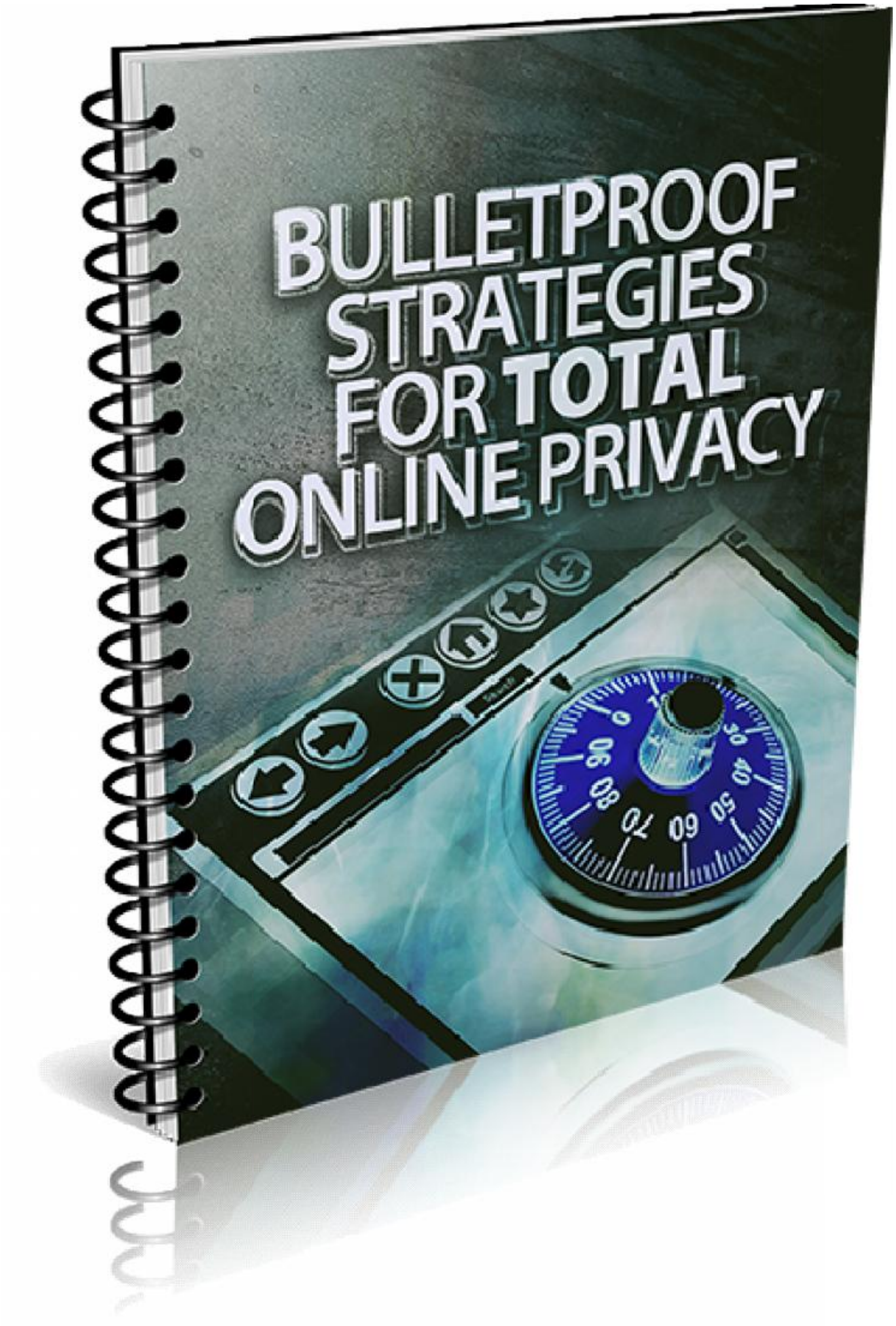

BY BRYAN WILDE

LEGAL DISCLAIMER: THE INFORMATION CONTAINED IN “**THE BULLETPROOF HOME”**, AND ITS SEVERAL COMPLEMENTARY GUIDES, IS MEANT TO SERVE AS A COMPREHENSIVE COLLECTION OF TIME-TESTED AND PROVEN STRATEGIES THAT THE AUTHORS OF THIS COURSE LEARN OVER THE YEARS, RELATED TO HOME DEFENSE, SURVIVAL/PREPAREDNESS. SUMMARIES, STRATEGIES, TIPS AND TRICKS ARE ONLY RECOMMENDATIONS BY THE AUTHORS, AND READING THIS EBOOK DOES NOT GUARANTEE THAT ONE’S RESULTS WILL EXACTLY MIRROR OUR OWN RESULTS. THE AUTHOR OF “**THE BULLETPROOF HOME”** HAS MADE ALL REASONABLE EFFORTS TO PROVIDE CURRENT AND ACCURATE INFORMATION FOR THE READERS OF THIS COURSE. THE AUTHOR WILL NOT BE HELD LIABLE FOR ANY UNINTENTIONAL ERRORS OR OMISSIONS THAT MAY BE FOUND.

THE MATERIAL IN “**THE BULLETPROOF HOME”** MAY INCLUDE INFORMATION, PRODUCTS, OR SERVICES BY THIRD PARTIES. THIRD PARTY MATERIALS COMPRISE OF THE PRODUCTS AND OPINIONS EXPRESSED BY THEIR OWNERS. AS SUCH, THE AUTHORS OF THIS GUIDE DO NOT ASSUME RESPONSIBILITY OR LIABILITY FOR ANY THIRD PARTY MATERIAL OR OPINIONS.THE PUBLICATION OF SUCH THIRD PARTY MATERIALS DOES NOT CONSTITUTE THE AUTHORS’ GUARANTEE OF ANY INFORMATION, INSTRUCTION, OPINION, PRODUCTS OR SERVICE CONTAINED WITHIN THE THIRD PARTY MATERIAL.

WHETHER BECAUSE OF THE GENERAL EVOLUTION OF THE INTERNET, OR THE UNFORESEEN CHANGES IN COMPANY POLICY AND EDITORIAL SUBMISSION GUIDELINES, WHAT IS STATED AS FACT AT THE TIME OF THIS WRITING, MAY BECOME OUTDATED OR SIMPLY INAPPLICABLE AT A LATER DATE. THIS MAY APPLY TO THE “**THE BULLETPROOF HOME”** AS WELL AS THE VARIOUS SIMILAR COMPANIES THAT WE HAVE REFERENCED IN THIS EBOOK, AND OUR SEVERAL COMPLEMENTARY GUIDES. GREAT EFFORT HAS BEEN EXERTED TO SAFEGUARD THE ACCURACY OF THIS WRITING. OPINIONS REGARDING SIMILAR WEBSITE PLATFORMS HAVE BEEN FORMULATED AS A RESULT OF BOTH PERSONAL EXPERIENCE, AS WELL AS THE WELL DOCUMENTED EXPERIENCES OF OTHERS.

