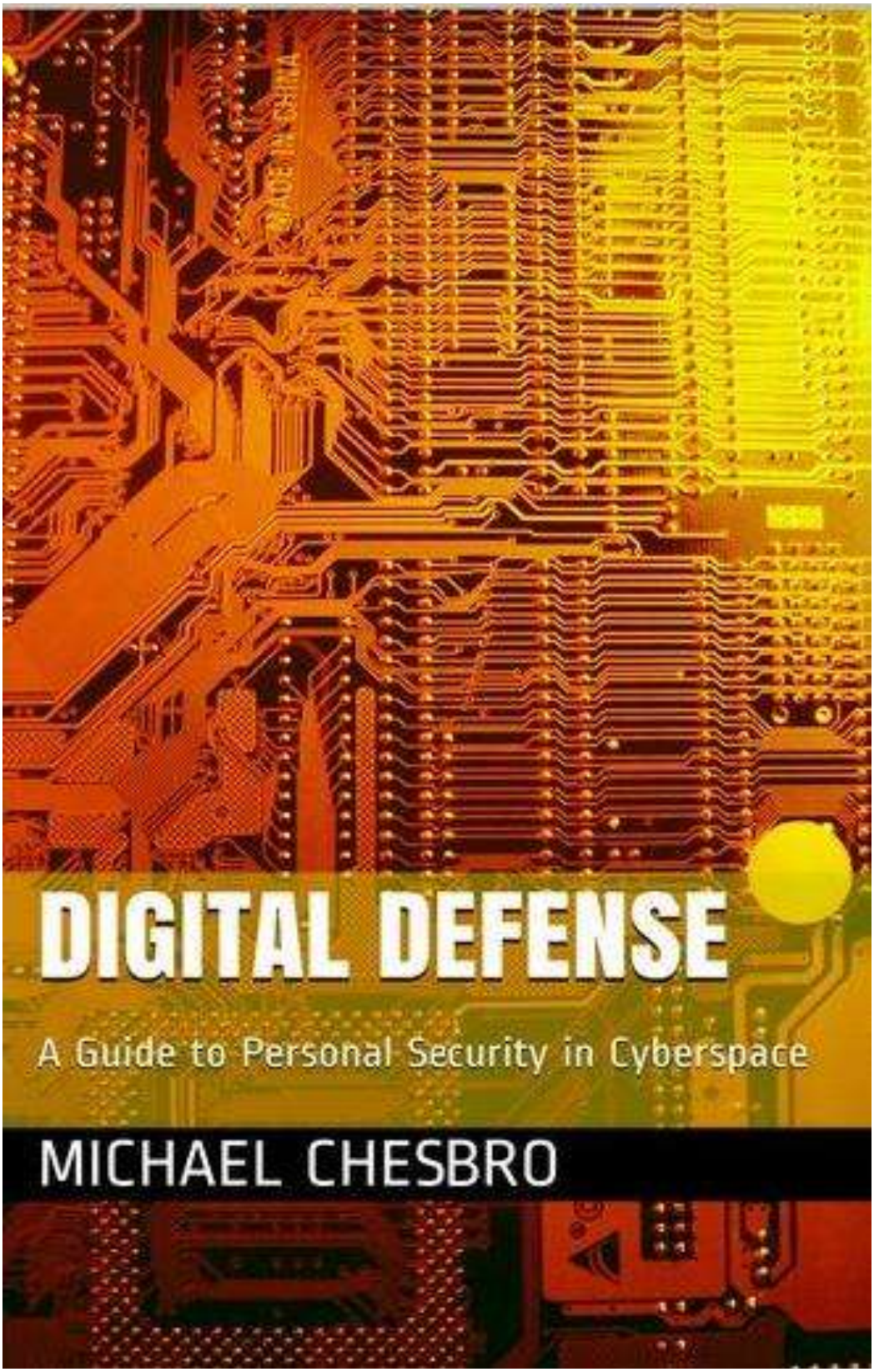
DIGITAL DEFENSE
A Guide to Personal Security in Cyberspace
MICHAEL CHESBRO

Digital Defense

A Guide to Personal Security in Cyberspace

By: Michael Chesbro

Digital Defense: A Guide to Personal Security in Cyberspace identifies the threats that we face in cyberspace, and then provides a number of free and low-cost on-line resources that that average person can use to make himself or herself more secure.

The guide does not presume to be all-encompassing, rather it looks at those products that have proven to be effective, while at the same time are easy for the average person to install and use.

By using this guide and exploring the on-line resources identified herein, you should be able to develop a cyber-security program that best fits your personal needs; and at the same time you should be able to develop a greater understanding of cyber-security concepts for the average user.

© 2013 Michael Chesbro

Contents

You Are Being Watched

Just because you're paranoid doesn't mean that the world isn't out to get you.

You are being watched. Your movements are being tracked. Your communications are being monitored. Your spending habits are being recorded. Every major facet of your life is being entered into databases where it can be retrieved and reviewed by others at any time in the future. Federal government agencies, such as the FBI, NSA, and IRS to name just a few, maintain databases that contain your personal information. State and local government agencies, such as the Department of Motor Vehicles or Department of Licensing, state tax agencies, and your local police department may all have records about you. If you own property, license a business, or register to vote information about you may be contained in public records. Banks, credit card companies, and credit reporting agencies all maintain records and track your financial activities. Businesses maintain records about their customers, and also gather information about people with whom they have never done business for the purposes of marketing, solicitation, and advertising. Telephone companies maintain records of the calls you place and those that are received at your number. This is true for both cellular telephones and for landlines. These telephone records are not kept just for the purpose of billing, because these records are maintained for years after the phone bills have been paid. With a cellular telephone not only are records of your calls made, but your location as well – either through the GPS in your phone, or by identifying to which cell-towers your phone connected. If you use a credit card to shop, the credit card company has a record of what you purchased (or at least where you shopped), and the merchant will often demand that you present ID along with your credit card (although demanding that consumers present ID when using a credit card violates the policies of both Visa and Mastercard). As part of its Mail Isolation Control and Tracking (MICT) program, the U.S. Postal Service takes a photograph of the outside of every piece of mail processed in the United States. According to reports in the *New York Times* these photographs of mail are primarily for sorting and tracking purposes, but have at times been given to law enforcement agencies to allow them to conduct investigations (Nixon 2013). If your wish to fly aboard a commercial aircraft you must show identification and you will be subjected to very intrusive screening before being allowed to board your flight. Similar ID requirements and screenings may apply to other forms of transportation as well, such as trains (i.e. Amtrak), and ships belonging to the various cruise

lines. Even bus and subway travel in some areas will subject you to ID and screening requirements. If you drive a car, the license plate identifies its registered owner to anyone with access to the state Department of Motor Vehicles database. If you have an electronic toll or parking pass, the date, time, and location of your vehicle is recorded every time you use your electronic pass. Although we tend to think of electronic toll passes as only recording information when we cross a toll bridge or drive along a toll road, there is really nothing to prevent electronic readers from being installed at other locations to monitor traffic patterns and identify visitors to specific areas. If you walk around in any major city, or even in some small towns, surveillance cameras record much of what you do. Walk into any bank, most government buildings, and many major department stores and you are captured on video. Video surveillance also often records parking lots, the entrances and exits of apartment buildings, and even your travel along the public streets.

If you have employer supplied Internet access, a work e-mail account, or a cell-phone provided by your employer, what you do on-line, the content of your email, and the calls you make can all be monitored by your employer. In most cases, employees have no expectation of privacy when using computers, telephones, and Internet connections provided by their employers. Courts have generally held that employers have a right to monitor communications on their own networks as long as they have a legitimate business purpose for doing so. However, even without a legitimate business purpose; there is little to prevent a network administrator from monitoring all traffic on the network.

Businesses aren't just monitoring and tracking their employees, they are also monitoring and tracking their customers. A July 2013 article in the *New York Times* revealed how major retailer Nordstrom's (and perhaps other companies as well) tracked the Wi-Fi signals of customer's cell-phones when they entered a Nordstrom's store. "*Nordstrom's experiment is part of a movement by retailers to gather data about in-store shoppers' behavior and moods, using video surveillance and signals from their cellphones and apps to learn information as varied as their sex, how many minutes they spend in the candy aisle and how long they look at merchandise before buying it.*" (Clifford & Hardy 2013)

It's not just businesses tracking your cell-phone, the government is doing so as well. On July 30, 2013 the Fifth Circuit Court of Appeals ruled that the government can track your cell-phone

location data without the need for a warrant. Part of the Court's reasoning was that use of a cell-phone is entirely voluntary, and thus a person carrying a cell-phone consents to some degree of tracking and monitoring. Cell-phone service providers collect and maintain cell-phone location data for their own business purposes, and the government is just collecting that information after the fact (Crump 2013). Depending on your cell-phone service provider your call detail records and records of the cell-towers used by the phone are maintained for one to two years. Text message details may be maintained for up to seven years. The details of your calls and text messages, and the cell-towers to which you connected are maintained in the records of cell-phone service providers for years. The government wanting to know where you were six months ago, or who you talked with last year need only obtain a copy of your cell-phone records.

In March 2013 the American Civil Liberties Union (ACLU) wrote:

> *"Of all of the recent technological developments that have expanded the surveillance capabilities of law enforcement agencies at the expense of individual privacy, perhaps the most powerful is cell phone location tracking. And now, after an unprecedented records request by ACLU affiliates around the country, we know that this method is widespread and often used without adequate regard for constitutional protections, judicial oversight, or accountability.*
>
> *All cell phones register their location with cell phone networks several times a minute, and this function cannot be turned off while the phone is getting a wireless signal. The threat to personal privacy presented by this technology is breathtaking.*
>
> *To know a person's location over time is to know a great deal about who a person is and what he or she values. As the federal appeals court in Washington, D.C. explained: "A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts.""*

The ACLU published a chart on their web-site that showed cell-phone data retention periods of the major carriers. That chart is available on-line at: https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart.

