INDIVIDUAL OPSEC & PERSONAL SECURITY

Includes: Information Security (INFOSEC) and Operations Security (OPSEC) for Government Employees

Michael Chesbro

How to Use This Guide

This document is intended to be a guide or index of information and resources that you can use to make your life a little bit more secure. As you read the information provided here you may find things that are directly applicable to your life and that you will want to implement immediately. Other things we will discuss here will be, perhaps, less applicable to you, but may be very useful to someone else.

Use what you find to be useful, and skip that which seem less valuable to you. Don't feel that you have to do everything listed here to add security to your life, or that you somehow create a vulnerability in your life if there is a security recommendation that you choose not to implement. Each person's life is different, and we all have different security needs that may change over time. Security isn't about the number of security measures that you implement, rather it is about understanding the threats that you face in your life, and determining what countermeasures you will implement against those threats.

Throughout this guide I have provided direct links to information and resources on the Internet. Use these links to gather more information and to implement OPSEC and personal security techniques that are applicable in your life.

On the day I published this guide, all of the links worked and returned the information referenced. However, the Internet is constantly changing, and links that are good today may be broken tomorrow. If a link appears to be broken when you click on it in this document, try copying and pasting it into your browser. If that does not take you to the information you are seeking, try searching for the topic with your favorite search engine. The information may still be available at a new link. Of course, sometimes information and resources are removed from on-line access or are no longer supported; so, if you see something that you like, save a copy of it to your computer so that you will have access to it in the future.

Finally, share the information in this guide with others, your friends, family, and co-workers. Like immunizations, the more people around you who are immune to a disease, the less likely you are to catch that disease. Similarly, the more people around you who have defenses against a security threat, the less likely you are to become susceptible to that threat because of something someone else did, such as a data breach, or e-mail compromise. When more people in your life regularly practice individual OPSEC and implement personal security in their own lives, there is a cumulative effect increasing the overall security of everyone in the group.

Understanding the Threat

There is no single solution for keeping yourself safe in cyberspace or in the physical world. Individual OPSEC and Personal Security isn't about which tools you use; rather, it's about understanding the threats you face and how you can counter those threats. To become more secure, you must determine what you need to protect, and from whom you need to protect it. Threats can change depending on where you're located, what you're doing, and with whom you're working. Therefore, in order to determine what solutions will be best for you, you should conduct a threat assessment of your personal life.

When conducting this threat assessment, there are five main questions that you should ask yourself:

1. What do you want to protect?

2. Who do you want to protect it from?

3. How likely is it that you will need to protect it?

4. How bad are the consequences if you fail?

5. How much trouble are you willing to go through in order to try to prevent those consequences? (Electronic Frontier Foundation, 2015)

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 even 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, nor do they have unlimited capabilities. It is quite 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 security plan, the weaknesses and exploitable vulnerabilities in one security measure may be covered by the strengths of another.

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 applications that we discuss here, choose the ones that you can and will employ on a regular basis. Good security employed consistently is better than great security employed occasionally.

What Is OPSEC (Operations Security)?

Operations Security, or OPSEC, is the process by which we protect unclassified information that can be used against us. OPSEC challenges us to look at ourselves through the eyes of an adversary (individuals, groups, countries, organizations). Essentially, anyone who can harm people, resources, or mission is an adversary.

OPSEC should be used to protect information, and thereby deny the adversary the ability to act. Nearly 90% of the information collected comes from "Open Sources". Any information that can be obtained freely, without breaking the law, is Open Source. It is social network sites, tweets, text messages, blogs, videos, photos, GPS mapping, newsletters, magazine or newspaper articles, your college thesis, or anything else that is publicly available.

Our OPSEC objective is to ensure a safe and secure environment. OPSEC is best employed daily when making choices about what communications to use, what is written in emails or said on the phone, postings on social networking sites and blogs. Any information you put in the public domain is also available to your adversaries.

The bottom line is that we can be our own worst enemy.

http://www.dodea.edu/offices/safety/opsec.cfm

What is Personal Security?

Personal security is a general condition that results after adequate steps are taken to (a) deter, (b) delay, and (c) provide warning before possible crime, (d) if such warnings occur, to summon assistance, and (e) prepare for the possibility of crime in a constructive manner. Reasonable efforts to execute these five tasks can greatly reduce security risks, sometimes to negligible levels. Security efforts will of course differ, based on the circumstances of each individual. Work or school responsibilities, area of residence, family activities, and other factors influence security needs. Some people may need to upgrade the security of homes; others of their children; yet others of their travel, computing, and so forth. Each person should consider selectively implementing the options most pertinent to their own needs.

http://www.dodea.edu/Offices/Safety/upload/pfpa_PersonalSecurity.pdf

Register Your Home and Cellular Telephones with the National Do Not Call Registry https://www.donotcall.gov

The National Do Not Call Registry gives you a choice about whether to receive telemarketing calls at home. Telemarketers should not call your number once it has been on the registry for 31 days. If you receive telemarketing calls after you have been listed in the registry for 31 days, you can file a complaint with the Federal Trade Commission. It is also important to note that legitimate telemarketing companies screen their call lists against the National Do Not Registry so any call you receive after registering your number is almost certainly a scam, attempt at identity theft, or some other type of criminal activity. Legitimate telemarketing companies don't call numbers listed in the National Do Not Call Registry.

Sign up for Nomorobo

https://www.nomorobo.com/

Nomorobo blocks robo calls. Robo calls are used by many organizations to solicit for their cause. Nomorobo is a free (for landlines) service that can help block these robo calls. Although Nomorobo isn't supported by every telephone service provider, if yours does it's worth considering Nomorobo as one of your personal privacy enhancing options.

Use Alternate and Burner Numbers to Safeguard Your Private Telephone Numbers

One of the most popular alternate telephone numbers is Google Voice, which lets you have one telephone number that rings on multiple devices (i.e. home, work, mobile). Other services, some of which are listed below, let you set up temporary telephone numbers that you can delete at any time. By using one or more of these services you can protect the privacy of your personal telephone numbers while still having a telephone number that you can provide to others when needed.

Google Voice - https://voice.google.com/

Burner - https://www.burnerapp.com/

CoverMe - http://www.coverme.ws/en/index.html

Hushed - https://hushed.com/

Sideline - https://www.sideline.com/

Vumber - https://www.vumber.com/

In their book, "*The Complete Privacy & Security Desk Reference: Volume I: Digital*" - https://goo.gl/phtVCd - the authors Michael Bazzell and Justin Carroll point out that having just a single cellular telephone number that you use for all of your voice communications is very inappropriate behavior if privacy is desired.

Opt-Out of Prescreened Credit and Insurance Offers

Many companies that solicit new credit card accounts and insurance policies use prescreening to identify potential customers for the products they offer. Prescreened offers - sometimes called "preapproved" offers - are based on information in your credit report that indicates you meet criteria set by the offeror. Usually, prescreened solicitations come via mail, but you also may get them in a phone call or in an email. If you decide that you don't want to receive prescreened offers of credit and insurance, you have two choices: You can opt out of receiving them for five years or opt out of receiving them permanently.

To opt out for five years: Call toll-free 1-888-5-OPT-OUT (1-888-567-8688) or visit https://www.optoutprescreen.com. The phone number and website are operated by the major consumer reporting companies.

To opt out permanently: You may begin the permanent Opt-Out process online, but to complete your request, you must return the signed Permanent Opt-Out Election form, which will be provided after you initiate your online request.

Opt-Out of Direct Marketing

Reducing the amount of junk mail (unwanted coupons, catalogs, etc.) delivered to your mailbox can be accomplished by signing up for mail preference services with Catalog Choice https://www.catalogchoice.org/ and with the Direct Marketing Association https://www.dmachoice.org/. By registering with these organizations your address will be added to the delete list used by advertisers to scrub their mailing lists.

The National Do Not Mail List - http://www.directmail.com/mail_preference/ - is run by DirectMail.Com, a private marketing firm. It is in the best interest of direct marketers not to send advertising to people who are unlikely to respond to it. When you sign up with the National Do Not Mail List, your name and address will be provided to direct mail marketers so that it can be removed from their mailing lists.

You can opt-out of having the Yellow Pages Telephone Directory delivered to your home by registering at https://www.yellowpagesoptout.com/.

Other on-line sources to opt-out of direct marketing include:

AARP - http://www.aarp.org/about-aarp/aarp-privacy-policy-opt-out1/

Acxiom - https://isapps.acxiom.com/optout/optout.aspx

American Cancer Society - https://www.cancer.org/about-us/policies/opt-out-form.html

Century Link - http://www.centurylink.com/help/privacy/optout_en.html

Comcast / Xfinity - http://customer.xfinity.com/help-and-support/account/do-not-call-do-not-mail-registry-requests

Epsilon - https://us.epsilon.com/consumer-information#Display

GEICO Marketing - https://www.geico.com/about/contactus/email/ (Select "Opt out of GEICO marketing communications" from the drop down menu.)