NO PART OF THIS PUBLICATION SHALL BE REPRODUCED, TRANSMITTED OR RESOLD IN WHOLE OR IN PART IN ANY FORM, WITHOUT THE PRIOR WRITTEN CONSENT OF THE AUTHORS. ALL TRADEMARKS AND REGISTERED TRADEMARKS APPEARING IN “**THE BULLETPROOF HOME”** ARE THE PROPERTY OF THEIR RESPECTIVE OWNER

KEEPING YOUR COMPUTER AND YOUR IDENTITY SAFE

As many as 90 percent of all homes in the United States own at least one computer or other Internet capable device and the number continues to grow. In a society that is becoming increasingly dependent on technology for everyday tasks computers, laptops, tablets, and smartphones have become a necessity for daily life. Social media, online banking, and even working from a mobile device are all commonplace and the abundant risks associated with performing these actions online has become more apparent in light of recent increases in cybercrime.

What is Computer Security?

Keeping your computer and personal information safe is a lot more than just installing antivirus software. Although antivirus software is an important aspect of maintaining a secure online environment, there are many other facets to a complete computer security solution.

Understanding how to protect yourself online starts with understanding the variety of dangers that are present. Well beyond the viruses that often make news headlines, threats can come from many unlikely sources. One of the main reasons why cybercrime is so prevalent and effective is that most Internet users do not understand the basics of computer security. This makes them extremely easy targets for online theft.

Possessing some general knowledge about the many threats to the integrity of your machine and your personal information is the basis of computer security. Armed with this knowledge, you are better able to make changes to your Internet habits and use tools when appropriate to mitigate the risks imposed by cybercriminals around the world.