If you travel internationally the probability that you will be tracked, searched, and monitored increases significantly. United States law has established an exception at the nation's borders to the 4th Amendment requirement for a warrant or probable cause in order to search and seize the

private property of a person crossing that border. The Department of Homeland Security (2013) stated:

> *"The overall authority to conduct border searches without suspicion or warrant is clear and longstanding, and courts have not treated searches of electronic devices any differently than searches of other objects... We also conclude that imposing a requirement that officers have reasonable suspicion in order to conduct a border search of an electronic device would be operationally harmful without concomitant civil rights/civil liberties benefits."*

Simply put, when crossing an international border, Customs and Immigration agents can search your belongings, to include the contents of your laptop computer, smartphone, and other electronic devices without the need for a warrant, or even the requirement that there be some suspicion that you are involved in criminal activity or other wrongdoing.

Depending on the purpose for your overseas travel, and where you travel, you may become the target of foreign intelligence agencies, corporate espionage, or criminal organizations. According to the FBI (2013):

> *"The willingness of US scientists and scholars to engage in academic exchange makes US travelers particularly vulnerable not only to standard electronic monitoring devices—installed in hotel rooms or conference centers—but also to simple approaches by foreigners trained to ask the right questions... Corporate espionage is an increasingly serious threat for a business traveler. The perpetrator may be a competitor, opportunist, or foreign intelligence officer. In many countries, domestic corporations collect competitive intelligence with the help and support of their government."*

The National Counterintelligence Executive (2011) issued similar warnings, also pointing out how these foreign spies and criminals are making use of cyberspace:

> *"Foreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security. Cyberspace—where most business activity and development of new ideas now takes place—amplifies these threats by making it possible for malicious actors, whether they are corrupted insiders or foreign intelligence services (FIS), to quickly steal and transfer massive quantities of data while remaining anonymous and hard to detect. Foreign collectors of sensitive economic information are able to operate in cyberspace with relatively little risk of detection by their private sector targets. The proliferation of malicious software, prevalence of cyber tool sharing, use of hackers as proxies, and routing of operations through third countries make it difficult to attribute responsibility for computer network intrusions. Cyber tools have enhanced the economic espionage threat, and the*

> *Intelligence Community (IC) judges the use of such tools is already a larger threat than more traditional espionage methods."*

The *Internet World Stats* web-site showed that, on June 30, 2012 an estimated 79% of North Americans, 68% of the population of Oceania & Australia, 63% of Europeans, 43% of Latin America and the Caribbean, 40% of the Middle East, and a lesser but growing percentage of the rest of the world were Internet users. In the year 2000 there were approximately 360,985,492 Internet users, but by the year 2012 that number had grown to 2,405,518,376 an increase of 566%. According to the Cellular Telecommunications Industry Association (CTIA) there were 326.4 million active devices, including smartphones, feature phones, tablets, hotspots, etc., in the United States and its territorial population (Puerto Rico, Guam and the U.S. Virgin Islands) in December 2012. If you are among this ever increasing number of Internet and cellular users, your on-line activity is being monitored as well. The web-sites you visit and the content you download is logged in the records of your Internet Service Provider (ISP). Your e-mail contacts, and often the content of your e-mail itself is available to your ISP, and thus to government agencies and perhaps corporations and private investigators with the right connections. Your cell-phone calls, text messages, smartphone access to the Internet, and the location of all or your cellular devices – either through GPS or cell tower triangulation – is recorded. Since most smartphones today contain a camera it is almost certain that in any crowd of people someone will be able to photograph you or record you on video. Whether someone is taking your photograph or recording you on video depends on how much attention you attract to yourself, and just how interesting those around you find your actions and activities to be.

According to the New York State Office for the Prevention of Domestic Violence (2010):

> *The incredible advances in technology in recent years have enabled us to be more connected to people and places than ever before. E-mail, texting, social networking, GPS, and other common technologies have become tools that many of us rely on heavily in our daily lives. For some people, however, these technologies have been used against them. They have been used to track people without their knowledge, to monitor what they do on their computer, and to impersonate them on-line. These people are victims of stalking through the use of technology, sometimes called "cyberstalking". As technology continues to grow and improve, so does a stalkers' ability to terrorize their victims.*

Government Monitoring

In May 2013, Edward Snowden, an employee of the Booz Allen Hamilton Corporation working as a contractor at the National Security Agency (NSA), leaked classified documents to the UK Guardian Newspaper disclosing a massive Internet surveillance program conducted by the NSA. The NSA surveillance program gathered communication metadata. Metadata does not contain the actual content of the communications, but it does contain the type of information found in an e-mail header, or such information as the originating and terminating telephone numbers and the length of the telephone call. With this type of data (metadata) the NSA is able to tell with whom you communicate, how frequently you communicate with someone, and the length of your communications. Knowing this data the government can build association matrices and link diagrams that reveal your friends, associates, and business relationships.

After disclosing the classified data about the NSA-PRISM program, Edward Snowden fled to Hong Kong, and then later to Russia. The United States government charged Snowden with the crimes of Unauthorized Communications of National Defense Information, Willful Communication of Classified Information to an Unauthorized Person, and with Theft of Government Property. At the time of this writing the United States was still seeking to locate and extradite Snowden back to the United States to stand trial.

Also in May 2013 several major news agencies reported that Federal Investigators secretly seized two months of telephone records of Associated Press reporters.

> *Gary Pruitt, the president and chief executive of The A.P., called the seizure, a "massive and unprecedented intrusion" into its news gathering activities. "There can be no possible justification for such an overbroad collection of the telephone communications of The Associated Press and its reporters," he wrote. "These records potentially reveal communications with confidential sources across all of the news gathering activities undertaken by The A.P. during a two-month period, provide a road map to A.P.'s news gathering operations, and disclose information about A.P.'s activities and operations that the government has no conceivable right to know."* (Savage and Kaufman 2013)

The call records seized by the government included the records for both office and private telephones of Associated Press reporters in New York, Hartford, Connecticut, and Washington, DC, as well as the Associated Press office located in the House of Representatives press gallery.

In all this included more than 20 different telephone lines used by over 100 Associated Press reporters and staff (Sherman 2013).

An August 2013 article in the *Olympian Newspaper* reported that members of the Joint Base Lewis-McChord (JBLM) Force Protection Division had spied on anti-war protestors. In a lawsuit filed against Force Protection Division personnel, the protestors alleged that that the spying had deterred their free speech and led to their unlawful arrest thereby violating their First and Fourth Amendment rights (Pawloski 2013). (JBLM is a combined US Army / US Air Force base near Tacoma, WA.) While it is unlikely that Army and Air Force personnel set out to intentionally violate the rights of American citizens, it is also clear that this type of "spying" violated Department of Defense Intelligence Oversight regulations which prohibits force protection personnel from collecting information on US Persons.

Other organizations may monitor the on-line activity of groups of individuals sweeping up the communications of everyone that comes in contact with any member of the group. In September 2013 CNN reported that a California school district had hired a company to monitor and report on the social media posts of 14,000 middle and high school students (Martinez 2013). The school district certainly isn't targeting its students for cyber-crime, and no doubt the school district will argue that monitoring the student's social media activity increases their safety and well-being. But, at what cost?

Cyber-criminals are certainly a threat to our on-line security and personal privacy. Identity thieves, cyber-stalking, phishing, and on-line fraud all pose a criminal threat. But perhaps the greater threat comes from those individuals and organizations who gather information about us and monitor our on-line activities, believing that what they are doing is legitimate and lawful when in fact their activities may be ill-considered, and even illegal.

One very important consideration with the interception and broad monitoring of communications for law enforcement and security purposes is that individuals charged with no crime, and guilty of no wrong-doing will seldom if ever be told that their private communications have been intercepted, recorded, and reviewed. Individuals charged with a crime and taken before a court will have the opportunity to review the evidence against them, to challenge the interception and use of their private communications, and perhaps have that information suppressed and removed

from government records. Innocent persons, never having their day in court will never know which, if any, of their private communications have become part of a corporate investigative repository or government database.

Petraeus and Broadwell – In 2012 a scandal emerged in the mainstream media when it was revealed that CIA Director, General David Petraeus, and Paula Broadwell, his biographer and former military intelligence officer, had been involved in an extra-marital affair. Although Petraeus and Broadwell had taken precautions to keep their intimate communications private, the discovery and disclosure of personal on-line communications lead to the media scandal and ultimately to the resignation of Petraeus from government service. According to Washington Post reporter Max Fisher (2012) Petraeus and Broadwell used a common G-mail account to communicate with each other. Both Petraeus and Broadwell knew the login and password for this account. To communicate they would login into the account and write an e-mail message as normal, but instead of sending the e-mail they would save the message as a draft and then log out of the Gmail account. Later the other person would login to the Gmail account and read the draft message, and perhaps leave a reply, also saving it as a draft instead of sending it. Because messages were never actually sent or received from the Gmail account there was no e-mail trail to follow, making it much more difficult to trace and identify this type of communication.

The mistake made by Petraeus and Broadwell was that the IP addresses of the computers they used to login to their shared Gmail account were recorded and maintained by Google. Attention became focused on Broadwell after Jill Kelley, social liaison to the military, reported to the FBI that she was receiving threatening e-mail from someone using a Gmail account. The FBI traced the IP address of the computer used to access the Gmail account that had been used to send threatening e-mail to Kelley back to Broadwell. Although the Gmail account used to send threatening e-mail to Kelley was not the same e-mail account shared by Petraeus and Broadwell, once the FBI began to look at other accounts accessed from Broadwell's computer the Gmail account shared by Petraeus and Broadwell was discovered and their affair revealed.

What should be learned from the experience of Petraeus and Broadwell is that true anonymity on the Internet can be extremely difficult. When the techniques used by the Director of the CIA and a former military intelligence officer to safeguard their personal communications fail; this should serve as a clear warning that anonymity is never a sure thing. It is also important to note that

while the relationship between Petraeus and Broadwell was a private matter; the relationship came to light after Broadwell allegedly communicated threats to Kelley triggering an investigation by the FBI. If you wish to safeguard your privacy, it is important to avoid becoming the subject of a criminal investigation or even giving the appearance of criminal activity. A criminal investigation will almost certainly expose parts of your life that while not criminal may be both personal and private. If you wish to live a private life, you cannot lead a criminal life.

No Security Is Perfect

No security is perfect. Countermeasures may not be 100% effective. Defenses may fail. Even good security protocols can be rendered ineffective by exploiting human weaknesses, vulnerabilities, and errors. On the other hand we must not develop a fatalistic attitude, believing that "if they really want to get us they will". Of course, if we assume an adversary with unlimited resources (such as a Federal government agency or major corporation) then we no doubt suffer a significant disadvantage, but it is always possible to increase the time, effort, and resources that an adversary must expend to effectively target you. Even if you are being targeted by a government agency or major corporation the techniques we will discuss can make the effort to target you worth more than the reward.

