an adult education provider, or even a tax preparer ready to serve you. Oh, wait – before any service can be provided, you need to pay an “authorization fee” or an “application fee.” The crook takes the money and disappears. Common sense is your friend here; avoid succumbing to something that seems too good to be true.

I.R.S. impersonations. Cybergangs send out emails to households and small businesses with a warning: you owe money. That money must be paid now to the Internal Revenue Service through a pre-paid debit card or a money transfer. These scams often prey on immigrants, some of whom may not have a great understanding of U.S. tax law or the way the I.R.S. does business. The I.R.S. never emails a taxpayer out of the blue demanding payment; if unpaid taxes are a problem, the agency first sends a bill and an explanation of why the taxes need to be collected. It does not bully businesses or taxpayers with extortionist emails.[1]

Three statistics might convince you to obtain cyberinsurance for your business. One, roughly two-thirds of all cyberattacks target small and medium-sized companies. About 4,000 of these

attacks occur per day, according to IBM. Two, the average cost of a cyberattack for a small business is around $690,000. This factoid comes from the Ponemon Institute, a research firm that conducted IBM's 2017 Cost of Data Breach Study. That $690,000 encompasses not only lost business, but litigation, ransoms, and the money and time spent restoring data. Three, about 60% of small companies hit by an effective cyberattack are forced out of business within six months, notes the U.S. National Cyber Security Alliance.[3]

Most online money threats can be avoided with good security software, the latest operating system, and some healthy skepticism. Here is where a little suspicion may save you a lot of financial pain. If you do end up suffering that pain, the right insurance coverage may help to lessen it.

John Ruzza is a Representative with Cambridge Investment Research, Inc., and may be reached at www.mainstreetfa.com, (269) 492-9701 or john@mainstreetfa.com. 2632 S 11TH Street Kalamazoo MI 49009

Citations.

1 - gobankingrates.com/personal-finance/avoid-12-scary-money-scams/ [8/28/17]
2 - eweek.com/security/the-true-cost-of-ransomware-is-much-more-than-just-the-ransom [8/18/17]
3 - sfchronicle.com/business/article/Interest-in-cyberinsurance-grows-as-cybercrime-12043082.php [8/28/17]