Types of Threats

Viruses and other forms of malware appear daily across the Internet. Malware is a term used to describe a variety of malicious software components that include Trojans, worms, spyware, and of course, viruses. Although countless variations exist, most malware that affects personal computing can be classified into a few major categories.

Viruses

By definition, a computer virus is a program that is capable of self-replicating. Although the term virus is commonly used to describe many forms of malware, many of these other types of malware do not self-replicate and should not be described as such.

Viruses are typically attached to program files designed to be installed and run on the computer system. As the virus replicates throughout a machine, system performance will be affected at the very least. A virus can be programmed to complete many different tasks up to and including completely destroying the hard drive of your machine consequently rendering it useless without a fresh software installation. This can result in the loss of all documents, pictures, and other valuable files.

Trojan Horse (Trojan)

Similar to the Greek myth from which it derived its name, a Trojan is designed to appear as a useful piece of software that drops a malicious payload simultaneously. The payload could be anything including programs that steal sensitive information, a key logger (program that records what you type), remote access to the computer through a backdoor, or even use of the webcam on your computer. Many times these Trojans are not detected until it is too late because they operate under the guise of a legitimate program that you may have downloaded. This could be an antivirus program or a movie download.

Worms

A worm shares similarities with both viruses and Trojans. Like a virus, a worm replicates itself. Instead of replicating within a specific computer, however, a worm will often seek to copy itself across a network or the Internet. Worms are typically installed alongside legitimate software that has been compromised similar to the way a Trojan is spread. In fact, many times worms are used to distribute Trojans across large corporate networks automatically. Worms can be found in malicious email attachments where they quickly email themselves to every person in the infected computer’s contact list or via social media sites like Facebook where they can quickly disseminate to multiple Facebook contacts at once.

Rootkits

A rootkit is not a specific type of malware itself. Rather, it is a new method of installing many common viruses and Trojans using root (administrator) access. The danger of a rootkit is that it is often much harder to detect and removal can be especially difficult because these programs are capable of disabling antivirus software as a result of the administrative privileges obtained. Most new antivirus products have rootkit detection built-in but this sneaky form of malware can slip through the cracks with ease.

Phishing

Phishing refers to the act of attempting to acquire private information such as passwords or even credit card numbers by pretending to be another, trustworthy entity. An example would be a website designed to look just like the Facebook login page when in reality it is not affiliated with Facebook at all. Instead, your login information is sent to a cybercriminal somewhere in the world who now has access to your Facebook account and all the personal information contained in it.

Botnets

A botnet is a collection of computers controlled by a program embedded within each machine. Although there are some benevolent botnets, most of them have malicious intent and are typically installed without the knowledge of the computer owner. Botnets can be used for many different purposes including Denial of Service (DoS) attacks that are capable of rendering an entire network useless. Usually a botnet is installed alongside other legitimate software similar to other forms of malware. A botnet may sit idly for months or even years without adversely affecting the machine at all. It will listen for instructions from a criminal and spring into action at a moment's notice when required to perform a task.

Spyware

Spyware is a software program designed to collect user information without knowledge or consent. Key loggers are a popular spyware implementation that records every keystroke and sends it to a remote location where the results can be analyzed by cybercriminals. Information obtained may include username and password combinations, credit card information, or other personal data.

Adware

Adware is not always intended to be malicious. Many companies that offer free versions of popular software include built-in advertisements that may pop up automatically. These advertisements are how companies justify giving the software away for no charge. Other forms of adware have the sole intention of coercing users into purchasing software and other products they don't need by constantly inundating them with purchase offers. Sometimes the advertisements are so intrusive that the computer is rendered practically useless.

Antivirus Software

Installing an antivirus program on a computer is one of the most common methods used to prevent virus infection. Most new computers come with at least a trial version of antivirus protection requiring that a license be purchased for continued protection.

Before going any further, it is important to understand a key distinction in terms. Although this software is often called "antivirus", it is more appropriate to call it "anti-malware" protection. In addition to protecting against computer viruses, modern antivirus software can also protect against spyware, phishing scams, botnets, and a host of other online dangers.