By increasing the effort required to target you it is often possible to cause an adversary to choose a different target. Cyber-criminals, corporate spies, foreign agents, and government investigators frequently target the 'low-hanging-fruit', they go after the easiest, most cost effective targets. Even if you are the specific target an adversary is after; it is important to remember that not all adversaries have unlimited resources. It is possible to employ security that requires greater resources to defeat than an adversary has readily available.

It is also important to employ security in depth. An adversary may be able to defeat a single security measure. No security is perfect. By increasing layers of security, building depth into your cyber-security plan, the weaknesses and exploitable vulnerabilities in one security may be covered by the strengths of another security measure.

Finally, remember that no security measure is of any value if it is not used. If security becomes too difficult, it will not be used regularly. The human factor is often the greatest weakness in any security program. When looking at the various security application in this guide, choose the ones that you can and will employ on a regular basis. Good security employed consistently is better than great security employed occasionally.

Using This Guide

This guide is for people concerned about their personal privacy. In writing this guide the author has made a few basic assumptions. First it is assumed that you are an average user of technology; you know how to use the digital devices that you own. You know how to download and install a program from the Internet, but that you are not a computer technician, systems administrator, or similar advanced user. Second, it is assumed that you will continue to use social media (i.e. Facebook, chat programs), send e-mail to friends, family, and co-workers, and that you carry and use smartphones / cell-phones and take advantage of the various features on these devices. Finally, it is assumed that you are not a person engaged in on-going criminal activity, and you are not on the run from the law. You are not being personally targeted by law enforcement or other government organizations.

Too often security advice includes recommendations such as don't use social media, keep your cell-phone turned off and remove the battery, avoid e-mail, and avoid technology to avoid being tracked. While these things will certainly reduce your digital footprint, they also limit your ability to make use of the advantages offered by technology. The purpose of this guide is to provide you with the tools necessary to enhance your security and protect your privacy in cyberspace without requiring you to totally give up your use of technology.

While using this guide it is advantageous to have access to the Internet. Several on-line resources are provided throughout the guide to improve your personal security. At the time this guide was published, all links worked, but as with many things on-line links to security products can change. If you find that a link for a product you want no longer works, you can often find the product by searching for the title using a major search engine such as Google or Bing.

Likewise, as you look at these products and choose the ones that best fit your needs, be sure to look at similar products that you come across that may not have been included in this guide. The purpose of this guide is not to list and review every possible method for enhancing your security in cyberspace, rather its purpose is to provide you with a number of free and inexpensive resources to improve your personal security, and to introduce you to various items that you may not have known were available.

Digital Defense

One of the first and most important steps in securing yourself in cyberspace is to secure access to your digital systems: computer, laptop, tablet, and smartphone. Access to these devices should be secured by a password, pin, or swipe pattern. Someone with casual access to your computer or someone who picks up your cell-phone from your desk should not be able to quickly access your data.

BIOS Password – The BIOS or 'Basic Input Output System' is operating instructions encoded on a chip (firmware) that provides start-up instructions for your computer. In most BIOS it is possible to set a password that is required before the system will start. When you set a BIOS password your computer will not start (boot) until that password is entered. A BIOS password is an important first step in securing any personal computer or laptop. To access your computer's BIOS you will need to press a specific key (F2, F11, DEL, or something else) during startup. The specific key to access your BIOS depends on your system, but should be listed in your computer's documentation, and may be displayed on the screen during startup. Once you have accessed the BIOS you should see an option to enter a password.

Windows Password – After the BIOS has completed its start-up functions, control of the computer is passed to the operating system. In this case we will assume that the operating system is Windows, and we will set a Windows password. When set this password is required before the computer finish booting and allow you to access the programs on your computer. In Windows 7 a password may be set by going to the 'User Accounts and Family Safety' section in the Control Panel. Having a Windows password set is an important next step in securing your computer.

With both a BIOS password and Windows password set on your computer you will be required to enter each of these passwords (they should be different) whenever you boot your computer. This adds depth to your computer security making it much more difficult for anyone to gain unauthorized access to your system. However, this will also add several more seconds to the time it takes you to start your computer because the boot process is going to stop twice and wait for you to enter your passwords. Once your computer has completed its startup sequence you

will not have to enter your passwords again unless you restart your computer or unless you have a screensaver password or password on wake set.

It is important to understand that both a BIOS password and Windows password can be bypassed. A BIOS password can be bypassed by removing the CMOS battery from the computer, or by flashing the BIOS (installing a new BIOS). A Windows password can be bypassed with programs such as Ophcrack (discussed later in this guide). But, these things take time and may be beyond the capability and knowledge of many attackers.

Screensaver Passwords & Password on Resume (Wake) – In Windows you can set both a screensaver and specify a length of time before your computer switches to sleep mode. Both the screensaver and sleep mode allow you to set a length of time before either the screensaver activates or the computer switches to sleep mode, and in both cases you can require a password when you resume using your computer. In Windows 7 this will be your Windows password. A screensaver or password on resume (wake) is a good idea if you walk away from your computer and forget to log-off or lock (press the Windows key and the letter "L" at the same time) your computer.

PIN, Password & Swipe Patterns on Cell-Phones and Tablets – Because your cell-phones and tablets are your most portable digital devices it is essential that they be protected with PIN, password, or swipe pattern. The specific method of setting a PIN, password, or swipe pattern on your cell-phone or tablet varies a little from one model to the next, but is generally under the settings menu. Some mobile devices allow stored data encryption. If your device allows encryption be sure that you have it turned on. An option to wipe all data on a smartphone after a number (often 10) of incorrect passwords are entered is available on many devices. This option will reduce the possibility that someone could gain access to the data on your phone by guessing your passcode. However, this option also creates a vulnerability if a child plays with your phone and entered a number of wrong passcodes, or if someone with malicious intent simply entered 10 wrong passcodes with the intent of deleting the data stored on your smartphone.

Choosing A Strong Password – A password is often the only thing that restricts access to our digital devices and to our encrypted files, communications, and accounts. Because of this it is essential that we choose strong passwords. Password strength is increased by length and by

complexity. In general the longer and more complex a password is, the stronger that password will be. However, the greater the length and complexity of a password, the more difficult that password can be to remember.

Password cracking programs continue to improve. To avoid having your password susceptible to these cracking programs there are some important considerations that must be taken into account. When choosing a password:

- Do not use any word found in a dictionary (to include foreign dictionaries)
- Do not use a word with a single character before or after it (i.e. 2Password or Secret%)
- Do not use a single word with letter substitutions (i.e. P@$$word)
- Avoid common keyboard patterns such as qwerty and asdfgh
- Passwords should be at least 10 characters long. Passwords of 14 characters or more provide better security.
- Passwords should contain a combination of upper and lower case characters, numbers, and symbols.

Microsoft Safety & Security Center – Password Strength Checker
https://www.microsoft.com/security/pc-security/password-checker.aspx

You can check the strength of your passwords using a password strength checker such as the one provided by the Microsoft Safety & Security Center.

Ophcrack (http://ophcrack.sourceforge.net/) – Ophcrack is a free, open source password cracking program, designed to crack Windows passwords. Ophcrack uses rainbow tables (pre-calculated password hashes), and brute force techniques to crack Windows logon passwords. You can download the Ophcrack LiveCD, burn the ISO to a disk and run it against your own computers to test the strength of your Windows logon password. Ophcrack cannot crack all passwords, but if you have a weak Windows password booting your computer with the Ophcrack LiveCD and letting the program run will often crack all the weak Windows logon passwords on your system.

Encrypting Data on Your Computer

Sensitive information stored on your computer should always be stored in an encrypted format. Encryption is especially important on any portable computer (such as a laptop), and is a good idea on any computer. After all, any computer can be lost or stolen.

Encrypting File System (EFS) – EFS is part of the professional editions of Windows (Windows 2000; Windows XP Professional; Windows Vista Business, Enterprise, Ultimate; Windows 7 Professional, Enterprise, Ultimate; and all versions of Windows Server), but is not fully supported in the Home versions of Windows. If you use a version of Windows that supports EFS you can encrypt files by right clicking on the file or folder you want to encrypt, click properties, then advanced, and then check the box "Encrypt contents to secure data." EFS relies on a symmetric key associated with a user's logon to encrypt files, and is transparent to the user, other than encrypted file names being highlighted in green. Because the files are automatically decrypted when opened and encrypted when closed there is no user interaction required which makes for a very efficient and user-friendly system to safeguard your files.

An EFS encrypted file cannot be read on another computer because the encryption key is not present. Likewise, on a computer with multiple users an EFS encrypted file cannot be read by another user because the file is not associated with the user logon used to create it. Thus, if someone steals your external drive, or attempts to bypass your logon by removing the hard drive from your computer and installing it in another computer without a password; your files still remain protected by the EFS. Of course, if someone can access your computer while you are logged on, they will have access to your EFS encrypted files as well. The primary limitation of EFS is that it is only available on the professional versions of Windows. If you don't use a compatible version of Windows, EFS may not be an option, but there are other file encryption programs that you can use, and if you do use EFS you can use it in conjunction with other encryption as well.

TrueCrypt – (http://www.truecrypt.org/) TrueCrypt is a popular, open source encryption program. TrueCrypt can be used to create a virtual encrypted volume on your hard drive, encrypt an external storage device such as a USB (Thumb) drive, or create a drive partition that mounts during Windows logon.