LexisNexis Direct Marketing Services - http://www.lexisnexis.com/privacy/directmarketingopt-out.aspx

Red Plum - https://www.redplum.com/tools/redplum-postal-addremove.html

SiriusXM E-mail Communications - https://pc2.mypreferences.com/SiriusXM/Customer/StandaloneUnsubscribe

State Farm - http://online2.statefarm.com/forms/sf/doNotSolicitRequest.xhtml

ValPak - https://www.valpak.com/coupons/show/mailinglistsuppression

Legitimate businesses will honor your opt-out requests. These businesses understand that not everyone wants to receive direct marketing and targeted offers for products and services; and that individuals who don't want to receive this type of advertising are unlikely to respond to it by making a purchase.

It is important to understand that there is also a disadvantage to opting out of direct and targeted marketing, and that disadvantage is that you will not receive offers for products and services that might not be generally available in the retail market. When you opt-out you are opting out of offers from legitimate businesses, some of which you might be interested in receiving.

Opting out of direct and targeted marketing is a choice each of us should make based on our own personal circumstances and preferences. We must each weight the value of our personal privacy and security against the convenience and advantage of receiving targeted advertising based on our shopping habits and interests identified in personal profiles built by marketing companies.

Remove Your Name from On-Line Directories and People Finders

On-line directories and people finders gather data from public records and other sources and then make the aggregation of that data available on-line. You can have your personal information removed from these directories by following the opt-out procedures provided by these companies. It is important to note that removing yourself from these directories does not remove your information from the original source where it was gathered. However, removing your personal information from these directories does help protect your privacy when someone is conducting on-line searches in an attempt to locate you. There are dozens of companies aggregating personal information from public records. Below are some of the most well-known of these companies and links to their opt-out pages.

AnyWho - http://www.anywho.com/help/privacy

Been Verified - https://www.beenverified.com/faq/opt-out/

Family Tree Now - http://www.familytreenow.com/optout

Intelius - https://www.intelius.com/optout.php

Instant Checkmate - https://www.instantcheckmate.com/optout/

LexisNexis - http://www.lexisnexis.com/privacy/

PeekYou - http://www.peekyou.com/about/contact/optout/

People Finder - http://www.peoplefinder.com/optout.php

People Smart - https://www.peoplesmart.com/optout-go

Phone Detective - https://www.phonedetective.com/PD.aspx?_act=OptOutPolicy

Pipl - https://pipl.com/help/remove/

Private Eye - https://secure.privateeye.com/optout-form.pdf

Spokeo - http://www.spokeo.com/opt_out/new

US Search - http://www.ussearch.com/privacylock

USA People Search - http://www.usa-people-search.com/manage/

Veromi - http://www.veromi.net/Help#26

White Pages - https://support.whitepages.com/hc/en-us/articles/203263794-Remove-my-listing-from-Whitepages-

ZabaSearch - http://www.zabasearch.com/block_records/

Review a Copy of Your Credit Report

AnnualCreditReport.com is the official site to get your free annual credit reports. This right is guaranteed by Federal law.

Federal law allows you to:

- Get a free copy of your credit report every 12 months from each credit reporting agency.
- Ensure that the information on all of your credit reports is correct and up to date.

Visit https://www.annualcreditreport.com/ to get a free copy of your credit report.

Add A Credit Freeze to Your Credit File If You Believe You Are at Risk

A credit freeze (sometimes called a security freeze) is designed to prevent the information in your credit file from being reported to others. Because most creditors will check your credit report before opening a new account a credit freeze is an effective means of protecting yourself against identity thieves who open accounts in your name.

There are some inconveniences associated with having a credit freeze / security freeze on your credit file when you try to establish new credit yourself, but for some people the additional protection provided by a credit freeze may be worth the associated inconvenience.

The Federal Trade Commission provides more information on credit freezes here:

http://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes

If you choose to place a credit freeze on your credit file, you will have to contact each of the major credit reporting agencies to complete the process.

Experian - http://www.experian.com/consumer/security_freeze.html

Equifax - https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

TransUnion - http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page

Experian 1-888-397-3742 | Equifax 1-800-525-6285 | TransUnion 1-800-680-7289

Request a Copy of Your Security Clearance Adjudicative & FBI Records

If you served in the military, or otherwise worked with the Department of Defense, the government conducted a background check on you. Adjudicative records for the DSS Investigative Records Repository (IRR), Defense Central Index of Investigations (DCII), Secure Web Fingerprint Transmission (SWFT), or JPAS are all available through a Freedom of

Information Act/Privacy Act request to the Defense Manpower and Data Center Office of Privacy. Simply mail a request to:

Defense Manpower Data Center,
ATTN: Privacy Act Branch
P.O. Box 168
Boyers, PA 16020-0168

FBI Investigative Records can be requested on-line at

https://www.fbi.gov/services/records-management/foipa/requesting-fbi-records More information about requesting your FBI Identity History Summary Check can be found at https://www.fbi.gov/services/cjis/identity-history-summary-checks

Request a Copy of Your State Criminal History and Police Records

Public records / privacy act laws in each state allow you to obtain a copy of criminal history / police records maintained about you (i.e. you can obtain a copy of your own records). Request a copy of records from your state by contacting the Identification Bureau in your state. Contact information for each state can be found at https://www.fbi.gov/services/cjis/identity-history-summary-checks/state-identification-bureau-listing In addition to any criminal history, you should request information on any time your name has been run in a criminal justice information systems database (such as NCIC) by someone within your state.

Request a Copy of Your Social Security Record of Earnings

You can get your personal Social Security Statement online by using your "my Social Security" account. To set up or use your account to get your online Social Security Statement, Sign-In or Create an Account at https://secure.ssa.gov/RIL/SiView.do

Request A Copy of Your Medical Information Bureau (MIB) File

MIB Group, Inc. (MIB) is an organization that compiles a central database of medical information. Approximately 18 million Americans and Canadians are on file in MIB's computers. More than 400 insurance firms use the services of MIB, primarily to obtain information about life insurance and individual health insurance policy applicants. You are entitled to a free medical record disclosure once a year. You can get a copy by calling the Medical Information Bureau toll-free at 1-866-692-6901 or online at http://www.mib.com/.

Family Educational Rights and Privacy Act (FERPA)

According to the US Department of Education, "a school may disclose directory information to anyone, without consent, if it has given parents: general notice of the information it has designated as "directory information;" the right to opt out of these disclosures; and the period of time they have to notify the school of their desire to opt out. FERPA defines "directory information" as information contained in a student's education record that generally would not be considered harmful or an invasion of privacy if disclosed. Directory information could include: name, address, telephone listing, electronic mail address, date and place of birth, dates of attendance, and grade level; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors, and awards received; and the most recent school attended." (US Department of Education, 2007) If you have children in school, or are attending school yourself, contact your school for their FERPA opt-out forms and procedures. See the Privacy Rights Clearinghouse report, "Privacy in Education".

Consider Single Use Credit Card Numbers When Shopping On-line

When you shop on-line or over the telephone it is necessary to provide a credit card number to complete your purchase. But what happens to your credit card data after the transaction is complete? Does the merchant keep your credit card information on file? Will you be charged for a re-occurring transaction when you only authorized an on-time charge?

To help protect you against identity theft and loss of your credit card data, both Bank America and Citibank allow you to generate single use credit card numbers for a specific merchant or transaction.

- Bank of America ShopSafe - https://www.bankofamerica.com/privacy/accounts-cards/shopsafe.go
- Citibank Virtual Account Numbers - https://www.cardbenefits.citi.com/products/virtual-account-numbers.aspx

The single use credit card number works just like the number, expiration date, and security code printed on your credit card, and of course these charges appear on your monthly bills as usual. However, single use credit card numbers are limited to a single merchant, a single transaction, or for a limited period of time set by you. Once the transaction is complete or the expiration date you assigned to the single use credit card number is reached, that number is canceled and can't be used if stolen or later accessed by an unscrupulous merchant.

Single use credit card numbers are an excellent security tool; unfortunately, most banks and credit unions don't offer this service. If you don't have a credit card issued by either Bank of America or Citibank, you can still take advantage of the security offered by single use credit card

numbers by subscribing to services like “Blur” from Abine, Inc. https://www.abine.com/index.html. Blur Premium Service lets you generate single use credit card numbers that can be used on-line just like your regular credit card number. Blur Premium cost $3.00 per month, in 2017.

A site similar to Blur is “Privacy” - https://privacy.com/ which also allows you to create single use debit card numbers. Privacy generates virtual card numbers that protect your security and privacy when you shop online. Privacy Visa Cards may be used everywhere Visa debit cards are accepted. Virtual cards work just like gift cards. They are locked down to a single merchant and you can make them single-use (burner cards) and set transaction or monthly spending limits on them. When you generate a new Privacy card you are provided with a random 16-digit Visa card number that you can use at on-line merchants that accept Visa debit cards. You can set spending limits, controls, and close this virtual card anytime you want. Your bank account isn't charged on card creation. It is only charged when you decide to actually spend using the card you generate.