Choosing the Best Antivirus Solution

There are many factors to consider when choosing antivirus software. Price is certainly an important factor for many people. Interestingly enough, there are many free antivirus programs available that will do an acceptable job of providing adequate protection from most threats. Choosing the best solution for you will depend on a number of factors dictated by the way you use the Internet and your computer hardware. The following steps will help you pick antivirus software that best meets your needs.

1. Determine what Operating System your computer is using. Examples include Windows, OSX (Apple), and Linux among others. If the operating system you are using is not readily apparent, consult the manual that came with your equipment to find out. Some antivirus programs are only compatible with specific operating systems limiting your choices to those that are appropriate for your application.
2. Assess the way you use the computer and the overall performance of the machine. If you enjoy online gaming frequently, antivirus software that suppresses potential warnings during gameplay is ideal. If you have an older computer, the impact of antivirus on overall system performance is an important consideration.
3. After narrowing down your choices based on the information gathered in steps one and two, check with antivirus certification agencies to compare the effectiveness ratings of your short list. These certification and testing agencies provide information about all major antivirus solutions. If a solution you are considering is not independently certified, it is best to look for another option.
4. While researching each antivirus program, look for the detection rates of each. The detection rate refers to the software's ability to detect malware before it has a chance to damage or compromise your system. A high detection rate signifies a program that has a better chance of stopping an attack before it starts.
5. Once you have narrowed your list down to two or three options, consider testing each one for at least a week or two. Determine how well your system handles the additional load of antivirus software running in the background and how comfortable you are using the interface of each solution. Even paid antivirus software companies usually offer a free trial period lasting anywhere from a week to a month before you have to purchase a license. This provides ample time to give each option an honest assessment before making a final decision.

Free vs. Paid

Antivirus software can cost hundreds of dollars per year although most residential licenses cost between $20 and $60 per year. Keep in mind that this figure is for one computer. Homes with multiple computers will need separate licensing for each machine. Many providers offer bulk discounts for those who require more than one license but costs can quickly escalate.

To combat the rising costs of antivirus software, many companies have begun offering free versions of their software. Often, these offerings are simply stripped down versions of the premium protection afforded to you after purchasing a license. Free versions will have the same virus definitions (a built-in database that tells the program what viruses to look for) and the same user interface. Free antivirus software is a viable option for many people. Most companies only permit free antivirus software to be installed on personal computers for residential use while businesses are typically required to purchase licensing for their machines to remain in compliance with the copyright laws that protect the software.

You may be wondering why people pay for antivirus software when free options (often from the same company) are available. The answer lies in the extra features provided by the premium, or paid, versions. Free programs provide antivirus protection. That is the extent of their purpose. If you download a virus-infected file or attempt to install a game laden with malware, free antivirus will alert you to the problem and remove the infected files.

Paid versions include many other features that ensure your online safety. Email scanning is a common feature not typically found in free antivirus programs. Malicious phishing websites are also detected in premium releases. Although phishing scams take many forms premium antivirus programs can usually detect these fake websites and warn you before inputting sensitive information.

Another benefit to premium antivirus software is the availability of customer support when trouble arises. Free products do not usually offer customer support. If they do, there is typically a charge associated with getting help and it can be very expensive. As a paid antivirus subscriber, you have access to support via online chat or telephone whenever you have a question or problem. If you run into issues installing or updating the product at any time, help is not far away. Customers using free versions are usually left to figure out problems on their own or not at all.

Either option will provide protection against online threats but the extent of that protection varies from product to product. Regardless of which option you choose make sure that regular updates are offered by the manufacturer. New viruses and other threats are created daily and a program that may protect you one day may be insufficient the next as new forms of malware emerge. Paid antivirus software almost always includes free automatic updates. Many free versions do as well although some may charge for automatic updating. Be sure to research whether or not your antivirus of choice offers free updates before making a decision. If the answer is not readily apparent, consider contacting the software company for clarification.

Network Security

No matter how secure your computer may be, once your information is sent over the air all bets are off. Browsing the Web in public places can be especially dangerous and open you up to an array of specialized attacks. Even in the comfort of your own home, a network (especially wireless) can be compromised with alarming ease. Fortunately, there are some precautions that can help to safeguard your network from unwanted intrusion.

Home Network Security

If your computers and other Internet-enabled devices are connected directly to a modem, there is little else you can do to protect your network. Although intrusion is still possible, it is much more difficult and probably not worth a criminal's time. Wireless (Wi-Fi) networks, however, pose a series of new threats that could leave your information subject to interception by someone within range of your Wi-Fi network.