Once mounted a TrueCrypt volume appears to be just another hard disk on your computer. TrueCrypt can be used on any computer as it works independent of a computer's operating system. When combined with a strong password (TrueCrypt recommends 20 characters or more) TrueCrypt provides a very secure, encrypted area to store your sensitive files. A 'Beginner's Tutorial' for new TrueCrypt users can be found on the TrueCrypt web-site at: http://www.truecrypt.org/docs/tutorial

Encryption Wizard (http://www.spi.dod.mil/ewizard.htm) – The Software Protection Initiative Technology Office is run by the U.S. Air Force and provides a publically available encryption program (Encryption Wizard) to protect the exchange of data between the Department of Defense and other organizations. According to the Encryption Wizard web-site: *"Encryption Wizard (EW) is a simple, strong, Java file and folder encryptor for protection of sensitive information (FOUO, Privacy Act, CUI, etc.). EW encrypts all file types for data-at-rest and data-in-transit protection. Without installation or elevated privileges, EW runs on Windows, Mac, Linux, Solaris, and other computers with Sun Java. Behind its simple drag-n-drop interface, EW offers 128-bit AES encryption, SHA-256 hashing, searchable metadata, archives, compression, secure deleting, and PKI/CAC/PIV support."*

Microsoft Office Encryption – Microsoft Office allows users to encrypt and password protect documents (MS Word), spreadsheets (MS Excel) and presentations (MS PowerPoint). This option was available in previous editions of MS Office, but in MS Office 2010 / MS Office 2013 the steps to use encryption and password protection have been simplified.

There are four simple steps to encrypting your documents, spreadsheets, and presentations in MS Office. The method is the same in MS Word, MS Excel, and MS PowerPoint. To use the encryption and password protection function in MS Office 2010 / 2013, click on the "File" tab in the upper left-hand corner of your document, spreadsheet, or presentation. This opens a menu where you click on the "Info" tab and then on the "Protect Document" button. This button opens a new menu, where you click on the "Encrypt with Password" option. This option opens a dialog box where you enter a password. After entering your password, click "OK" and the dialog box will appear a second time where you must re-enter / confirm your password. Click "OK" after re-entering your password and your document, spreadsheet, or presentation is encrypted and password protected.

Once a document, spreadsheet, or presentation has been encrypted in MS Office whenever you attempt to open it you are presented with a dialog box where you must enter the correct password. If the correct password is entered your document, spreadsheet, or presentation will open normally. If an incorrect password is entered you will be unable to access your information until the correct password is entered. There is no limit on the number of times a password may be tried – so choose a strong password to keep it from being guessed.

By default MS Office 2010 / 2013 uses – AES (Advanced Encryption Standard), 128-bit key length, SHA1, and CBC (cipher block chaining) – for encryption (Microsoft MSDN Library 2011). This is industry standard and provides very strong encryption. It is important to be sure that you are saving using the MS Office 2010 / 2013 format (i.e. .docx, .xlsx, .pptx) and not in the MS Office 97-2003 compatible format (i.e. .doc, .xls, .ppt) in order to take advantage of strong encryption. It must be remembered however that the key to unlocking that encrytion is the password used to protect the document, spreadsheet, or presentation. A weak password results in overall weak protection, regardless of how strong the encryption algorithm may be.

To have the best security it is essential that you choose a strong password. In most cases a password of 10 or more characters, containing upper and lower case letters, numbers, and symbols will provide good security. Longer and more complex passwords may provide stronger security, but they will be more difficult to remember. If you forget your password you will lose access to the information contained in your document, spreadsheet, or presentation.

In MS Office 2013, Microsoft has included a "DocRecrypt Tool" that allows an escrow key, created from an organization's private key certificate store, to be embedded in password protected MS Office documents. This allows password protected documents to be decrypted ("unlocked") using the escrow key instead of the password. While the intent of the DocRecrypt Tool is to allow an organization's IT/Security personnel to recover a document where the user has forgotten the password or left the company; escrowed decryption keys also weaken the security of encrypted documents. Concerning the escrowed keys, Microsoft said:

> *"You, the IT admin, are the keeper of the escrow key which is generated from your company or organization's private key certificate store. You can silently push the public key information to client computers one time through a registry key setting that you can manually create or you can create it through a Group Policy script. When a user later creates a password-protected Office 2013 Word,*

> *Excel, or PowerPoint file, this public key is included in the file header. Later, an IT pro can use the Office DocRecrypt tool to remove the password that is attached to the file, and then, optionally, protect the file by using a new password."* (Microsoft MSDN Library 2013)

Simply put, someone with access to the network can install an escrowed decryption key that will decrypt all MS Office documents protected with a password. This has the advantage of allowing the recovery of documents where the password has been forgotten, but also creates a security vulnerability when users are unaware of the escrowed decryption key associated with their MS Office documents.

7-Zip (http://www.7-zip.org/) – Z-Zip is a free, open source file compression program, supporting multiple formats such as 7z, XZ, BZIP2, GZIP, TAR, ZIP and WIM. An advantage of 7-Zip is that it supports AES-256 encryption in both the 7Z and ZIP formats. A Z-Zip archive on your computer, encrypted with AES-256 and protected with a strong password, provides very good security for your sensitive documents and programs. Additionally, files compressed and encrypted with 7-Zip can be e-mailed to others with confidence that they will only be accessible to someone who knows the password associated with those files.

Securely Deleting A File

When you delete a file in the normal manner (drag a file to the 'Recycle Bin' and empty the Recycle Bin) the content of that file still remains on your computer. The computer simply removes the name of the file from the index and marks the space on the disk where the deleted file still resides as being available for use. Until that space is overwritten by a new file, the deleted file remains on the disk and remains easily recoverable.

To securely delete a file, the space that it occupies must be overwritten by other data. In most cases a single overwrite with random data will prevent it from being recovered, however against advanced computer forensics additional overwriting is recommended. The Department of Defense standard (DoD 5220.22-M) uses a system of three overwrites, first overwriting the file area with zeros, then overwriting it again with the number 1, and finally overwriting the file area a third time with random characters. For the most secure erasing of files there is the 'Peter Gutmann shredding algorithm' which overwrites the file area 35 times using various methods to ensure complete data destruction.

Examples of secure erase programs include:

- Eraser (http://eraser.heidi.ie/)
- File Shredder (http://www.fileshredder.org/)
- Freeraser (http://www.codyssey.com/)
- Microsoft SDelete (http://technet.microsoft.com/en-us/sysinternals/bb897443)
- CCleaner (http://www.piriform.com/ccleaner)
- Darik's Boot and Nuke (DBAN) (http://www.dban.org/) – DBAN is designed to completely format all hard drives on a computer.

The listed secure erase programs are not the only ones available, and may not even be the best ones for your needs, but they are all quality programs that will complete destroy the files they are run against.

Protecting Against Viruses, Trojans, Worms, & Other Malware

Malicious software (Malware) includes a wide variety of code including viruses, Trojans, worms, spyware, adware, ransomware, bots, and more. It is important to take precautions to protect yourself against malware in order to prevent your digital devices from being compromised. There are a number of commercial products, but freeware products can often be just as effective. Some examples of these freeware programs are:

AVG Free Anti-Virus (http://free.avg.com/us-en/homepage)

Bitdefender Anti-Virus Free Edition (http://www.bitdefender.com/solutions/free.html)

CClean (http://www.piriform.com/ccleaner)

Malwarebytes (http://www.malwarebytes.org/)

Microsoft Security Essentials (http://windows.microsoft.com/en-us/windows/security-essentials-download)

While some of these programs can be used together, others may conflict (such as a conflict between Bitdefender and Microsoft Security Essentials). You should choose the programs that best fit you needs.

Updates – Operating system developers (Microsoft, Apple, Linux) release updates and patches from time to time. These updates help keep your computer running smoothly and improve the security of your system by patching vulnerabilities. In general you want to turn on automatic updates to keep your system up to date. According to the Microsoft web-site: *"If you turned on automatic updating, then most security, reliability, and compatibility updates will be downloaded and installed automatically. Many updates, however, aren't installed automatically. This includes optional updates and updates that require you to accept new terms of use. You'll need to go to Windows Update to check for updates that need to be installed manually. If you don't use automatic updating, you should check for updates at least once every week. Microsoft typically releases important updates on the second or fourth Tuesday of the month. However, updates could be released at any time."*

Physical Security of Your Digital Devices

Physical security of your digital devices is essential to preventing unauthorized access and compromise of your private information. Physical access to a computer can mean total access to the data stored on the computer.

- If you use a DSL or Cable connection make sure the exterior interface box (where the line come into your house) is locked.
- Lock your CPU tower / case. Many cases have locking lugs that allow you to prevent someone from opening the case by locking the case with a small padlock. Cases that can't be locked should be secured with security seals to detect tampering.
- Use a cable lock to keep someone from stealing your whole computer. This is especially important for laptops, but is also a good idea for desktop computers and their associated peripherals.
- Store external drives and media (i.e. DVD, CD) in a secure location when they are not in use.
- Record the serial numbers and descriptions (make, model) of all your digital devices.

Defense On-Line

In many cases we use our digital devices to connect to the Internet. We exchange e-mail, use search engines to find and download information, shop, bank, and conduct other business on-line. A May 2012 study sponsored by Check Point Software Technologies found that:

> *"Cyber criminals today are increasingly leveraging malware, bots and other forms of sophisticated threats to attack organizations for various reasons, including financial gain, business disruption or political agendas. In many cases, cybercriminals often target multiple sites and organizations to increase the likelihood of an attack's initial success and viral spread. With new variants of malware being generated on a daily basis, many companies struggle to fight these threats separately and the majority of attacks are often left undetected or unreported."* (Ponemon Institute 2012, 1)

The United States Department of Homeland Security (2013a) warned:

> *"Today's world is more interconnected than ever before. Yet, for all its advantages, increased connectivity brings increased risk of theft, fraud, and abuse. As Americans become more reliant on modern technology, we also become more vulnerable to cyber-attacks such as Corporate Security Breaches, Spear Phishing, and Social Media Fraud. Cyber-security is a shared responsibility, and each of us has a role to play in making it safer, more secure and resilient."*

Defense on-line requires that we protect our on-line identities and safeguard access to our on-line activities. Because cyber-crime is not restricted by geography (a cyber-criminal may target you from the other side of the country or the other side of the world) the likelihood of becoming a victim of cyber-crime, cyber-stalking, and illegal monitoring and surveillance is greatly increased if we take no precautions to prevent it.

Every device that connects to the Internet has a unique identification number. This unique number is called an Internet Protocol or IP address and it serves to identify the specific device connected to the Internet. It is important to understand that everything done on the Internet is associated with a particular IP address, and thus every action on-line can be traced. You can see what your IP address by going to various sites on-line which will detect and report your IP address. Some of these web-sites are:

- http://whatismyipaddress.com/
- http://www.whatismyip.com/

- http://ipaddress.com/
- http://www.ipchicken.com/
- http://ip-check.info/?lang=en

Just as these web-sites can detect your IP address, so too can any web-site you visit. Just knowing your IP address can provide your general location, and of course your Internet Service Provider knows exactly where you connected to the Internet. You Internet Service Provide can also see everything that you do on-line. Everything that you do on-line passes from your computer, to your Internet Service Provider's servers, and then out to elsewhere on the Internet.