A disadvantage to single use card numbers is that they can only be used on-line. However, if you have an iPhone / iPad you can use Apple Pay - https://www.apple.com/apple-pay/ - to make purchases, in select stores, without having your credit / debit card details disclosed to the merchant. This helps protect you in case of a data breach.

Avoid Using Your Debit Card for Point of Sale Purchases

According to the Privacy Rights Clearinghouse - https://www.privacyrights.org/ - "Consumers often use debit cards instead of credit cards for smaller purchases, such as at fast food restaurants. However, debit cards expose consumers to greater fraud risks than credit cards. This is particularly true when the restaurant has not upgraded its payment terminals to utilize safer chip technology... So why is using a debit card riskier than using a credit card? For starters, if your card information is used unlawfully, your bank is not obligated to restore the funds to your account for at least two weeks while it investigates the incident. During this time period, you may not have your funds available in your account to pay your mortgage, rent, loans, or other bills... With a credit card, you do not have to pay for the fraudulent charges while your bank investigates. In addition, debit cards don't carry the same legal protection as credit cards. Federal law limits your liability on a debit card to $50, but only if you notify your financial institution within two business days of discovery of the theft. If you wait longer than 60 days, you could lose all the money in your checking account, and any other accounts tied to the card. With a credit card, you have no liability at all as long as you have possession of your card." (Recent Chipotle Breach Highlights Debit Card Risks)

Prepaid Gift Cards

If you are making a face-to-face purchase, then cash is the choice that offers you the greatest privacy, but cash simply isn't an option for on-line purchases. However, you can purchase prepaid Visa, Mastercard, and American Express gift cards that work on-line just like a credit/debit card, but don't link back directly to you. These prepaid gift cards have a small purchase fee above the value of the gift card itself. For example, in 2017 the $200 Vanilla Visa Gift Card sold at Walmart for $206.88. In some cases when using a gift card to make purchases on-line you will need to have a name and address associated with the card being used to make the purchase match the Address Verification System (AVS) used by credit card companies. In this case you will need to register your name and address (or some name and address) with the gift card issuer's web-site. We note that the name and address you register with the card does not have to be your own. The registered name and address for the card just must match the "billing address" you use when placing your on-line order. Prepaid gift cards are very useful for adding an additional layer of privacy to purchases of digitals services and products, such as subscribing to a Virtual Private Network (VPN). By using a prepaid gift cards these digital services and products are not linked to your personal financial accounts.

Safeguard Your Social Security Number

Be very protective of your Social Security number. It is the key to much of your personal information. You should provide your Social Security Number (SSN) only when absolutely necessary and only when specifically required by law; for example, on tax forms, and on other transactions in which the Internal Revenue Service (IRS) may be interested. That includes most banking, stock market and other investments, real estate purchases, many insurance documents, and other financial transactions as well as employment records.

Federal law requires private businesses to collect your SSN in certain situations. A business must collect your SSN when you are involved in a transaction in which the Internal Revenue Service requires notification, or you are engaged in a financial transaction subject to federal Customer Identification Program rules. Except in those few situations where your SSN is required by federal law, you are not legally compelled to provide your SSN to private businesses. There is no law, however, that prevents businesses from requesting your SSN, and there are few restrictions on what businesses can do with it. But even though you are not legally required to disclose your SSN, the business does not have to provide you with service if you refuse to release it. So, in a sense, you are strong-armed into giving your SSN. (Privacy Rights Clearinghouse) In July 2017, the Government Accountability Office published a report on the Need to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display of SSN - http://www.gao.gov/assets/690/686088.pdf.

Avoid Showing ID When Making a Credit Card Purchase

Some merchants may ask that you present ID when making a purchase with a credit card. In most cases the cashier ringing up your purchases just matches the name on the credit card to the name on the ID you present. These merchants wrongly believe that this somehow makes you safer by ensuring that you only use a credit card in your own name. However, there is nothing illegal about using someone else's credit card as long as you have their permission to do so. Furthermore, the major credit card companies know that presenting ID really does very little if anything to stop credit card fraud, but does significantly increase the likelihood of you becoming a victim of identity theft. Because of this the major credit card companies prohibit merchants from requiring that customers present ID as a condition of making a purchase with a properly signed credit card. The credit card companies ask that cardholders report merchants that are in violation of their policies. Here is Mastercard's on-line reporting form https://www.mastercard.us/en-us/consumers/get-support/report-problem-shopping.html. You will see that one of the specific violations listed by Mastercard is "The merchant/retailer required identification." VISA in its "Counterfeit Fraud Mitigation Best Practices" manual states: "it is important to remember that a Visa merchant must not require a cardholder to provide supplemental information such as government ID, driver's license, etc. as a condition of honoring the card." (VISA, 2016)

According to consumer reporter Susan Hogan, WPRI News (September 9, 2015) Businesses cannot require credit card users to show ID - The report states "Security experts say the information on your driver's license could be enough to steal your identity, which is why the Federal Trade Commission is cracking down on retailers who ask consumers to show theirs... Both MasterCard and Visa actually prohibit merchants from requiring identification as a condition for accepting their credit cards, provided the card is signed." http://wpri.com/2015/09/09/businesses-cannot-require-credit-card-users-to-show-id/.

A February 2014 study by Javelin Strategy & Research found that "an increasingly common method of identity theft is account takeover fraud... instead of just using a card for unauthorized transactions, fraudsters dive deeper and hack into existing accounts, change settings and make purchases in your name on-line." In order to do this effectively, the criminal needs additional personal information beyond that contained in the credit card transaction. This additional information is exactly what you provide by showing ID when making a credit card purchase.

Use Postal Money Orders

The United States Postal Service sells money orders which can be purchased and cashed at any post office. Although many financial transactions are electronic today, there are still times when you many want to send or receive money through the mail. Available in amounts up to $1,000

each, a postal money order is a simple way to send money through the mail. Postal money orders also add a layer of privacy to your transaction in that, unlike when writing a personal check, you don't reveal your personal banking details to the recipient of the postal money order.

Protect Your Postal Mail

Mail placed in a mail box on the outside of your home, or in a mail box along the public street is not secure. Anyone passing by can remove your mail from an unsecured mailbox and be gone in a matter of seconds. One of the best ways to protect your postal mail is to have it delivered to a PO Box at your local Post Office. Having mail delivered to a PO Box also helps to limit the need to disclose your home / street address. The Post Office will have your associated street address, but they won't release it to the general public. You may also choose to use a Commercial Mail Receiving Agency (CMRA), such as your local "UPS Store" - https://www.theupsstore.com/ - to receive your mail. CMRA operate under US Postal Service regulations for receipt and delivery of mail, but also provide additional services to their customers. Some CMRA specialize in providing services to transient populations, such as RV Travelers. These specialized CMRA can also protect your personal privacy by giving you an address in a different state. Examples of these specialized CMRA include:

Escapees RV Club Mail Service - https://www.escapees.com/support/mail-service

My Dakota Address - http://www.mydakotaaddress.com/

Package Deliveries

Commercial carriers like UPS and FedEx will only accept shipments to valid street addresses. They do not deliver to PO Boxes, although they will deliver to a CMRA. If you don't want packages delivered to your home, both UPS and FedEx have a "hold for pick up" option where they hold your package at the local processing hub, and you go there to pick up your package. Just show up with your ID and the package tracking number and pick it up – there are no additional fees. It pays to determine where your local UPS and FedEx hubs are located and whether it would be convenient for you to pick up your packages at these hubs.

If your local UPS and FedEx hubs are not a good option for you, find out what CMRA are conveniently located near your home or work. If you don't have an account with a CMRA, most of them will still receive a package for you on an occasional basis, for a fee. The advantage to having a package shipped to a CMRA is that your address isn't associated with the package. You will have to present ID and probably know the tracking number for the package, but for an occasional delivery you most likely won't need to have a regular account with the CMRA.

Get a Paper Shredder for Your Home

To help protect yourself against identity theft, stalking, and similar crimes it is important that you never place intact documents containing your personal, private, or financial information in the trash. A paper shredder is the best way of destroying sensitive documents before disposing of them in your trash or recycle bin. Paper shredders for home use range in price from around $50 to several hundred dollars. For home use a cross-cut shredder costing less than $100 will more than meet the needs of most users. An example of a good paper shredder for home use is the Amazon Basics 8-Sheet Micro-Cut Paper/CD/Credit Card Shredder http://goo.gl/UHYxUK.

If you can't afford to purchase a personal shredder for your home; check with your local sheriff, police department, crime stoppers organization, or bank for information about upcoming community shred events. Many times, these organizations will hire industrial mobile shredders to allow community members to destroy personally sensitive documents for free.

Secure Your Browser and On-line Activities

Install Mozilla Firefox - https://www.mozilla.org/en-US/firefox/new/ - and set it as your default browser. We choose Firefox because it allows for the best security configuration in the Windows operating environment.

Install the following add-ons to Firefox…

HTTPS Everywhere - https://www.eff.org/https-everywhere
Privacy Badger - https://www.eff.org/privacybadger
Adblock Plus - https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/

HTTPS Everywhere attempts to encrypt your connections to the web-sites that you visit on-line, while Adblock Plus and Privacy Badger keep those sites from downloading adware or other unwanted programs to your computer.

