Protecting Yourself Against Cyberattacks

How vulnerable is your data?

25% of Americans were cyberhacked between March 2014 and March 2015. The American Institute of CPAs announced that alarming discovery in April, publishing the results of a survey conducted by Harris Poll. Disturbing? Certainly, but the instances of pre-retirees being victimized were even greater – 34% of adults aged 55-64 reported having their data stolen or compromised within that period.[1]

Small businesses are also commonly victimized. While identity theft has eroded consumer and employee trust in Target, Sony, Home Depot, Anthem and Wells Fargo, they will survive; a small business with limited IT resources may not. Symantec says that 30% of all targeted cyberattacks occur against firms employing fewer than 250 workers. The National Cyber Security Alliance says that the average small business that gets hacked has a 60% chance of closing its doors within six months.[2]

Hackers will not put your household out of business, but they can steal the assets within your checking account or your workplace retirement plan in seconds. They can also take your Social Security number, email address, annual income data and more and sell it or retain it to hurt you in the future.

Cyberattacks within the financial world are especially frightening. Bank and brokerage accounts are respectively insured by the FDIC and SIPC, yet that insurance only protects a customer or client in cases of institutional failure. It does not cover cybertheft.[3]

How can you strengthen your online defenses against cyberthieves? One way to do that is through two-factor authentication, or 2FA.

Corporations are starting to realize the vulnerability of a username-password combination. Given that so many usernames are derivations of real names, and given that many passwords are still mentally convenient, a hacker can access such accounts with relative ease.

If a company installs another security factor beyond the username-password combination – such as a voiceprint audio I.D. or a one-time numeric code texted to your phone to permit account access – hacking an account becomes much harder. This two-factor authentication may become the norm in the near future.

Too many Americans use simple passwords, sometimes at multiple websites. (Did you know that "password" is one of the most commonly used passwords?) Fortunately, free software has emerged to generate random passwords for different accounts. High net worth households are discovering Norton Identity Safe, RoboForm, LastPass, Dashlane and other apps capable of creating super-strong passwords.[4]

Aside from using stronger passwords, avoid falling prey to the classic mistakes. When you use free Wi-Fi at a coffeeshop or airport or make a bid at an online auction site of questionable origin, you are taking your chances. The same goes for opening mystery email attachments and sharing private data on websites lacking the HTTPS protocol.

Will cybersecurity improve in the coming years? A widely adopted 2FA standard may make online theft much harder to pull off. Other defenses are being touted, some with more merit than others. Using a fingerprint as a password sounds good, but has a crippling drawback: you can change a password, but try changing your fingerprint. Some consumers are getting new EMV-equipped credit and debit cards that rely on microchips rather than magnetic strips; many of these are not the chip-and-PIN cards common to Europe, however. Instead, they are chip-and-signature cards. The second security factor is simply you signing your name. Cybersecurity analysts believe that while the chip-and-signature cards are better than the old technology, they fall short of chip-and-PIN cards.[5]

True cybersecurity may prove elusive, but personal vigilance and password management software are good steps toward building a better defense against cyberattacks.

Citations.

1 - aicpa.org/Press/PressReleases/2015/Pages/AICPA-Survey-One-in-four-Americans-Victimized-by-Information-Security-Breaches.aspx [4/21/15]
2 - wscpa.org/more/news/article/wscpa-blog/2015/04/23/think-you-are-too-small-to-be-a-target-of-cyber-crime-think-again-?Site=WSCPA#.VVExkpMsDCo [4/23/13]
3 - dailyfinance.com/2015/02/12/anthem-customers-protect-your-accounts/ [2/12/15]
4 - businessinsider.com/9-things-youre-doing-that-make-you-a-perfect-target-for-hackers-2015-5?op=1 [5/6/15]
5 - washingtonpost.com/news/get-there/wp/2015/04/30/your-new-credit-card-may-not-be-as-safe-as-you-think/ [4/30/15]