Whether you were given a wireless router from your Internet Service Provider or you purchased one at the local electronics store, there are some basic configuration steps that are required for security purposes. By default, many wireless routers come programmed with standardized settings that are well known to criminals and can compromise your entire network in a matter of seconds.

1. Change the default username and password combination of the equipment. Most routers are sent from the factory with a default username and password combination that is well known to hackers around the world. If you fail to change this information immediately, anyone can log into the network and make configuration changes that will subject you to further attack.

2. Use password encryption technology to protect the network. Every modern router will support some form of encryption and it should be enabled. Even though these encryption methods are not foolproof, few things are more dangerous than broadcasting an unencrypted password around for anyone to stumble upon.

3. Make sure the password you create for accessing your network is a secure one. Refrain from using easily guessed passwords such as the name of the family dog. Many routers will come pre-programmed with a unique, randomly generated password that is acceptable in most instances. Although it may be harder to remember, a random series of letters and numbers is always more secure than a commonly used word or phrase.

4. Consider using Media Access Control (MAC) address filtering. Every Internet capable device has a unique MAC address that identifies it on a network to other machines. Most routers have a setting that allows setting the MAC addresses of all your devices into a "safe list." Devices on this list are allowed access to the network while devices with other MAC addresses are not. This will prevent many attacks from occurring as network access becomes much more difficult even if the password is known.

5. Most routers also provide a built-in firewall that prevents some forms of forced network access. Often this setting can be turned on or off depending on the application. Some online games, for instance, will not function with the firewall turned on. Under normal circumstances, make sure the firewall of the router is enabled.

Public Network Security

Having access to Wi-Fi in public places can be a great way to surf the Web or get some work done on the go. It is also an excellent place for criminals to gain easy access to your personal information. Coffee shops, airports, and Internet cafes are havens for hackers who can see everything you are doing using various tactics. They may even be able to gain access to your files while you are using your computer connected to a public network.

Although the wording will differ depending on the operating system you use, most devices will prompt you with a security warning when you connect to a new wireless network. Typically it will ask you if this network is in a public place and protect your files if you answer yes. Settings for private networks (such as your home) are usually more lenient and allow for file and printer sharing. Used in a public network, these settings can allow criminals to access your files. Always be sure to turn off file sharing and network discovery options when using publically available Wi-Fi.

In addition to the potential security breach created by leaving your files open for access, there is another dangerous form of hacking that is often experienced on public networks known as a “man in the middle” attack. A hacker equipped with a special piece of hardware is able to intercept all communications between computers on the network and the wireless access point. Even encrypted communications are not secure in many instances. Online banking transactions, credit card information, and sensitive login details are all compromised during a man in the middle attack.

Unfortunately, there is little that can be done to prevent this type of threat. The best practice is to refrain from accessing sensitive information whenever possible while using public wireless service. If access to sensitive information is required, look for the padlock symbol near the address bar in your browser. This signifies that the connection is encrypted and reduces the likelihood of a breach. It is not foolproof and an adept hacker can get through the encryption if they want to but it will prevent many attacks.

Password Security

It may seem like common knowledge that strong passwords are one of the best defenses against computer crime but the reality is that it is an area of computer security not usually given much thought. The online giant Google recently reported that poor passwords persist as one of the primary causes of computer crime and identity theft in the world.

People tend to create passwords that they will remember easily. A pet’s name, favorite sports team, or family member’s birthday are all common passwords. Unfortunately, these passwords are also easy to guess or crack using available technology. Many times people will use the same password or a variation of it for multiple online activities. Once a hacker figures out one password, it can open up your entire world to a criminal intent on stealing your money, your identity, and anything else they can get their hands on.

Make sure to use random passwords that are difficult to guess. Refrain from using words or common phrases and try to use a combination of letters, numbers, capital letters, and symbols. There are free password generation tools available online that create random passwords. These passwords will be difficult to remember but provide a much better level of security for your personal information.

One trick that helps you remember all your secure passwords is to use a separate program or smartphone app that is designed to keep track of them. Using a single password, you will have access to all of your other passwords. Of course this system is only as robust as this single password and it should follow the same secure password conventions already discussed.