Adjust the privacy settings on your social media accounts to ensure good privacy and security of your personal information. Information on enhancing the security of your social media accounts can be found on 'Social Media Smartcards' (developed by Novetta in consultation with the FBI).

- Facebook - http://security.arizona.edu/sites/securitysiab/files/facebook_smartcard.pdf
- Google+ - http://security.arizona.edu/sites/securitysiab/files/google_smartcard.pdf
- LinkedIn - http://security.arizona.edu/sites/securitysiab/files/linkedin_smartcard.pdf
- Twitter - http://security.arizona.edu/sites/securitysiab/files/twitter_smartcard.pdf
- Smartphone - http://security.arizona.edu/sites/securitysiab/files/smartphone_smartcard.pdf

US Army CID, Cyber Crime Investigation Unit also posts several Cybercrime Prevention Flyers on-line at: http://www.cid.army.mil/cciu-advisories.html.

The **DOD Chief Information Officer** provides Social Media Education and Training at: http://dodcio.defense.gov/Social-Media/SMEandT/

Review the NSA's Best Practices for Keeping Your Home Network Secure

The National Security Agency provides customers with a wealth of knowledge and assistance for their Information Assurance (IA) goals. You can obtain a copy of "Best Practices for Keeping Your Home Network Secure" here https://www.iad.gov/iad/library/ia-guidance/security-tips/best-practices-for-keeping-your-home-network-secure-updated.cfm

Empty Your Computer Recycle Bin

Don't allow "deleted" documents to be stored in the Recycle Bin. Consider setting the Recycle Bin properties to: "Don't move files to the Recycle Bin. Remove files immediately when deleted." Better yet, use secure file deletion programs such as Eraser - https://eraser.heidi.ie/ - or Freeraser - http://www.freeraser.com/.

Run an Anti-Virus Program

Run a virus scan on your computer. If you have a current anti-virus program, run that program and let it scan your entire computer. If you don't have an anti-virus program installed on your computer, you can download free versions of the commercial anti-virus programs offered by many companies such as: Avast Anti-virus, AVG Anti-virus, Avira Anti-virus, Bitdefender Anti-virus, Comodo Anti-virus, or Panda Anti-virus. Additionally, check with your Internet Service Provider (ISP) to find out if they provide anti-virus programs for their customers. Many ISP provide anti-virus and Internet security software for free, or at a substantially reduced cost, for their customers. There are also various on-line anti-virus scanners. For an on-line anti-virus service, I like VirusTotal - https://www.virustotal.com/#/home/upload. When choosing an anti-virus product, I recommend reviewing anti-virus testing sites such as AV Test and AV Comparatives. Free anti-virus products will help protect your computer, but the paid versions of these products offer greater functionality and more enhanced protection for your system. When purchasing an anti-virus product, I recommend (in 2017) those offered by Bitdefender and Kaspersky.

Run Anti-Malware Programs

After you have run the anti-virus scan on your computer, the next step is to download three additional programs: CCleaner - http://www.piriform.com/ccleaner, Malwarebytes Anti-Malware - https://www.malwarebytes.com/, and Spybot Search & Destroy - https://www.safer-networking.org/. These programs help detect and repair problems on your computer that may not found by your anti-virus program. All three programs, CCleaner, Malwarebytes, and Spybot Search & Destroy offer free versions of their software. (Possible alternatives to CCleaner are BleachBit - https://www.bleachbit.org/ and Glary Utilities - http://www.glarysoft.com/, although CCleaner remains our first choice. Malwarebytes and Spybot Search & Destroy are alternatives to each other, but we have had the best success running them in conjunction with each other. If one program misses a piece of malware, the other is likely to catch it.) If you use CCleaner you can improve the program by running CCEnhancer which is a program that adds additional rules and definitions to the CCleaner winapp2.ini file; allowing it to clean a greater number of programs.

Install a Firewall

Further enhance the security of your computer and home network by installing a firewall. A basic firewall has been built into Windows since the introduction of Windows XP in 2001. At a minimum make sure that the Windows firewall is turned on. You can check the status of the Windows firewall from the control panel 'System and Security' area. The Windows firewall protects your system from outside attacks, but more robust protection can be obtained by running an advanced firewall. Install either the Comodo Firewall - https://personalfirewall.comodo.com/ or the Zone Alarm Firewall - https://www.zonealarm.com/software/free-firewall/. Both of these firewalls are free.

Use Search Engines That Do Not Track You

Google, Bing, Yahoo, Yandex - all the major search engines track your search history and build profiles on you, serving different results based on your search history. Usually your searches are saved along with the date and time of the search, some information about your computer (e.g. your IP address, User agent and often a unique identifier stored in a browser cookie), and if you are logged in, your account information (e.g. name and email address). With only the timestamp and computer information, your searches can often be traced back to you. With the additional account information, (i.e. when you run a search on Google while logged into your Google account) your on-line searches are associated directly with you.

Search engines that don't track your searches include:

DuckDuckGo - https://duckduckgo.com/

Startpage - https://www.startpage.com/

Ixquick - https://www.ixquick.eu/eng/

Disconnect Search - https://search.disconnect.me/

Lukol - http://www.lukol.com/

MetaGer - https://metager.de/en

Oscobo - https://oscobo.co.uk/

Encrypt Your E-mail

If you access your e-mail using MS Outlook or Mozilla Thunderbird https://www.mozilla.org/en-US/thunderbird/ you will be able to install a digital certificate that allows you to digitally sign and encrypt your e-mail. You can obtain a free digital certificate from Comodo https://www.comodo.com/home/email-security/free-email-certificate.php. Once you have your digital certificate installed you can digitally sign all for your e-mail and encrypt e-mail sent to other people who also have their own digital certificate installed.

Open PGP is an unofficial Internet standard for e-mail encryption, and anyone seriously interested in personal privacy and security should have and maintain a PGP key pair. GNU Privacy Guard for Windows (GPG) https://www.gpg4win.org/ is one of the easiest ways to set up Open PGP on your Windows computer. If you have not used a PGP type product in the past, you may find that there is a slight learning curve when you start using GPG. That being said, GPG is not particularly difficult to learn and the documentation available with the software provides clear instructions for setting up and using the program.

A similar program for conducting public key encryption in web-based e-mail programs is Mailvelope https://www.mailvelope.com/ which can be downloaded as either a Google Chrome Extension or a Firefox add-on. Install Mailvelope as an add-on to your Firefox browser. Once installed open Mailvelope, choose options and generate a key pair. You can now exchange encrypted messages with other Mailvelope and Open PGP users.

Another useful tool for using Open PGP encryption is GPG4USB http://www.gpg4usb.org/. GPG4USB combines a text editor and an Open PGP key manager into a small file. You can generate key sets, import external keys (such as the keys you generated in Mailvelope), and encrypt / decrypt messages in the text editor.

Use a Privacy Focused (encrypted) Web-based E-mail Service

Gmail, Hotmail (Outlook), Yahoo Mail, and similar e-mail providers all provide good quality web-based e-mail services. What they don't provide however is strong security for your e-mail messages. By using a privacy focused web-based e-mail service you still have good quality e-mail, but with the added advantage of having strong security for all of your messages. Some of the best privacy focused e-mails services include:

Lavabit - https://lavabit.com/

Protonmail - https://protonmail.com/

Scryptmail - https://scryptmail.com/

Sendinc - https://www.sendinc.com/

Tutanota - https://tutanota.com/

Unseen - https://www.unseen.is/

Location security can be added to your e-mail by creating and always accessing the account on the TOR network. Examples of e-mail services accessible on the TOR network include:

ProtonMail – http://protonirockerxow.onion

Mail2Tor – http://mail2tor2zyjdctd.onion

TorBox - http://torbox3uiot6wchz.onion

It must be understood however that TOR does not protect the content of your e-mail from data breaches, or if the actual e-mail servers are compromised. A comment from the Reddit web-site serves as an example: *"The first free. onion accessible email service that was widely used was tormail.net / tormail.org during 2011-2013. Tormail was taken down by the FBI because it happened to be hosted at FreedomHosting (a free. onion web host) whose server(s) the FBI seized because FH was allowing other things that were horrible (CP) to be hosted. The FBI now has full access to all the non-PGP encrypted information that was on the tormail server when they seized it, and they have used their access to that information in multiple investigations. Remember this when using such email services."* (Reddit)

Check Whether Your E-mail Address Has Been Part of a Data Breach

Data breaches happen more frequently than you might think. When an organization's customer or client list is compromised, so too is your personal information if it was part of the compromised data. Sites such as Breach Alarm, Have I Been Pwned, and Hacked-Emails keep track of data breaches when they are reported and allow you to check whether your information was included in one of these data breaches. Enter your e-mail address on the following web-site and they will let you know whether your e-mail was part of a reported data breach.

Breach Alarm - https://breachalarm.com/

Have I Been Pwned - https://haveibeenpwned.com/

Hacked-Emails - https://hacked-emails.com/

If you find that your e-mail address was part of a data breach, it is likely that other information was compromised as well (possibly your name, address, telephone number; and maybe even credit card information).

