10 Tips to Improve Online Security

Print

Like it or not, it has become more difficult than ever to maintain a sense of security in an ever-changing, digital world. We all love the convenience that technology provides. You can do your banking, pay bills, video chat with your physician, e-mail your attorney, make changes to your 401k, or achieve a seemingly limitless range of other important tasks. All of this can be done within a few hours, and without leaving the comfort of your home.

We all value these conveniences because time is our most precious resource. However, it's important to remember that the convenience of technology can sometimes adversely affect our security. From a technological standpoint, the more convenient something is, the less likely it is to be secure. To grasp the importance of this fact we need to understand what security means.

Security is a lot like insurance. It is oftentimes impossible to appreciate the value of security until it is needed most or no longer there. In my 15+ years of experience in dealing with cybersecurity, I have rarely seen a case where an individual could not have avoided a bad situation by following just a few basic rules.

#1 - Strong Passwords

Passwords should always be 8 or more characters long. Using uppercase, lowercase, numbers, and symbols also greatly decreases the chances of someone guessing your password. Avoid things that are easily guessed (i.e. birthdays, kids/spouses/pets names, repeating letters, incremental numbers, and so on). It seems foolish, but the password 123456 has been "hacked" more than 25 million times!

#2 - Virus Protection

Most common day Operating Systems have some form of built-in virus protection, but it is seldom adequate. Even the high-quality, free virus protection options are far superior to the built-in versions that came defaulted with your computer. Virus protection keeps you safe from a myriad of threats like ransomeware, trojan horses, worms, viruses, bot nets, and spam e-mail, just to name a few.

#3 - Secure Mobile Devices

Computers have quickly evolved from giant bricks that barely fit on your desk to devices that easily fit into your pocket. Chances are that if you have a smart phone, it's a more tempting target than your desktop or laptop. Smart phones often hold credit cards, banking/finance logins, photos, passwords, contacts, web history, smart home features (think door locks and garage doors), and much more. Something as simple as putting a six digit (not easily guessed) pin code on your mobile device before it can be used can drastically reduce your risk of compromise.

#4 - Backups

In my experience, this is an item that is often overlooked that can really save your bacon. Keeping an offline backup of your data costs next to nothing and can be priceless should you ever need it. You can accomplish this by purchasing a USB drive and occasionally making a copy of your data. Store the drive in a safety deposit box, a safe, or any other secure location. While online backups are an available option, some industry professionals (myself included) are not entirely sold on the idea just yet. What if a bad actor was able to lock you out of your computer or mobile device? How much would you be willing to pay to regain access to your files? With good backups, you'll never need to answer this question.

Over please...

#5 - Don't Save Passwords In Internet Browsers

How many times has a pop-up appeared on a web page where you clicked a response button before reading what it said? Be careful that you are not saving your password to the web browser, especially on a shared computer or public setting. While it's an incredibly convenient feature, not having to log in each time you visit a website, it's also an incredibly risky behavior. Storing passwords is akin to leaving your doors unlocked.

#6 - Know What You Are Clicking

SPAM and phishing e-mails are more prevalent than ever. These e-mails were once easy to spot, but have gotten much better in recent years. There are a couple of simple "rules of the road" to help you safely navigate your e-mail. If you don't 100% trust an e-mail, do not click any links or open any attachments. Malicious code can execute if you do. Take the time to inspect any e-mail for typos, inconsistencies, and unusual requests for input from you. There are very few (if any) cases where you should legitimately provide things like login and password, account number, or any personal information via an e-mail.

#7 - Limit What You Share With The World

Social media is a fantastic way to keep in touch with friends, family, and loved ones. With all of the wonderful convenience of social media comes some risk as well. First, it's important to know how to limit who sees what via your social media accounts. Every type of social media account will have various settings that control what you share, and with whom you share it. A quick Internet search can point you in the right direction to help shore up the security of your social media profiles. It's also incredibly important to limit what you share, period. An estimated 80% of modern day criminals are checking their target's social media accounts. If you are posting social media pictures of your two week long vacation in Aruba, that makes you a decidedly easy target to exploit.

#8 - Suspicious Phone Calls

A more recent development in cyber crime includes vishing. This is the practice of using phone calls to exploit victims. Common examples include calls purporting to be from reputable companies such as Microsoft, the IRS, banks, the local police, etc. These calls often create a sense of panic or urgency in order to make you give up valuable information. Common examples include someone telling you that your computer is infected with a virus, that you owe back taxes, or that there is a warrant out for your arrest. You should never trust these callers or provide them any information whatsoever. Don't talk to them at all and hang up as soon as possible. They can be very persuasive and persistent.

#9 - Update, Review, Repeat

While it can be incredibly inconvenient, updates are a necessary evil. Keep your mobile devices, phones, desktops, laptops, TVs, and all of your smart devices up-to-date. Updates may revert your system back to the least secure options. It's important to review the security settings of your accounts and devices after completing updates to ensure that your systems are as secure as possible.

#10 - Know Your Limits

Lastly, and possibly most importantly, know your limits. If you're not a cyber security guru, find someone who is. The most preferable situation is that you have someone in your life who can help you navigate the online security landscape. Maybe a son, granddaughter, coworker, cousin, or friend. If you don't have someone that you trust to help you keep your online presence safe and in order, there are a number of quality professional services available. You likely have a primary care physician for your physical health, an attorney for your legal protection, and a financial advisor for your investment management, so why would you leave your cyber security to go unchecked?

Print