Unsafe Internet Practices

Even when you follow every computer security recommendation that you can, your computer is only as safe as the person using it. Even the best antivirus software can’t stop you from downloading a file or installing a program if you choose to do so. Everyday people fall victim to malware not because they did not have antivirus installed or because their Wi-Fi network wasn’t secured properly but simply because they practice unsafe browsing habits that leave them more susceptible to attack.

Online file sharing is a common method of infection. Often these sites are used for illegal purposes to begin with such as downloading movies or music without proper licensing. In addition to the possible legal consequences imposed by these actions, many of the files floating around these file sharing sites are laden with viruses and other malware. After downloading an infected movie file, malware is often installed in the background.

In general, downloading any file when you are not 100 percent sure of the origin is unsafe. People will often search the Web for free versions of expensive software. Unfortunately, hackers prey on these individuals by offering “free versions” of software that are nothing more than viruses.

Email attachments from unknown sources are another danger. If you do not know the sender, do not open any attachments contained within an email. Sometimes even images within an email can have hidden malware lurking inside them. If you receive an unsolicited email from an unknown source it is usually best to delete the message without even opening it.

Physical Security

When most people think of computer security, many of the things that have already been discussed come to mind. Another often overlooked aspect of computer security is the physical security of your device. Especially as consumers rely more heavily on portable machines such as laptops and tablets, criminals are on the prowl for unattended equipment. Aside from the obvious loss of a valuable piece of equipment, the amount and type of personal data stored can make the loss astronomical.

Computer theft is on the rise with as many as 2 million laptops being stolen each year in the United States alone. This figure does not include theft of smartphones or tablets which often house much of the same sensitive information as their larger counterparts. Physically securing your equipment is at least as important as any other security measure you take. After all, what good is a secure computer that has been stolen?

A laptop lock is a simple, inexpensive way to secure your machine in public places. Similar to a bike lock, a cable loops through an opening in the laptop or through a specialized slot (known as a Kensington slot) and hooks to an immovable object making it difficult to take quickly. Even if you step away from your computer for only a moment, a thief can take it. Locking it up prevents this common mishap from occurring.

Some companies have begun offering software based solutions that include GPS tracking to help locate stolen laptops. These services also allow subscribers to remotely wipe the computer which greatly reduces the chance of identity theft or bank fraud if the laptop is not recovered.

Even if your laptop is not stolen and you are not the victim of a public network attack, your information is still not completely safe. When people are in close proximity to one another such as in an airport, on a train, or in a coffee shop, other people may be able to see your computer screen and gain sensitive data just by watching you. In a matter of minutes a potential thief could be able to ascertain where you live, where you bank, and what company you use for car insurance. Coupled with a well-placed phishing scam, your personal information is immediately at risk.

The best way to protect yourself from prying eyes is to install a privacy screen. These screens are readily available and inexpensive. A privacy screen only provides a viewable angle when looking directly at the screen from a short distance. This prevents others from viewing sensitive information without your knowledge and consent.

Mobile Device Security

Recent studies suggest that the number of mobile devices used in the United States exceeds the population and the numbers continue to grow. On average, consumers own two mobile devices and these smartphones and tablets are just as powerful as computers. Keeping your information safe in a mobile world is just as important as computer security for protecting your investment and your identity.

The same techniques used to safeguard your computer's Wi-Fi connection should also be implemented for your cell phone or tablet. These devices are not impervious to hackers and as more people go mobile, criminals are beginning to move away from conventional computer viruses and instead focusing on mobile malware.

Like their larger desktop counterparts, antivirus protection is available for mobile devices as well. Often these programs are made available by the same companies that provide computer security solutions. Good antivirus protection for your mobile device is just as important; especially if you shop online or access your bank account using the device.

Due to their small size, mobile phones are even more susceptible to physical theft than laptops or large tablets. It is easy and all too common for a phone to be left on a desk or chair practically begging unscrupulous people to steal it. Fortunately, there are many software options available that can safeguard your information even if you do misplace it. Logging into a secure website from a computer allows you to locate the missing device or at the very least wipe your information from the device. Similar to losing a laptop, the loss of a phone is a mildly tragic financial set back but the ramifications of your identity being compromised are outright devastating.