Many Internet Service Providers maintain logs of your Internet activity for six to eighteen months. These logs are available to various government agencies upon request, but are also susceptible to hacking, theft, and random browsing by your Internet Service Provider. Furthermore, anyone sniffing (monitoring) your traffic to and from the Internet can also create a record of all your on-line activity.

HTTPS Everywhere (https://www.eff.org/https-everywhere) – An important step in securing your on-line activity is to encrypt your Internet traffic. HTTPS Everywhere is a collaborative project between the Electronic Frontier Foundation (EFF) and the TOR Project. HTTPS Everywhere is available for both the Firefox and Chrome browsers. Simply install HTTPS Everywhere as a browser extension and the program will attempt to encrypt your connection to each web-site that you visit. Not every web-site supports https encryption, but for those that do HTTPS Everywhere enhances your on-line security by making use of the encryption. It is important to note that encrypting your on-line activity does not mask your IP address, the IP addresses of the sites you visit, the amount of time you spend on a site, or the size of the files you upload or download. What HTTPS Everywhere does is protect the content of your on-line activity: the text of your e-mail, the content of the articles you read, or the specific items you order from an on-line store.

Hiding Your IP Address – While encryption may conceal the content of our on-line activity, to conceal our on-line identity we must hide our IP address. One of the most common and easiest methods of hiding an IP address is to use a proxy server. A proxy server accepts incoming requests and then forwards these requests out to the Internet. Responses are then received by the

proxy server and returned to you at your computer. Internet sites see the IP address of the proxy server and not the originating IP address of your computer.

An example of a web-based proxy server is Hide My Ass (https://hidemyass.com/). To see how a proxy server hides your IP address first go to one of the web-sites mentioned above (such as http://www.ipchicken.com/) that identify and report your IP address. Record your IP address without using the proxy server. Next go to the Hide My Ass proxy (or another proxy server of your choice), and from the proxy go to IPChicken.Com. You will see a completely different IP address. By using a proxy server your IP address is hidden on the Internet, but of course the administrator of the proxy server itself will know your actual IP address and the web-sites that you visit.

A large list of proxy servers can be found at: http://www.publicproxyservers.com/

To keep a proxy server administrator from being forced to monitor and disclose your internet connections, you may want to use a proxy server in a country other than your own. It is also possible to chain proxy servers together – go from one proxy to another proxy and then out to the Internet. While this increases the difficulty of monitoring your on-line activity, it can also slow down your Internet connections because they must be routed through additional servers.

TOR – The Onion Router (https://www.torproject.org/) – TOR is free, open source software that helps to protect your on-line privacy and personal freedom by distributing your on-line activity through a series of relays run by volunteers around the world.

In simple terms, TOR works by encrypting your Internet requests, including destination data, multiple times. Your request is sent to the first relay node in the TOR network where the first layer of encryption is removed (decrypted) and then your request is passed to a second TOR relay, where the next layer of encryption is removed, then your request is passed to a third TOR relay, or exit node where your request (i.e. view a web-page) is sent out to the Internet. Information obtained as part of your request is retrieved from the Internet and returned to you through the TOR network. Someone monitoring your computer's Internet connection will only see encrypted requests sent to the TOR network. Someone looking at the logs of a particular web-site will see no connection to your computer, only requests coming from a TOR exit node.

TOR also supports hidden services. These hidden services are sites built within the TOR network itself. Because a TOR hidden service does not require an exit node, these sites are more secure and not subject to eavesdropping in the same way as external sites may be. TOR hidden services are hosted on a server set up by the person or group offering the hidden service, and are only accessible through TOR.

JonDoNym (https://anonymous-proxy-servers.net/) – JonDoNym is a proxy client that will anonymize your online activity. JonDoNym offers both a free and paid premium version. In addition JonDoNym offers a LiveCD. According to the JonDoNym web-site: *"Jondo Live-CD/DVD offers a secure, pre-configured environment for anonymous surfing and more. It is based on Debian GNU/Linux. The live system contains proxy clients for JonDonym, Tor Onion Router and Mixmaster remailer. JonDoBrowser is pre-configured for anonymous web surfing and TorBrowser is installed too. Thunderbird for e-mails, Pidgin for anonymous instant messaging and chats, Parole media player, MAT for cleaning documents and more application are part of the live-cd. The DVD version contains additional software: LibreOffice.org, GIMP, Wuala, Calibre for eBooks and some other tools."*

I2P Anonymous Network (http://www.i2p2.de/) – I2P is an anonymizing network used to enhance communications security and protect personal privacy. I2P has been operating since 2003 and seeks to provide its users secure communications, even when operating in hostile environments.

Freenet Project (https://freenetproject.org/) – Freenet is a network intended to allow its users to share files, chat, browse the Internet, and publish information anonymously. Freenet uses encrypted nodes, and routes traffic through multiple nodes, thereby making it extremely difficult for anyone to monitor Freenet traffic or determine who has requested information or what the content of that information is.

The Amnesic Incognito Live System (TAILS) (https://tails.boum.org/) – TAILS is a Debian-based Linux distribution that attempts to safeguard your privacy and anonymity on-line. Once you boot your computer from a DVD or USB (Thumb) Drive containing the TAILS system, your connections to the Internet go through TOR, programs encrypt your files, e-mail, and chat

sessions, and downloads to your computer are restricted unless you specifically authorize those downloads.

Lightweight Portable Security (http://www.spi.dod.mil/lipose.htm) – Using a LiveCD to protect yourself on-line is recommended by the Department of Defense for its personnel accessing the Internet from outside the military networks. Lightweight Portable Security is publically available. According to their web-site:

> *"Lightweight Portable Security (LPS) creates a secure end node from trusted media on almost any Intel-based computer (PC or Mac). LPS boots a thin Linux operating system from a CD or USB flash stick without mounting a local hard drive. Administrator privileges are not required; nothing is installed. The LPS family was created to address particular use cases: LPS-Public is a safer, general-purpose solution for using web-based applications. LPS-Public allows general web browsing and connecting to remote networks. It includes a smart card-enabled Firefox browser supporting CAC and PIV cards, a PDF and text viewer, Java, and Encryption Wizard - Public. LPS-Public turns an untrusted system (such as a home computer) into a trusted network client. No trace of work activity (or malware) can be written to the local computer. Simply plug in your USB smart card reader to access CAC- and PIV-restricted US government websites."*

Private Browsing

Private browsing is a feature available in Internet Explorer, Firefox, Opera, Chrome, and Safari browsers. When browsing the Internet using a private browsing mode, your history, cookies, and temporary Internet files are not saved to your computer. Simply put, private browsing keeps your on-line activities from being stored in your browser.

- To turn on private browsing in Internet Explorer and Firefox, press CTRL+Shift+P.
- To turn on private browsing in Opera and Chrome, press CTRL+Shift+N
- In Safari choose the gear icon in the top right corner of your browser and select "Private Browsing…"

Private browsing does not anonymize your browsing session or keep your Internet Service Provider from seeing what you do on-line. But, private browsing does keep this information from being stored in browser where it could be reviewed at a later date.

Sandboxie (http://www.sandboxie.com/) – Sandboxie is a program that creates a virtual environment to protect you while you are on-line. Sandboxie helps to keep malware, cookies, viruses, browsing history, and temporary files from being stored on your computer. When these items are downloaded to your computer while on-line they are all trapped within Sandboxie and can be easily deleted when you complete you on-line activities.

Private Communications

> *Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical minority views… Anonymity is a shield from the tyranny of the majority… It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation… at the hand of an intolerant society.* (McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995))

The Court held in *McIntyre v. Ohio Elections Commission*, there is a place, and perhaps a need, for anonymous speech. However, true anonymity on the Internet can be very difficult to obtain. Computers accessing the Internet are identified by their Internet Protocol (IP) addresses. E-mail is associated with the computer used to create and send it, and individuals are often associated with a computer they use regularly. As e-mail travels across the Internet it may be intercepted, recorded, and read. E-mail may also be copied and stored on the servers and backup systems of Internet service providers. Just because both the sender and recipient of an e-mail delete their copies does not mean that it is gone. Copies of that e-mail may, and probably do, exist. In the United States once e-mail is 180 days old it is no longer a protected communication under the Electronic Communication Act, and is thereafter defined as a stored record which no longer requires a warrant in order for it to be disclosed to government agencies (see: 18 USC 2703). On-line chats (instant messaging) may also be intercepted and recorded. Chat logs with comments you made at the spur of the moment in an on-line conversation months or even years ago can come back to haunt you. Comments made in on-line forums, information on a personal web-page, or posts to social media, such as Facebook and Twitter, can all reappear long after the individual making comments and posts has assumed they are gone and forgotten.

Encrypt Your E-mail – One of the most important steps in protecting yourself in cyberspace is to encrypt your e-mail. Encryption protects the content of your e-mail from being read by anyone other than a person in possession of the correct decryption key for that message.

E-mail does get misdirected from time to time, more importantly however is the fact that e-mail may be stored on the servers and back-up files of your ISP and e-mail provider. If your e-mail is encrypted the fact that it is stored on some back-up file at your ISP is much less concerning. Even if someone looked at the messages you sent, the content of those messages couldn't be read. Encryption does not prevent someone from counting the number of e-mail messages you

send and receive, nor does it generally prevent someone determining with whom you are communication (with what e-mail addresses you are exchanging messages), but it does protect the content of those messages.

Digital Certificates – One method of encrypting e-mail across multiple systems and with multiple users is through the use of digital certificates. A digital certificate is a data file containing the necessary information for a user to sign, encrypt, and decrypt e-mail. Digital certificates can be used with most any e-mail client that supports S/MIME (Secure/Multipurpose Internet Mail Extensions); such as Outlook, Netscape, Mac Mail, Thunderbird, and Eudora. The advantage of this is that regardless of what e-mail system a person is using, it is usually possible to exchange encrypted e-mail through the use of digital certificates.