Use Google Alerts to Monitor the Internet for Your Personal Information

Google Alerts - https://www.google.com/alerts - allows you to create an alert for specific search terms (such as your name) and have Google send you an e-mail any time there are new occurrences of those terms cataloged by Google. Google Alerts can contain all of the parameters allowed in a Google search, so you can design alerts to watch specific sites, or to watch for your name in combination with other information such as your place of employment.

Encrypt Your DNS Traffic

Whenever you connect to the Internet your connection requests are resolved through a domain name server (DNS). In the same way that HTTPS encrypts your web-traffic, it is important to also encrypt your DNS traffic. DNSCrypt - http://dnscrypt.org/ - is a lightweight program that encrypts and authenticates your connections with a DNS server. DNSCrypt helps to prevent DNS Spoofing and safeguards against an adversary monitoring your DNS requests. DNS Crypt works in a manner that is similar to how SSL/TSL encrypts HTTP/HTTPS traffic, except that DNS Crypt uses elliptic-curve cryptography. By running DNS Crypt on your computer, you can help to protect yourself against spoofing, man-in-the-middle attacks, and monitoring of your DNS requests.

Secure Your Home Wireless Network

Many people run a home wireless (WiFi) network. This allows connection of laptops, tablets, smartphones, and other devices from anywhere within and around your home. However, if you leave your home WiFi network unsecured it is available to anyone close enough to receive your WiFi signal. (As a general rule of thumb, WiFi signals from commonly used home routers travel 150 feet indoors and 300 feet outdoors. WiFi signals can be received at much greater distances using specialized antennas.) To access your router, type its IP address into the browser of any computer connected to your network. The router's IP address will often be either 192.168.0.1 or 192.168.1.1. However, if this is not the case on your home network, open the Windows command prompt and run the 'ipconfig' command. Look for your Default Gateway IP address. Enter the Default Gateway IP address on your browser's URL line and it will access your home network router. You will likely be prompted for a login and password. This may be included on the label on the back / bottom of your router, or you may need to search for the default login and password for your particular make and model of router on-line. A good place to find most router default passwords is http://www.routerpasswords.com/. Now that you have logged into your router, change the admin password to something other than the default you were able to look up on-line. Change your SSID to something that does not identify your router type (i.e. your router SSID should not be linksys or netgear, etc.), and something that does not identify you personally (i.e. don't set your SSID as your name). You may also choose to hide your SSID so that it is not broadcast. In this way, someone scanning for WiFi networks won't see your home network in the list of those present in the area.

Google location services maps publicly broadcast WiFi data, including the SSID and MAC address of the router. This can result in Google collecting and data-basing information about your home router. If you don't want Google to map your home WiFi router you can opt-out by appending a nomap suffix to your SSID name. If your router name is "MYROUTER" you will need to change it to "MYROUTER_nomap". This will result in Google not mapping your router through Google Location Services, or if it is already in the database it will be dropped the next time some device connects to the Internet through your SSID_nomap address. Set your wireless security mode to WPA2 and set a strong password for your WiFi network. WPA2 gives you the strongest encryption. WPA is weaker encryption but is still being used on some WiFi networks. Avoid WEP as this provides only basic encryption that can be easily cracked. If for some reason your router doesn't support WPA2 maybe it's time to upgrade your router.

Protect Your On-line Chats with OTR Encryption

Use encrypted chat programs to protect your on-line conversations from being intercepted and monitored. Pidgin Instant Messenger https://www.pidgin.im/ is a universal chat client that consolidates all of your chat programs in one place. Using OTR Encryption

https://otr.cypherpunks.ca/ , a plug-in for Pidgin, you can encrypt your chats to protect your personal privacy. The Electronic Frontier Foundation has detailed instructions on how to use Pidgin and OTR https://ssd.eff.org/en/module/how-use-otr-windows.

Other secure chat programs include Cryptocat https://crypto.cat/ and Ricochet IM https://ricochet.im/ which runs over the TOR Network https://www.torproject.org/.

Use a Secure Messaging App to Communicate Privately with Friends and Family

With standard SMS text messaging, your communications are neither secure nor private. Your cellular service provider maintains records of your calls and text messages. Chloe Albanesius writing in PC Magazine (September 30, 2011) stated, *"According to data gathered by the Department of Justice... AT&T, for example, retains information about who you are texting for five to seven years. T-Mobile keeps the same data for five years, Sprint keeps it for 18 months, and Verizon retains it for one year. Verizon is the only one of the top four carriers that retains text message content, however, and it keeps that for three to five days. Call detail records, meanwhile, are retained for one year by Verizon, five years for T-Mobile (two years for pre-paid), five to seven years for AT&T, and 18 to 24 months for Sprint."* While Verizon is the only carrier that stored text message content as a general practice, there is nothing to prevent other carriers from doing so, or from changing their data retention policies in the future.

A secure messaging app encrypts your private communications, preventing them from being read by anyone other than by the intended recipient. Some of the best secure messaging apps include:

Signal Private Messenger - https://whispersystems.org/

Wickr Me - https://www.wickr.com/

Telegram (with 'Secret Chats') - https://telegram.org/

Chat Secure - https://chatsecure.org/

Threema - https://threema.ch/en/

WhatsApp - https://www.whatsapp.com/

Viber - https://www.viber.com/

Facebook Messenger also has an option to use encrypted "secret" chats. This option is not on by default, but with the latest versions of Facebook Messenger you can choose to encrypt your chats with others. More information is available on the Facebook help page at https://www.facebook.com/help/messenger-app/1084673321594605/

Secure File Sharing

Using Dropbox - https://www.dropbox.com/ - you can share large files and collaborate on projects with others who have access to your Dropbox account. You can share files with anyone, even people who do not have a Dropbox account, by getting a link to the file in your Dropbox and sharing that link with others. To get a link for an item in your Dropbox, just log in to Dropbox on-line, select the item you want to share, click the "Share" button and copy the link. The link will be similar to the one shown here, and will contain the name of your file as part of the link.

https://www.dropbox.com/s/wp58xt1zofu6gn9/Get%20Started%20with%20Dropbox.pdf

Dropbox users with a paid account (i.e. Dropbox Plus or Dropbox Business) can password protect the files they share, requiring users to both have the link to the file and know the password to open it. Paid Dropbox users can also set a time when the link to the file will expire. If you are using the free version of Dropbox you can still share files, and you can expire the sharing link manually at any time. The free version of Dropbox doesn't allow you to password protect your files, but you can always create a password protected document first (i.e. MS Office password protected document) and then share that document from your Dropbox account.

This same type of file sharing can also be done using Google Drive - https://www.google.com/drive/. To get a link to share your files from Google Drive: Click the file you want to share. Then, click Share or Share Add people. At the top right, click Get shareable link. Next to "Anyone with the link," click the Down Arrow to choose what someone can do with your file: view, comment, or edit. You don't have the option to password protect this link, but as with Dropbox, you can always password protect your documents before uploading and sharing them on Google Drive.

Of course, sites like Dropbox and Google Drive aren't just for sharing items on-line. These sites are primarily Cloud storage for your documents, photos, and similar digital records. As a best practice, everything you upload to the Cloud should be encrypted. Boxcryptor - https://www.boxcryptor.com/en/ - is a program designed to encrypt the things you store in the Cloud, and with its 'Whisply' - https://whisp.ly/en - service allows you to send files with end-to-end encryption right from your browser.

In 2015, Amnesty International recommended the program MiniLock to encrypt files and protect your privacy on-line. MiniLock uses your e-mail address and a long passphrase to generate a key (MiniLock ID) that is used to encrypt files. You provide your MiniLock ID to others so that they can encrypt to you, and you use their MiniLock ID to encrypt messages to them. A MiniLock ID is a 45-character alpha-numeric string that works as a public key for encryption. Using the same e-mail address and the exact same pass-phrase will generate the same MiniLock ID (key pair) each time. Note however that including even an extra space (say at the beginning or end of your

e-mail address or passphrase) will generate a completely different MiniLockID. I like MiniLock, but note that it is only available as an add on for the Chrome Browser, which limits its usefulness as a general secure file sharing / encryption program. Still the need for the Chrome browser isn't an overwhelming problem since it is freely available world-wide. MiniLock was designed by Nadim Kobeissi, the creator of Cryptocat, a chat program that I also like.

Defend Against Keystroke Loggers

A keystroke logger monitors what you type on your keyboard and sends a log of those keystrokes to whomever planted the logger on your computer. A simple and effective program for defeating keystroke loggers is KeyScrambler - https://www.qfxsoftware.com/. KeyScrambler encrypts your keyboard input at the Windows kernel (keyboard driver) level, making it very difficult for a keylogger to intercept what you type before it is encrypted. Your key strokes remain encrypted within your operating system until they reach the destination application on your system, where KeyScrambler's decryption function converts the keystrokes back to plain text. Because a keystroke logger has to operate between the keyboard and the destination application; with KeyScrambler installed keystroke loggers can only record encrypted text.