Since mobile devices are often connected to the cellular network there is an additional threat not present with laptops or other devices requiring Wi-Fi. Cellular phones use radio transmissions to communicate with the network. Encryption algorithms are in place to help safeguard your data as it travels through the air. Although difficult, hackers do have the ability to intercept cellular transmissions and decrypt the data. Conducting business online via your smartphone is a convenience and sometimes even a necessity. Try to keep these sensitive transactions to a minimum when using the cellular network to reduce the chances of having your data intercepted

Identity Theft

In an age driven forward by technology, identity theft has become a serious concern for many. Recent statistics regarding identity theft are staggering. Over 50 percent of all stolen identities reported are a result of online theft. This could be a credit card number, a social security number, or online banking information among other things. Over 1 in 10 Americans have already been a victim of identity theft and the figures continue to grow.

Technology has made everyday transactions much easier. Unfortunately, technology also makes it easier than ever for thieves to steal your information and use it for numerous malicious reasons. Preventing identity theft is a daily effort that requires vigilance and knowledge of the behaviors that make you susceptible to identity theft.

Phishing scams are one of the biggest perpetrators of online identity theft. An email that looks like it's from your bank could actually open a website looking for your online account information. Although the fake website may look legitimate, banks and other financial institutions will never ask for personal information that they already have. Any email asking for personal information should be scrutinized carefully as it may actually be a phishing scheme.

Using up-to-date antivirus software as described above is another effective means of protecting yourself. Not only can malware wreak havoc on your computer, it has the potential to allow hackers access to personal information without your knowledge.

Even though antivirus software is an important component in any online security plan, new viruses may be released before antivirus manufacturers are able to block them. For this reason it is important to monitor your online usage and stay clear of questionable sites. Peer-to-peer (P2P) programs such as FrostWire are an excellent place to share files but are often smeared with viruses and other malware that automatically installs on your system once the file has been downloaded. Even if a software update is released a couple of days after infection, the damage has already been done and your information could be halfway around the world.

Varying your passwords between websites greatly reduces your risk of a widespread identity crisis. Even if one of your passwords is compromised, the multitude of other websites you frequent will not be affected. Remember that software is available to help you keep track of all your passwords securely. Do not write them all down and carry them in your wallet or in another conspicuous spot.

Online shopping is another tool that cybercriminals use to trick you into divulging sensitive information. Even though an obscure website may be offering a slightly better price on that new item you are shopping for, it may be just a ploy to get your credit card information. If you have any doubt that an offer is too good to be true, use an online tool such as Web of Trust to check the validity of the website. If it is not listed in one of these directories, chances are the website is a scam.

One technique that has gained popularity for safe online shopping is the use of third party payment processors such as PayPal. PayPal keeps your payment information safe and send the payment to the merchant on your behalf. Using a system like this means that your personal credit card information is not being transmitted directly to the merchant and provides an extra layer of protection.

Although Facebook, Twitter, and other social media outlets are fun and a great way to share with friends and family, be careful not to share too much information. Even with strict privacy settings in place, it is often possible for others to see information that can then be used to steal your identity.

Monitor your credit profile often. Many credit services are available that will even provide alerts when a new account is opened in your name. If you have not initiated such a transaction, it is usually a sign that your identity has been compromised. By taking an active role in checking your credit profile, you are better able to thwart an attack against your livelihood than someone who does not check on their financial health at least once a month.

There are services available that charge a monthly fee to monitor your credit for you. Life Lock is an example of one such service. Not only do they take an active role in securing your identity so you don’t have to but they also offer a guarantee in the rare event that the service does not catch a theft attempt. Keep in mind that although these services are convenient they are not necessary. Monitoring your own credit on a regular basis and reporting any discrepancies you find is often enough to spot an attack before it gets out of control.

Just because the majority of identity theft is occurring online does not mean that mail and other correspondence historically associated with identity theft are no longer of concern. As much as 43 percent of modern identity theft is still a result of stolen physical property such as wallets or paperwork. Mail containing sensitive information that is discarded improperly is still a favorite among identity thieves. Make sure that any mail with personal information of any kind is shredded before going into the garbage or burned safely.

Keeping yourself safe online may seem complicated. To the uninitiated it may appear to require a lot of work. In reality, a little research and planning combined with some common sense and due diligence is all that is required to ensure a safe online experience. Once the framework is in place and becomes a habit, online safety is no more inconvenient than putting on a seatbelt when you get in your car. So buckle up and stay safe because the Internet is a powerful tool that can also be very dangerous for those who are not prepared.