To use digital certificates to encrypt e-mail it is first necessary to obtain a personal digital certificate. Digital certificates are data files issued by certification authorities (CA). Three of the most popular and widely accepted certification authorities are: VeriSign, Comodo, and GlobalSign. To obtain a personal digital certificate simply visit one of the certification authorities' web-sites, fill out the certificate application and then download and install your digital certificate. A digital certificate may be associated with an e-mail address, or may be associated with a specific individual through the submission of identification documents to the certification authority when the digital certificate is requested. Digital certificates associated with an e-mail address may be available for free, while those associated with a specific individual through the submission of identification documents usually charge a small annual fee. For personal e-mail security, having the digital certificate associated with just an e-mail address may be sufficient, however individuals using digital signatures in a business or professional capacity may want to have their digital certificate associated to their personal identity as well. In either case the encryption is the same, and the digital certificates function in the same way.

A personal digital certificate can be obtained from:

VeriSign (https://www.symantec.com/verisign/digital-id)

Comodo (https://www.instantssl.com/ssl-certificate-products/free-email-certificate.html)

GlobalSign (https://www.globalsign.com/personalsign/)

Once you have obtained your personal digital certificate you can sign e-mail to validate that it is from you and has not been altered. By exchanging digital certificates with other people you can send encrypted messages that can only be decrypted on the computer containing your digital certificate's private key. One of the easiest methods for exchanging digital certificates is to send someone a digitally signed message and have the recipient then add your certificate to their contacts folder.

JavaScrypt: Browser-Based Cryptography Tools (http://www.fourmilab.ch/javascrypt/) – One of the simplest encryption programs available to protect your e-mail is a JavaScript implementation of the Advanced Encryption Standard (AES). This JavaScrypt encryption program uses a 256 bit key and runs entirely in your browser. JavaScrypt is a symmetric (shared key) encryption program. Both the sender and receiver of a message must have the same key that is used to encrypt and decrypt the message. An advantage of this program is that it works in any browser (i.e. Firefox, Chrome, IE). There is no need to install anything. Simply save the program to your computer and use your browser to encrypt and decrypt messages. The disadvantage to this (and all symmetric encryption) is that you must agree on a key (password) with whomever you are sending and receiving encrypted messages.

Axantum – AxCrypt (http://www.axantum.com/AxCrypt/Default.html) – AxCrypt is a free, open source file encryption program that integrates seamlessly with Windows. AxCrypt uses AES encryption with 128 bit keys. Once installed you can encrypt and decrypt files and folders with AxCrypt simply by right-clicking on the file or folder of your choice and then picking an option from the AxCrypt menu. Encrypted files and folders can be stored on your computer or easily sent as attachments through e-mail. A useful feature of AxCrypt is the ability to associate encrypted files with a key file (say on a USB drive). When associated with a key file AxCrypt encrypted files will automatically decrypt and open when the key file is present. Without the key file AxCrypt encrypted files cannot be decrypted.

Pretty Good Privacy (PGP) – PGP is an encryption program developed by Philip Zimmermann in 1991. Since its initial release PGP has become the unofficial standard for e-mail encryption and communications security on the Internet. In June 2010, PGP was acquired by the Symantec Corporation. The Symantec Corporation no longer offers a freeware version of PGP, but there are various freeware versions available from other sources. A freeware, open source version of

PGP is GNU Privacy Guard for Windows (GPG4Win) (http://www.gpg4win.org/). Like PGP, GPG4Win is an asymmetric encryption program (two key, Public Key / Private Key). When using an asymmetric encryption program you provide your public key to anyone who may want to send you an encrypted message. You can even publish your public key on the Internet. Your public key is used to encrypt messages, but cannot be used to decrypt a message. You of course keep your private key a secret. It is your private key that is used to decrypt messages.

Because PGP has existed for so long, and has become an unofficial standard, it is important to have your own PGP/GNU key pair. PGP/GNU is an excellent way to secure your on-line communications, but even if you choose to use a different method as your primary means of e-mail encryption; PGP/GNU provides a universal standard and allows anyone with your public key to send you an encrypted message.

If you use PGP you may want to publish your PGP Public Key to a PGP Key Server. By doing so, anyone who wants to send you an encrypted message can quickly obtain a copy of your public key. Some popular PGP Key Servers are:

- Keyserver at PGP.Com (https://keyserver.pgp.com/vkd/GetWelcomeScreen.event)
- MIT PGP Public Key Server (http://pgp.mit.edu/)
- PGP Public Key Server at the University of Mainz, Germany (http://pgp.uni-mainz.de/)

Hushmail (https://www.hushmail.com/) – Hushmail is a web-based e-mail service (similar to Hotmail or Gmail), offering PGP encrypted messages, file storage, and instant messaging (chat). Hushmail costs $35 - $50 per year if you wish to take advantage of all their services, but Hushmail also offers a free encrypted e-mail account, with the only limitations being that you must sign in at least one time every three weeks, and your on-line storage is capped at 25MB.

Hushmail is an excellent and very secure service. The company is located in Canada, and like every Canadian company must respond to subpoenas from a Canadian court. In 2007 Hushmail was forced to turn over account information and decryption keys of Hushmail accounts identified as being involved in on-going criminal activity. An article, "*Encrypted E-Mail Company Hushmail Spills to Feds*" detailing Hushmail's disclosures was published in Wired Magazine in November 2007. The article is worth reading in its entirety, but the following extract points out

that Hushmail was only able to decrypt account information because the account user chose to use Hushmail with reduced security in order to achieve greater convenience. The Wired Magazine article pointed out that:

> *"Hushmail uses industry-standard cryptographic and encryption protocols (OpenPGP and AES 256) to scramble the contents of messages stored on their servers. They also host the public key needed for other people using encrypted email services to send secure messages to a Hushmail account.*
>
> *The first time a Hushmail user logs on, his browser downloads a Java applet that takes care of the decryption and encryption of messages on his computer, after the user types in the right passphrase. So messages reach Hushmail's server already encrypted. The Java code also decrypts the message on the recipient's computer, so an unencrypted copy never crosses the internet or hits Hushmails servers.*
>
> *In this scenario, if a law enforcement agency demands all the e-mails sent to or from an account, Hushmail can only turn over the scrambled messages since it has no way of reversing the encryption.*
>
> *However, installing Java and loading and running the Java applet can be annoying. So in 2006, Hushmail began offering a service more akin to traditional web mail. Users connect to the service via a SSL (https://) connection and Hushmail runs the Encryption Engine on their side. Users then tell the server-side engine what the right passphrase is and all the messages in the account can then be read as they would in any other web-based email account.*
>
> *The rub of that option is that Hushmail has — even if only for a brief moment — a copy of your passphrase. As they disclose in the technical comparison of the two options, this means that an attacker with access to Hushmail's servers can get at the passphrase and thus all of the messages."* (Singel 2007)

Hushmail used to its full capability is extremely secure, and even using the reduced security mode where the encryption engine is run on the Hushmail servers, one still obtains good security. But it's important to remember that no security is perfect, nor is security provided by companies like Hushmail intended to allow criminals to escape law enforcement. In response to a subpoena from a Canadian court Hushmail decrypted and disclosed information from three accounts being used by Chinese steroid chemical providers underground laboratories engaged in international drug trafficking. Remember, security is best maintained by not becoming involved in criminal activity and thus not becoming the target of a law enforcement investigation.

Anonymous E-mail

Sometimes you may not wish to protect the content of your e-mail, rather you may want to make a public comment without disclosing your identity. There are several reasons that a person might want to do this. Perhaps you are a whistleblower and want to report illegal or unethical activity, but fear retaliation. Maybe you want to comment publically on a commercial product (either positively or negatively) without appearing to give an official endorsement based on your position or employment. Maybe you want to make a political comment (support or oppose a particular position) without entering into an on-going debate with friends or co-workers. Or… maybe you just want to participate in on-line forums and list servers while maintaining your personal privacy.

While perfect anonymity is unlikely, there are several sites on the Internet that allow an individual to send a pseudo-anonymous e-mail. A few examples of sites providing anonymous e-mail services included: AnonyMouse (http://anonymouse.org/), Anonymous Speech (http://www.anonymousspeech.com/), Silent Sender (https://www.silentsender.com/), and TorMail (http://tormail.org/) – Tormail can only be accessed through TOR. These web-sites allow the user to send an e-mail which has the header information and from address removed. These anonymous e-mail sites are useful when it is necessary to send a brief message without having it traced back to the sender. Although these services may allow a recipient of the e-mail to reply to the sender, these services are not really intended for an on-going exchange of e-mails.

Sites like **RiseUp.Net** (https://riseup.net/en) provide increased anonymity and security for activists and individuals involved in social protest movements. The RiseUp web-page says: *"Riseup provides online communication tools for people and groups working on liberatory social change. We are a project to create democratic alternatives and practice self-determination by controlling our own secure means of communications."* While RiseUp and similar services do help to protect one's on-line communications, it can be very difficult to obtain a RiseUp account, unless one is actively involved in the activities conducted and supported by RiseUp and can obtain "invite codes" from current RiseUp members. Furthermore, while RiseUp users' accounts may be protected by RiseUp policy and social contract, the administrators of the RiseUp network can still access the account information of their users.

A common way of hiding your true identity on-line is to set-up a web-based e-mail (i.e. Hotmail, Gmail, Yahoo mail) under a fake name and profile. While this will associate your fake name with this e-mail address, if you access the account from home then your IP address will be associated with your e-mail fake name and profile. If you want to make an anonymous web-based e-mail you must set it up through a proxy (preferably TOR), and you must never access the account from any computer that can be connected to you without going through TOR or a proxy server when you do so.

Bitmessage (https://bitmessage.org/wiki/Main_Page) – Bitmessage is a P2P communications protocol based on the Bitcoin encryption methodology. Bitmessage can be used to send a message to a single individual or to publish messages to a group of subscribers. Based on the encryption methodology used by Bitmessage, each message requires a proof of work and takes around four minutes to send. Depending on your computing power, long messages could take a considerable amount of time to send. Bitmessage protects the identity of both the sender and receiver of a message.

Self-Destructing Messages

Self-destructing messages are messages that can be read once, and which after being opened automatically delete themselves from the server on which they have been stored. Self-destructing messages also attempt to keep the recipient of the message from saving it or forwarding it to another person.