Encrypt Sensitive Information on Your Home Computer

It is important to safeguard sensitive information stored on your computer. An effective way of doing this is to use an encrypted drive or encrypted container to secure your files when they are not in use. For a long time TrueCrypt https://www.grc.com/misc/truecrypt/truecrypt.htm was favored as the open source standard for disk encryption. In September 2014, the TrueCrypt developers claimed that the program was no longer secure and stopped all further support and development of the program. The TrueCrypt developers offered no detailed explanation for why the program was suddenly being declared unsecure. An independent review of the code, completed in April 2015, found no significant cryptographic weaknesses, and many people still use TrueCrypt for their disk encryption.

For individuals with doubts about the current security of TrueCrypt there is a replacement called VeraCrypt https://www.veracrypt.fr/en/Home.html that functions in much the same way as TrueCrypt, and is in fact just a continued development (a fork) for the TrueCrypt program. Another similar open source program is DiskCryptor https://diskcryptor.net/wiki/Main_Page, a program that supports full-disk encryption.

If you do not currently use disk encryption, download either VeraCrypt or DiskCryptor and create an encrypted container on your hard-drive in which you will store your sensitive files and documents.

If you are running the Pro or Enterprise editions of Windows 10, Windows 8 or 8.1, or the Enterprise or Ultimate versions of Windows 7 or Windows Vista, then Bitlocker Drive Encryption is included with your operating system. Bitlocker is not included with the Home versions of Windows. If Bitlocker is available with your version of Windows, the Bitlock Drive Encryption Manager will be in your Windows Control Panel. Bitlocker is designed to be used with a Trusted Platform Module (TPM). The TPM is a special chip in your computer that performs cryptologic functions. If your computer contains Bitlocker and a TPM, follow the instructions in the Bitlock Drive Encryption Manager to turn-on and configure Bitlocker. Some computers may be running a version of Windows that contains Bitlocker, but not have a TPM installed. If this is the case, you will need to make an adjustment to your system settings to allow Bitlocker to function.

To use Bitlocker without a TPM, run your computer's CMD prompt (command-line interpreter) as administrator and type "gpedit.msc". From the displayed menu, go to Operating System Devices (this is found under: Computer Configuration > Administrative Templates > Windows Components > Bitlocker Drive Encryption > Operating System Devices). In the Operating System Devices menu, select 'Require Additional Authentication at Start-Up', and be sure that the 'Allow Bitlocker without TPM' block is checked. Apply these changes. Exit the CMD prompt and return to the Bitlock Drive Encryption Manager in the Windows Control Panel. Follow the instruction to turn-on and configure Bitlocker. If your version of Windows supports it, I strongly recommend that you use Bitlocker full-disk encryption. Please note that Bitlocker initial encryption is very slow. To initially fully encrypt a large (1TB+) drive can take several hours.

Both VeraCrypt and Bitlocker (Bitlocker to Go) can be used to encrypt external hard-drives, and I strongly recommend that you use encryption to protect all external and portable drives. On USB drives I also like hardware encryption, and recommend both the Aegis Secure Key - USB 3.0 Flash Drive and the DataShur Pro - USB 3.0 Flash Drive.

If you want to encrypt just single files and folders, AxCrypt https://www.axcrypt.net/ integrates seamlessly with Windows and provides an easy-to-use, secure option. A standalone version of AxCrypt is available for Windows 32 and 64 bit. It is directly executable - no installation required. I recommend using the standalone version of AxCrypt.

The US Air Force Software Protection Initiative provides a free program, Encryption Wizard https://www.spi.dod.mil/ewizard.htm, that you can run from your computer desktop that will provide strong encryption to protect your personal information.

Use Anonymous E-mail Forwarding & Temporary E-mail Addresses

Anytime you provide your personal e-mail address to someone you open yourself up to potentially being flooded with SPAM, Phishing attempts, and all sorts of other unwanted e-mail. Using anonymous e-mail forwarding and temporary e-mail addresses protects your personal e-mail account from a flood of unwanted mail, while still allowing you to receive and reply to validation e-mail when you sign-up for a web-site or service on-line.

Anonymous e-mail forwarding lets you create multiple e-mail addresses that forward to your primary e-mail account. If one of the e-mail forwarding addresses you create starts receiving lots of SPAM or other unwanted e-mail, you can turn it off without having to disrupt your primary e-mail address. Sites that let you create permanent anonymous e-mail addresses include: Not Sharing My Info http://notsharingmy.info/ and 33Mail https://www.33mail.com/

Temporary e-mail addresses are designed to let you sign up for on-line services and reply to a validation e-mail, but usually last no more than a few minutes to a few days. Incognito Mail http://www.incognitomail.com/, Guerrilla Mail https://www.guerrillamail.com/, YopMail http://www.yopmail.com/en/, 10 Minute Mail - https://10minutemail.com/, Maildrop https://maildrop.cc/, and Mailinator https://mailinator.com/ are all sites that let you create a temporary e-mail address to receive e-mail. To help fight spam most temporary e-mail site don't let you originate an e-mail, but you can reply to e-mail that you receive.

Use A Password Manager

Password managers allow you to create and manage strong passwords across multiple sites. Password managers allow you to use long, complex passwords, without the need to remember more than a single master password for the password manager of your choice. Some of the most popular (and secure) password managers include: LastPass https://lastpass.com/, Keepass http://keepass.info/, KeepassX https://www.keepassx.org/, Password Safe https://pwsafe.org/, Dashlane https://www.dashlane.com/passwordmanager, Norton Identity Safe https://identitysafe.norton.com/, and RoboForm http://www.roboform.com/password-manager.

Set up Two-Factor Authentication to Protect Your On-line Accounts

Two-factor authentication is an additional security step that helps protect your on-line accounts. When you attempt to log in to an account from an unregistered computer, sites using two-factor authentication send you an addition code (i.e. a 6-digit number) that you must enter before accessing your account. This additional code is sent as a text message (SMS) to your cell-phone or may be obtained by using an app such as Google Authenticator, Authy Authenticator, or Microsoft Authenticator. With two-factor authentication set up, a person trying to break into

your on-line accounts would not only have to guess your password, but would also need to have possession of your cell-phone to obtain the additional security code. Some places where you can use two-factor authentication are: Google, Apple, Facebook, Twitter, Dropbox, PayPal, Microsoft, Coinbase. Yahoo Mail, Snapchat, Tumblr, VK, Pinterest and WordPress, among many others.

Use TOR and TAILS

"The Tor software protects https://www.torproject.org/ you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites that are blocked. The Tor Browser lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser to protect your anonymity, and is self-contained (portable)."

Tails https://tails.boum.org/ is a live operating system, that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your privacy and anonymity, and helps you to:

- use the Internet anonymously and circumvent censorship;
- all connections to the Internet are forced to go through the Tor network;
- leave no trace on the computer you are using unless you ask it explicitly;
- use state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging.

Use a Virtual Private Network

A Virtual Private Network (VPN) creates an encrypted connection (sometimes referred to as a tunnel) between your computer and the servers being run by the VPN. Traffic is passed from your computer through the tunnel to the VPN servers and then out to the Internet. Traffic from the Internet returns to the VPN servers where it is encrypted and passed back to you over the encrypted connection. In this way, anyone monitoring your computer can only see an encrypted connection to the VPN, and web-sites looking at incoming connections can only see that it comes from a VPN server. These web-sites cannot see that the connection originated from your computer. Examples of VPN providers include:

Express VPN - https://www.expressvpn.com/

IP Vanish - https://www.ipvanish.com/

Nord VPN - https://nordvpn.com/

Pure VPN - https://www.purevpn.com

Vypr VPN - https://www.goldenfrog.com/vyprvpn

Because all your traffic passes through the VPN, it is possible for the VPN operator to see (log) all of your activity. When choosing a VPN it is important to choose a VPN provider that maintains a "no log" policy. Most VPN will cost you a few dollars per month, although there are free / advertisement-supported VPN as well. Examples of free VPN include Tunnel Bear https://www.tunnelbear.com/, and Windscribe https://windscribe.com/.

Free Anonymous Proxies – An anonymous proxy works a bit differently than a VPN in that the proxy only handles traffic through your web-browser, while a VPN can be configured so that all data from your computer passes through the VPN. An anonymous proxy is useful when you just need to visit a web-site without leaving your IP address in the logs for that site, while a VPN provides you an encrypted connection. Connections through a proxy server may not be encrypted. Both the anonymous proxy and the VPN hide your IP address.

Anonymouse - http://anonymouse.org/anonwww.html

Hidester - https://hidester.com/

Hide Me - https://hide.me/en/proxy

Kproxy - https://kproxy.com/

Improve Your Home Security with Crime Prevention & Neighborhood Watch Programs

Use Checklists and Guides from the National Crime Prevention Council
http://www.ncpc.org/resources/files/pdf/neighborhood-safety/

Consider starting or participating in a Neighborhood Watch Program
https://www.bja.gov/Publications/NSA_NW_Manual.pdf

Review the State Department Guidance on Personal Security
At Home, On the Street, While Traveling
http://www.state.gov/m/ds/rls/rpt/19773.htm

You can also develop a general crime profile of your neighborhood by using on-line databases such as: Spotcrime - http://spotcrime.com/, Neighborhood Scout -

http://www.neighborhoodscout.com/, Crime Reports - https://www.crimereports.com/, My Local Crime - https://www.mylocalcrime.com/, City Data - http://www.city-data.com/, and Family Watchdog - http://www.familywatchdog.us/.

Learn How to Protect Yourself from and Respond to Scams and Frauds

The USA.gov web-site - https://www.usa.gov/scams-and-frauds - provides information about protecting yourself from scams and frauds. The Federal Trade Commission - https://www.consumer.ftc.gov/scam-alerts - also provides information about recent scams, as does the Internal Revenue Service (IRS) - https://www.irs.gov/uac/tax-scams-consumer-alerts. The FBI's Internet Crime Complaint Center (IC3) - https://www.ic3.gov/preventiontips.aspx - provides fraud and scam prevention tips, along with the National Criminal Justice Reference Service - https://www.ncjrs.gov/fraudawareness/prevention.html.

The Better Business Bureau (BBB) - https://www.bbb.org/scamtracker/us - scam tracker and BBB scam tips sites - https://www.bbb.org/scamtips - are very useful for seeing what type of scams are happening and learning how to avoid them. The BBB says: "There are thousands of new scams every year, and you can't keep up with all of them (we know, we try!). But if you can just remember these TEN THINGS, you can avoid most scams and help protect yourself and your family - https://www.bbb.org/avoidscams/.

1. Never send money to someone you have never met face-to-face.

2. Don't click on links or open attachments in unsolicited email.

3. Don't believe everything you see.

4. Don't buy online unless the transaction is secure.

5. Be extremely cautious when dealing with anyone you've met online.

6. Never share personally identifiable information.

7. Don't be pressured to act immediately.

8. Use secure, traceable transactions.

9. Whenever possible, work with local businesses.

10. Be cautious about what you share on social media.

Limit the Amount of Information That You Provide to Government Agencies

According to a 2015 Gallup Poll, 75% of Americans see widespread corruption in their government (Gallup, 2015). It is not just a belief that the government is corrupt, but an actual fear of this corruption by the majority of Americans that raises the greatest concern. According to the Chapman University Survey of American Fears: "Of the 89 potential fears the survey asked about, the one that the highest share of Americans said they were either "afraid" or "very afraid" of was federal government corruption. It was also the only fear that a majority of Americans said they shared." (Rampell, 2015) Within the top fears of Americans, after fear of corruption of government officials, the Chapman University Survey found that Americans also feared, cyber-terrorism, corporate tracking of personal information, government tracking of personal information, and identity theft (Zolfagharifard, 2015). The Pew Research Center conducted a study of public trust in government between 1958 and 2014 and found that Americans' trust of their government was at an all-time low in 2014 (Pew Research Center, 2014).

In July 2017, the Government Accountability Office published a report that stated: significant breaches of personally identifiable information (PII) have occurred within the federal government in recent years that have resulted in the unauthorized disclosure of information about millions of Americans. For example, the Office of Personnel Management (OPM) experienced a massive breach in June 2015 that involved the background investigation records of 21.5 million current and former federal employees. "Data breaches - including the unauthorized use and disclosure of PII such as SSNs - pose a persistent threat to government operations and the personal privacy of affected individuals. Thousands of information security incidents involving PII occur every year. For example, in fiscal year 2016, federal agencies reported 8,233 data breaches involving PII to the U.S. Computer Emergency Readiness Team." (http://www.gao.gov/assets/690/686088.pdf)

When conducting business with a government agency, only provide information specifically required by law. Certain government agency records are public record. Anyone can access the information you disclose to the agency within that record. Public records such as county assessor, county recorder, DMV and business licenses all may be available as a public record. Ask the agency if it allows address information to be confidential in certain situations. If possible, use a post office box and do not provide your middle initial, phone number or your Social Security number. If you own property or a car, you may want to consider alternative forms of ownership, such as a trust. This would shield your personal address from the public record. The Privacy Rights Clearinghouse report "Government Records and Your Privacy" provides more detail on how government records can be used to invade your privacy.

Install a Burglar Alarm and Other Home Security Devices

A study conducted by the University of North Carolina at Charlotte: "Understanding Decisions to Burglarize from the Offenders Perspective" (2012) http://airef.org/wp-content/uploads/2014/06/BurglarSurveyStudyFinalReport.pdf found that: “Indicators of increased security (alarm signs, alarms, dogs inside, and outdoor cameras or other surveillance equipment) was considered by most burglars when selecting a target.” and “About 60% of the burglars indicated that the presence of an alarm would cause them to seek an alternative target altogether.” Even fairly inexpensive alarm systems such as the Simplisafe2 Wireless Home Security System - http://goo.gl/0klTLL or the Fortress Security Wireless Home Security Alarm System with Auto Dial - http://goo.gl/yTbxEX can enhance the security of your home. The security of your home increases even more by adding security cameras such as the Vimtag Wireless Security Camera with Two-Way Audio and Night Vision - http://goo.gl/Mr5xUM. Additional security devices such as 24-Hour Digital Timers - http://goo.gl/7njaSP, FakeTV Burglar Deterrent- http://goo.gl/hLRp86, and Heavy-Duty Motion Sensor Security Lights - http://goo.gl/uwM9BG all add even more security to your home.

A Wireless Driveway Alarm - https://goo.gl/MzyRbv - can signal you whenever someone accesses your property, and a Video Doorbell - https://goo.gl/G5LuJv - allows you to see anyone at your door via video streamed to your smartphone or tablet.

In addition to having high-quality dead-bolt locks https://goo.gl/JNg2qU installed throughout your home, you may wish to consider the addition of Door Armor - http://goo.gl/feO5Ul, Window Security Film - http://goo.gl/9x2yPe, and using Master Lock Dual-Function Security Bars - http://goo.gl/lgX6l0 to increase security.

If you can’t afford a home security system, placing a Yard Sign - https://goo.gl/qzZoJU - warning of a security system, and installing a couple of fake security cameras - https://goo.gl/ydpudB - can still server as a deterrent to a criminal looking at your home.

Consider Personal Safety Apps

There are several personal safety apps that you can download to your smartphone. These apps will send alerts to contacts that you designate or call the police when specified conditions are met. These conditions may be something that you do, such as activating the app (pressing an emergency button), or something that you fail to do, such as failing to respond to a text message or enter a verification code. Personal safety apps to consider include: Safe Trek - https://www.safetrekapp.com/ - Kite String - https://www.kitestring.io/ - Bugle - http://www.gobugle.com/ - and Hiker Alert - https://hikeralert.com/.

Remove Pictures of Your Home from Google Maps Street View

Google offers a street level view of much of the world on its Google Maps site. This street level view may include pictures of your home if it is visible from a public street. Google gives you the option of having things such as your face, car/license plate, and home blurred in Google Maps Street View. To do this, find your home, or other item that you would like to have blurred in Street View and click on the "Report a Problem" link in the lower right corner of the image. Fill out the form to request that Google blur selected items to protect your privacy.

Keep an Inventory of Your High-Value Items
Participate in Operation Identification

1. Mark property or valuables with an identifying mark, preferably your driver's license with state abbreviation followed by number: Example: CA-B1234567

2. Inventory your marked property on a form with descriptions including brand, model number, and serial number. Keep it in a safe place.

3. Display the Operation ID decal on windows to show your participation in the program and to discourage burglary.

Take Precautions Against Surveillance

The purpose of surveillance is to identify a potential target based on the security precautions that individual takes, and the most suitable time, location, and method of attack. Surveillance may last for days or weeks.

Naturally, the surveillance of a person who has set routines and who takes few precautions will take less time.

Detecting surveillance requires a fairly constant state of alertness and, therefore, must become a habit. A good sense of what is normal and what is unusual in your surroundings could be more important than any other type of security precaution you may take. Above all, do not hesitate to report any unusual event.

There are three forms of surveillance: foot, vehicular, and stationary. People who have well-established routines permit surveillants to use methods that are much more difficult to detect.

If, for example, you leave the office at the same time each day and travel by the most direct route to your home or if you live in a remote area with few or no alternate routes to your home, surveillants have no need to follow you all the way to your residence.

You should:

- Vary your routes and times of travel.
- Be familiar with your route and have alternate routes.
- Check regularly for surveillance.

Stationary surveillance is most commonly used by terrorist organizations. Most attacks take place near the victim's residence, because that part of the route is least easily varied. People are generally most vulnerable in the morning when departing for work because these times are more predictable than evening arrivals.

Many surveillance teams use vans with windows in the sides or back that permit observation from the interior of the van. Often the van will have the name of a business or utility company to provide some pretext for being in the area.

Where it is not possible to watch the residence unobserved, surveillants must come up with a plausible reason for being in the area. Women and children are often used to give an appearance of innocence. Try to check the street in front of your home from a window before you go out each day.