Privnote (https://privnote.com/) is a message encryption service provided by the technology company Insophia, located in Montevideo, Uruguay. Privnote works by encrypting a message created on the Privnote web-site, storing that encrypted message on the Privnote servers, and providing a link to view that message. An example of a link to a message on the Privnote server looks like this: https://privnote.com/n/mewehlwavzmvhpeq/#tfhduyzlckqeokqf. A person simply follows this link to view the message. Once the message has been opened (someone has clicked on the link) the message is deleted from the Privnote servers. Thus a person gets to read a message sent through Privnote one time before it is deleted. If there is a need to keep the information sent through Privnote, the recipient can copy and paste the text of the message to another document, or make a screenshot of the decrypted Privnote message. Messages left unread on the Privnote servers are automatically deleted after 30 days.

OneShar (https://oneshar.es/) – A system much like Privnote is Oneshar. Oneshar allows a user to create a message of up to 1000 characters in length, then encrypts the message and provides the user with a link to access the message. Oneshar also allows the creator of the message to set a time of 30 minutes, 1 hour, 2 hours, 4 hours, 8 hours, or 1, 2, or 3 days before the message is deleted from the Oneshar servers.

NoteDIP (http://notedip.com/) is another service for sending self-destructing messages. NoteDIP allows one to specify a password in order to access NoteDIP link containing the message. NoteDIP also allows for the sender to include an e-mail address to receive notification when a message has been read.

Destructing Message (http://www.destructingmessage.com/) creates a link to a created message and includes a self-destruct time that begins a countdown when the message is opened. The time until the message self-destructs after being opened can be set for 15, 30, or 45 seconds, or 1, 2, or 5 minutes. After the timer reaches zero the message is destroyed.

TMWSD "This Message Will Self Destruct" (https://www.thismessagewillselfdestruct.com/) Like other self-destructing message services, TMWSD creates a link to the message you have created. TMWSD allows for a password requirement to access the message, and also allows one to create multiple links to the same message (each of which allows the message to be read just one time).

Burn Note (https://burnnote.com/) operates from the web and from both iOS and Android mobile apps. When a Burn Note message is opened by the recipient a sender-set count-down from 1 to 120 seconds starts, and upon reaching zero the message is deleted. Burn Note messages allow setting of a password to open the message as well. A unique feature of Burn Note is the spotlight feature that displays only part of the message at a time (the part under the spotlight) thus resisting copy and paste and screen shots of the entire message.

Temporary E-mail Addresses

Sometimes you may need an e-mail address that is valid for a few minutes or maybe a few days. A temporary e-mail address can be useful when requesting information on-line, or when signing up for access to an on-line service. You may not want to have your personal e-mail address flooded with advertising (SPAM) just because you inquire about a product. Maybe you want to inquire about a personal or sensitive topic without having that inquiry associated with your name or private e-mail.

YOPmail (http://www.yopmail.com/en/) allows you to create an anonymous, disposable e-mail address that lasts for eight days. YOPmail addresses are not password protected, thus anyone knowing a YOPmail e-mail address can check the inbox. To counter this, YOPmail creates an alias for each e-mail address. E-mail sent to a YOPmail alias is forwarded to the associated YOPmail e-mail address. Thus anyone checking the alias inbox always sees an empty inbox. To prevent YOPmail from being used to send SPAM or for other types of criminal activity, you cannot send e-mail from a YOPmail address. The exception to this is that you can send e-mail from one YOPmail address to another YOPmail address. This allows YOPmail to be used for short-term private / anonymous communication.

Incognito Mail (http://www.incognitomail.com/) – With Incognito Mail you can create an e-mail address that lasts for just 60 minutes. This gives you time to receive and respond to on-line registration requests, while safeguarding your personal e-mail address. To use Incognito Mail create or generate a random Incognito Mail address and then reload the web-page to check for incoming e-mail. Incognito Mail doesn't allow you to send original e-mail, but you can reply to e-mail received in your inbox as long as the e-mail address is active.

Guerrilla Mail (https://www.guerrillamail.com/) – Guerrilla Mail works on the public inbox concept, where anyone who knows the e-mail address can check mail in the inbox. It also allows the establishment of an alias which will forward e-mail sent to the alias to the associated Guerrilla Mail inbox, thereby leaving the alias inbox empty. Guerrilla Mail deletes the content of an inbox after an hour, whether the message has been read or not. Guerrilla Mail also lets a user compose and send original e-mail. Attachments (up to 150MB) may be included with a sent e-mail.

Steganography

Steganography is a word from the Greek, meaning hidden writing. Steganography programs let you, for example, hide a message in a picture. With a good steganography program there will be little if any difference between the appearance of a picture with a hidden message and one without a hidden message. The advantage of steganography is that it does not appear that you are sending a message, or at least the message you send openly can be completely different than the message you have hidden using steganography.

Some steganography programs encrypt messages before hiding them, while other steganography just conceal the plaintext message. For best security messages should always be encrypted before being hidden using steganography. If the steganography program that you use does not encrypt messages, just encrypt your message first using an encryption program and then hide the encrypted message using a steganography program.

Some steganography programs are:

OpenPuff (http://embeddedsw.net/OpenPuff_Steganography_Home.html)

QuickStego (http://quickcrypto.com/free-steganography-software.html)

SilentEye (http://www.silenteye.org/index.html)

Spam Mimic (http://www.spammimic.com/index.shtml) – Short messages can be concealed in what appears a spam message. This on-line program is limited to very short messages, but there are still many interesting uses for this service.

Secure Your On-Line Chats

Chat is real-time communication between two or more people on-line. Chat clients include AIM, Facebook Chat, Google Talk, ICQ, MSN, Yahoo, and many others.

Pidgin (http://www.pidgin.im/) - Pidgin is a universal chat program that brings all your chat clients together in one place. By using the "Off The Record" (OTR) (http://www.cypherpunks.ca/otr/) plugin with Pidgin you are able to encrypt all your chats with anyone else using Pidgin and OTR. Other encryption plugins for Pidgin include Pidgin-Paranoia (http://pidgin-paranoia.sourceforge.net/) which uses one-time-pads to encrypt chat sessions, and Pidgin-Encryption (http://pidgin-encrypt.sourceforge.net/) which encrypts conversations using stored RSA keys.

Cryptocat (https://crypto.cat/) – Cryptocat is a browser extension for Firefox, Chrome, Safari, and OS-X. It is not currently available for Internet Explorer. Cryptocat provides an encrypted connection for your chat sessions. Cryptocat is extremely simple to use. Simply open Cryptocat in your browser, enter a "conversation name" a nickname to use in the chat, and click on connect. Cryptocat establishes an encrypted connection and opens a chat room using the conversation name you chose for this session. Anyone can enter the chat room by entering the same conversation name into Cryptocat. After everyone has exited the chat room all records of the chat are deleted.

ChatCrypt (http://www.chatcrypt.com/) – ChatCrypt is a web-based chat service that uses a JavaScript implementation of AES-256 to encrypt messages before they are sent to the chat room. To use ChatCrypt everyone participating in the chat must share a common password (exchanged beforehand by secure means). From the ChatCrypt web-site enter a chat room name, username, and a shared password. Anyone knowing the chat room name can enter the room, but without knowing the correct password will only see usernames and encrypted text. A WHOIS search shows that the chatcrypt.com domain is registered in Makkoshotyka, Hungary.

Cell-Phone / Mobile Device Security

We rely on our cell-phones, smartphones, and mobile devices for an ever increasing number of options. Of course we make telephone calls, and send text messages, but we also rely on these devices to store data such as our contacts list and address book, photos, calendar, and schedules. In many cases we use our smartphones to surf the Internet, shop on-line, and conduct other transactions such as banking. It is best to think of our smartphones as small computers that can make telephone calls, rather than phones that can access the Internet. Other mobile devices such as iPads and tablets are just larger, more powerful versions of your smartphone.

Cell-phones work by communicating with cell-sites / cell-towers using a radio signal. These are low power radio signals, with relatively short range, so cell-sites must be located fairly close to a cell-phone user. If you get beyond the radio range of your cell-phone (out of range of the cell-site) you will get a no signal / no service message. The short range of the cell-phone signal means that the physical location of a cell-phone can be associated with a single cell-site, or a more precise location can be triangulated when the cell-phone is in range of more than one cell-site.

Virtual Private Network (VPN) – An important step is securing your mobile devices is to install and use a VPN. A VPN creates a secure tunnel between your mobile device and the Internet gateway that you access through your service provider. The VPN encrypts your communications and helps mask your location. One example of a VPN is Hotspot Shield (www.hotspotshield.com/) which offers both a free trial version, and an annual subscription for just a few dollars per year. A VPN is important on mobile devices because we access the Internet from many different places during the day (coffee shops, airports, work sites, and other public locations). The VPN shields the Internet connections that you make from your mobile device, but it doesn't shield your cellular connections (your cell-phone provider will still have a record of the phone calls you make).

Find My Phone App – An important item to have on your smartphone and mobile devices is an application that will allow you to locate your phone if it is lost or stolen. Additionally these applications will also let you delete all the data on your phone if it is lost or stolen and cannot be found. Searching for "*Find My Phone*" in either the iTunes or Google Play store will provide you

with access to this application. Once you have Find My Phone installed you will be able to locate your mobile devices based on their GPS location, displayed on a web-page or on another mobile device, play a sound on a misplaced device to help you locate it, and delete all data on your device if you are unable to locate it or believe it has been stolen.

Wickr App (https://www.mywickr.com/en/index.php) – The Wickr App encrypts your text messages, and also lets you set a time after which the messages will expire and be deleted. Wickr also integrates with Box (https://www.box.com/), Drop Box (https://www.dropbox.com/), and Google Drive (https://drive.google.com/). Wickr is a free application.

SeeCrypt (https://www.seecrypt.com/) – SeeCrypt is an application that lets you make secure voice calls and send encrypted text messages. New SeeCrypt users get the first three months of usage for free, and thereafter pay just three dollars for month unlimited secure communications.

Secret Massage (http://www.secretmessageapp.com/) – The Secret Message App allows you to send encrypted text messages to someone with whom you share a common password. Secret Message is a free application that is useful for securing the content of text messages you send to and receive from friends and family. Because Secret Message requires a shared password/key you will have to agree on this before you are able to exchange secure text messages with someone.

Regardless of which secure communications application you choose, everyone with whom you wish to communicate securely must have the same application installed. When choosing a secure communications application it is important to choose one that is compatible across multiple operating systems (i.e. works on IPhone, Android, Windows, and Blackberry phones). Encourage your friends, family, co-workers, and anyone else with whom you communicate on a regular basis to download and use a secure communications application. If different applications have specific features that you like (or that someone you communicate with likes) you can always download and use more than one application. Multiple secure communications applications are not particularly difficult to use, but the easiest option is for everyone to have and use a common application.

Making Private Telephone Calls

In some cases you may wish to make a call without having your telephone number displayed on caller ID. In North America you can prevent caller ID from displaying your number by dialing *67 before dialing the number you wish to call. This does not work when calling toll-free numbers (i.e. 800 numbers) or when calling pay-per-call numbers (i.e. 900 numbers). Additionally telephone subscribers can elect not to accept private or blocked calls to their number (anonymous call rejection). The number you called will still appear in your call records maintained by the telephone company, so *67 doesn't provide any real privacy, but it is a simple and free method of preventing your telephone number from being displayed in caller ID in some cases.

While *67 will hide your phone number from caller ID, greater anonymity can be obtained by using a prepaid cell-phone service. There are several prepaid cell-phone companies, such as Go Phone (http://www.att.com/shop/wireless/gophone.htm), Tracfone (https://www.tracfone.com/), Net10 (http://www.net10wireless.com) and many others. If you purchase a prepaid cell-phone with cash, and add air time by purchasing an air time card with cash as well, you have cell-phone that is not associated with your name.

Burner Phone (https://www.burnerphone.us/) – Burner phone is a prepaid cell-phone designed to be purchased, used for 30 days, and then thrown away. For a flat fee ($75 when this was written) you receive a cell-phone with power cord, and 30 days of unlimited nationwide talk and text. Use time begins when you first turn the phone on, and after 30 days your account deactivates. You can then destroy or recycle the physical phone. The Burner Phone Company claims that after they process and ship your order they destroy the sale/transaction record thus making it impossible for anyone to obtain your personal information from the company.

Burner App (http://burnerapp.com/) – The Burner application is used on your personal cell-phone to provide you with disposable telephone numbers for voice and text messages. With Burner App you use your regular cell-phone/smartphone and with the installed Burner App add additional, disposable numbers to your phone. When you no longer need the temporary number you burn (delete) it and it is removed from your phone.

Vumber (http://www.vumber.com/) – Vumber is service which allows you to associate additional telephone numbers with your cell-phone, home phone, or other phone you own. You can both make and receive calls through your Vumber telephone number. According to the Vumber web-site: *"When someone calls: You can a) answer; b) send them to Vumber Mail; c) give them a busy signal; d) tell them the number is out of service; or e) play a custom message you create. You can call from your Vumber, too. Simply dial your Vumber and then dial the number. It's that easy. Vumber gives you a virtual phone number in minutes, which lets you protect your private phone number."*

Information Assurance Training

To operate safely in cyberspace it is important to be aware of current threats and effective countermeasures. Free on-line cyber-security awareness training is available from a number of government agencies. Some courses are designed to enhance public awareness, while other are focused on specific government agencies, but made available to members of the general public as well. Training courses are available on-line from the Department of Defense and from the Department of Homeland Security.

DoD Information Assurance Support Environment (IASE) On-line Training – The Department of Defense Information Assurance Support Environment (IASE) (http://iase.disa.mil/eta/) offers training to support military and government personnel. Many of the IASE courses can be completed on-line and are available to the general public. In 2013 the

IASE courses available to the general public, by way of example, included:

- CyberAwareness Challenge
- Smartphones and Tablets
- Social Networking
- Phishing
- Personally Identifiable Information

and a series of Information Assurance Awareness Short Courses, that included:

- Telework
- Insider Threat
- Wireless
- Passwords
- Peer-to-Peer
- Social Engineering

In addition to the information assurance awareness courses listed above, the IASE offered a series of more technical courses on-line, which included:

- Computer Network Defense
- Enhancing Information Assurance through Physical Security
- Domain Name System Basic Concepts Overview
- Introduction to IDS Analysis
- DoD Intrusion Detection System (IDS) Analysis Part 2
- IDS Analysis Part 3, CND Analysis: A Structured Approach to Intrusion Analysis
- System Administrator Incident Preparation & Response

DHS / FEMA Cyber-Security Training – The Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) in conjunction with Texas A&M Engineering Extension Service (TEEX) offered a series of free, on-line cyber-security courses. According to their web-site (http://www.teex.com/teex.cfm?area=NERRTC&templateid=1856):

> The Cyber Security online courses are designed to ensure that the privacy, reliability, and integrity of the information systems that power our global economy remain intact and secure. These DHS/FEMA-certified courses are offered through three discipline-specific tracks targeting general, non-technical computer users, technical IT professionals, and business managers and professionals.

The courses offered were:

Non-Technical / General User

- AWR-175-W Information Security for Everyone
- AWR-174-W Cyber Ethics
- AWR-168-W Cyber Law and White Collar Crime

Technical / IT Professional

- AWR-173-W Information Security Basics
- AWR-178-W Secure Software and Network Assurance
- AWR-138-W Network Assurance
- AWR-139-W Digital Forensics Basics

Managers and Business Professionals

- AWR-176-W Business Information Continuity
- AWR-177-W Information Risk Management
- AWR-169-W Cyber Incident Analysis and Report

InfraGard Awareness Security Awareness Course (https://www.infragardawareness.com/)
The InfraGard course is designed to improve security awareness of employees at small businesses, as well as helping individuals learn to protect themselves and their families from cyber-crime and identity theft.

Conclusions

Having read this guide and adopted some of the suggestions offered herein you will have improved your personal security in cyberspace. Access to your digital devices is now protected by strong passwords and encryption. Your stored data is encrypted, as are your e-mail and chat sessions, text messages, and phone calls. You can send anonymous messages allowing you to express an opinion or report wrong-doing without fear of retaliation. You can securely delete data from your digital devices so that it cannot be recovered, and if a device is lost or stolen you can locate it, or failing that remotely wipe all data on the device to prevent it from being used by the thief.

You may have taken advantage of free on-line computer security awareness training. This training is designed to make you safer in cyberspace, and is recommended for anyone that spends time on-line, uses social media, or uses computers at work.

Finally remember that this guide is intended to help the average person become more secure in cyberspace. A number of free and low-cost resources have been presented that can be used to improve your security and protect your privacy, but not every resource may listed is right for all situations. You should look at the various resources presented, and use those that best meet your personal needs.

References

ACLU. (2013). Cell Phone Location Tracking Public records Request. March 25, 2013. https://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request

Cellular Telecommunications Industry Association (CTIA). (2013). *50 Wireless Quick Facts*. http://www.ctia.org/advocacy/research/index.cfm/aid/10323

Clifford, Stephanie and Quentin Hardy. (2013). Attention, Shoppers: Store Is Tracking Your Cell. *The New York Times.* July 14, 2013. http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html

Crump, Catherine. (2013). *Federal Appeals Court Rules the Government Can Track Your Cell Phone Without a Warrant.* ACLU. July 30, 2013. https://www.aclu.org/blog/technology-and-liberty/federal-appeals-court-rules-government-can-track-your-cell-phone-without

Department of Homeland Security. (2013). *Civil Rights/Civil Liberties Impact Assessment: Border Searches of Electronic Devices.* http://www.dhs.gov/sites/default/files/publications/crcl-border-search-impact-assessment_01-29-13_1.pdf

Department of Homeland Security. (2013a). *Combat cyber-crime.* http://www.dhs.gov/combat-cyber-crime

FBI. (2013). *Safety and Security for the Business Professional Traveling Abroad.* http://www.fbi.gov/about-us/investigate/counterintelligence/business-brochure

Fisher, Max. (2012). "Here's the e-mail trick Petraeus and Broadwell used to communicate." The *Washington Post*. November 12, 2012. http://www.washingtonpost.com/blogs/worldviews/wp/2012/11/12/heres-the-e-mail-trick-petraeus-and-broadwell-used-to-communicate/

Internet World Stats. (2012). http://www.internetworldstats.com/stats.htm

Martinez, Michael. (2013). *California school district hires firm to monitor students' social media*. CNN. September 14, 2013. http://www.cnn.com/2013/09/14/us/california-schools-monitor-social-media/index.html

National Counterintelligence Executive. (2011). *Foreign Spies Stealing US Economic Secrets in Cyberspace.* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

New York State Office for the Prevention of Domestic Violence. (2010). *The Use of Technology in Stalking.* http://opdv.ny.gov/public_awareness/bulletins/winter2010/winter2010_bulletin.pdf

Nixon, Ron. (2013). "Postal Service Confirms Photographing All U.S. Mail". *The New York Times*. August 2, 2013. http://www.nytimes.com/2013/08/03/us/postal-service-confirms-photographing-all-us-mail.html

Pawloski, Jeremy. (2013). Documents link Army to man accused of spying on anti-war protesters. *The Olympian Newspaper*. August 20, 2013. http://www.theolympian.com/2013/08/20/2681787/documents-link-army-to-man-accused.html

Ponemon Institute. (2012). *The impact of cybercrime on business.* Check Point Software Technologies. http://www.checkpoint.com/products/downloads/whitepapers/ponemon-cybercrime-2012.pdf

Savage, Charlie and Leslie Kaufman. (2013). Phone Records of Journalists Seized by U.S. *The New York Times*. May 13, 2013. http://www.nytimes.com/2013/05/14/us/phone-records-of-journalists-of-the-associated-press-seized-by-us.html

Sherman, Mark. (2013). *Gov't obtains wide AP phone records in probe.* http://bigstory.ap.org/article/govt-obtains-wide-ap-phone-records-probe

Singel, Ryan. (2007). Encrypted E-Mail Company Hushmail Spills to Feds. *Wired Magazine.* Novemver 7, 2007. http://www.wired.com/threatlevel/2007/11/encrypted-e-mai/

Copyright Notice

Digital Defense: A Guide to Personal Security in Cyberspace

Copyright: Michael Chesbro

Published: October 1, 2013

Publisher: Michael Chesbro

Finis

Digital Defense