If you suspect that you are being followed, drive to the nearest police station, fire station, or the U.S. mission. Note the license numbers, color and make of the vehicle, and any information printed on its sides that may be useful in tracing the vehicle or its occupants.

Don't wait to verify surveillance before you report it.

Be alert to people disguised as public utility crews, road workers, vendors, etc., who might station themselves near your home or office.

Whenever possible, leave your car in a secured parking area. Be especially alert in underground parking areas.

Always check your vehicle inside and out before entering it. If you notice anything unusual, do not enter the vehicle.

Household staff and family members should be reminded to look for suspicious activities around your residence; for example, surveillance, attempts to gain access to your residence by fraudulent means, and telephone calls or other inquiries requesting personal information.

Tell your household staff and family members to note descriptions and license numbers of suspicious vehicles.

Advise them to be alert for details. Household staff can be one of the most effective defensive mechanisms in your home--use them to your advantage.

While there are no guarantees that these precautions, even if diligently adhered to, will protect you from terrorist violence, they can reduce your vulnerability and, therefore, your chances of becoming a victim. (Surveillance - US Department of State, p.21)

Take A Firearms Safety Course

The Washington, DC Metropolitan Police Department offers an on-line firearms safety course - https://dcfst.mpdconline.com/. There is no cost for taking this course and it should take approximately 30 minutes to complete. Even if you don't own a firearm, understanding how firearms function and how to safely handle them is important.

According to U.S. Bureau of Justice Statistics data, having a gun and being able to use it in a defensive situation is the most effective means of avoiding injury (more so even than offering no resistance) and thwarting completion of a robbery or assault. In general, resisting violent crime is far more likely to help than to hurt, and this is especially true if your attacker attempts to take you hostage, such as sometimes happens in a carjacking situation. Most often with gun defenses, criminals can be frightened away or deterred without a shot being fired. Estimates of these types of defensive uses of firearms are wide ranging, from a low of 65,000 to 82,000 annual defensive gun uses (DGUs) reported to the U.S. Department of Justice's National Crime Victimization Survey (NCVS), to a high end of some 2.1-2.5 million annual DGUs, but they seem to occur at least as often (if not far more often) each year as misuses of firearms by violent criminals. (http://www.bjs.gov/content/pub/pdf/fv9311.pdf)

If you choose to carry a firearm for personal protection, get training from an NRA Certified Instructor http://www.nrainstructors.org/search.aspx. Obtain legal guidance on the proper use of a firearm for personal protection from an attorney specializing in this area of law.

Take Free, On-line, Courses to Enhance Your Security Awareness and Knowledge

DoD Information Assurance Support Environment (IASE) - Cybersecurity Online Training

https://iase.disa.mil/eta/Pages/index.aspx

Department of Defense Information Assurance Support Environment (IASE) 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. Security awareness courses include:

- Cyber Awareness Challenge
- Smartphones and Tablets
- Social Networking
- Phishing Awareness
- Personally Identifiable Information (PII)
- Portable Electronic Devices / Removable Storage Media

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) - https://teex.org/Pages/Program.aspx?catID=607 - offers a series of free, on-line cyber-security courses. The courses offered are:

Cyber 101 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

Cyber 201 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

Cyber 301 Managers and Business Professionals

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

The Center for Development of Security Excellence, Security Awareness Hub - https://securityawareness.usalearning.gov/ - offers several security awareness courses that are available to the general public.

The Federal Emergency Management Agency (FEMA) - https://training.fema.gov/is/ - offers several emergency management courses on-line. Among these courses are security awareness courses, including:

- IS-106 Workplace Violence Awareness Training
- IS-906 Workplace Security Awareness
- IS-907 Active Shooter: What You Can Do
- IS-912 Retail Security Awareness: Understanding the Hidden Hazards
- IS-914 Surveillance Awareness: What You Can Do
- IS-915 Protecting Critical Infrastructure Against Insider Threats
- IS-916 Critical Infrastructure Security: Theft and Diversion - What You Can Do

Level I Antiterrorism Awareness Training - http://jko.jten.mil/courses/atl1/launch.html is the annual training required for all DOD personnel. The course is also available to the general public.

DEA Serving Abroad for Families and Employees (SAFE) Course (J3O P-US358) requires that you have access to JKO - https://jkodirect.jten.mil/ - and provides good personal security information for those who can access the training. The purpose of this five-hour course is to provide a safety and security training to Drug Enforcement Administration (DEA) employees and their families assigned or TDY overseas. This is a Department of State (DOS) requirement for issuance of country clearance.

Cyber Security Fundamentals Training (Army) - https://ia.signal.army.mil/IAF/default.asp - This course provides individuals an understanding of the information systems security policies, roles, responsibilities, practices, procedures, and concepts necessary to perform the functions of an Information Assurance Security Officer (IASO). The lessons presented will aid the IASO in developing an effective security approach and in selecting cost-effective controls to meet the requirements of laws, directives, and regulations.

National OPSEC Program - Interagency OPSEC Support Staff (IOSS) - https://www.iad.gov/ioss/ - The primary responsibility of the Interagency OPSEC Support Staff (IOSS) is to act as a consultant to other U.S. government departments or agencies by providing technical guidance and assistance that will result in self-sufficient OPSEC Programs for the protection of U.S operations. Members of the IOSS staff assess OPSEC programs, assist in OPSEC program development, conduct surveys, assessments and provide OPSEC training. IOSS training is not available to the general public, however if you are a Government Employee or a contractor who supports a government contract which has an OPSEC requirement or Public Safety Personnel, you are eligible to apply for an IOSS account.

Recommended Reading and References

- ARS Teschica: A beginner's guide to beefing up your privacy and security online https://arstechnica.com/information-technology/2016/12/a-beginners-guide-to-beefing-up-your-privacy-and-security-online/

- Electronic Privacy Information Center: EPIC Online Guide to Practical Privacy Tools
  https://www.epic.org/privacy/tools.html

- Advanced DIY Privacy for Every Woman
  https://chayn.gitbooks.io/advanced-diy-privacy-for-every-woman/content/

- Jolly Roger: Dark Web Beginners Security Guide
  https://darkwebnews.com/help-advice/dark-web-beginners-security-guide/
- Tom's Guide: 13 Security and Privacy Tips for the Truly Paranoid
  https://www.tomsguide.com/us/pictures-story/545--13-paranoid-security-privacy-tips.html

- Consumer Reports: 66 Ways to Protect Your Privacy Right Now
  https://www.consumerreports.org/privacy/66-ways-to-protect-your-privacy-right-now/

- Security & Counter-Surveillance: Information Against the Police State
  http://325.nostate.net/library/security-countersurveillance.pdf

- Electronic Frontier Foundation: Surveillance Self-Defense
  https://ssd.eff.org/en

- Information Security for Journalists
  https://files.gendo.ch/Books/InfoSec_for_Journalists_V1.1.pdf

- Security in a Box
  https://securityinabox.org/en/

- Security Culture: A Comprehensive Guide -
  https://www.inventati.org/securityau/securityau-v1.pdf

- Privacy Tools
  https://www.privacytools.io/

- Heimdal Security: 131 Cyber Security Tips that Anyone Can Apply
  https://heimdalsecurity.com/blog/cyber-security-tips/

- Security Culture: A Comprehensive Guide -
  https://www.inventati.org/securityau/securityau-v1.pdf

Information Security (INFOSEC) and Operations Security (OPSEC) for Government Employees

Encryption

Encryption is an essential function in protecting the content of your electronic communications. Encryption works by taking data (text, pictures, video, audio files, etc.) and scrambling that data so that it becomes unintelligible. Decryption is the reversal of the encryption process, thereby returning the encrypted data back to its original form so that it can once again be understood. The exact process of encryption and decryption can be mathematically complex, and is beyond the scope of our discussion here. What is important to understand however is that a strong encryption algorithm, properly implemented, will protect the content of your communications from being understood by anyone who does not possess the proper key to decrypt your messages and return them to an intelligible form.

Digital certificates, also called S/MIME (Secure / Multipurpose Internet Mail Extension) certificates, allow you to digitally sign and encrypt your electronic communications. A digital certificate may be included with your official / business e-mail account. If you have a government issued common access card (CAC) or personal identity verification (PIV) card your digital certificate is contained in the chip on the card. (A common access card (CAC) is a smart card used by service members and employees of the United States Department of Defense (DoD). The Personal Identity Verification (PIV) card is used by employees of other non-DOD Federal agencies.) The advantage of having a digital certificate on a CAC or PIV is that it allows you to carry it from one place to another, and log-in to government computers at multiple locations.

If you already possess a CAC you can use it to send and receive encrypted e-mail and access CAC restricted web-sites and programs (such as ActivClient, AKO, OWA, DKO, JKO, NKO, BOL, GKO, Marinenet, AF Portal, Pure Edge Viewer, ApproveIt, DCO, DTS, TENS, Disa Enterprise Email) from your personal computer at home. To use your CAC from home you will need a CAC reader attached to your computer. You may be able to have a CAC reader issued to you by your agency, or you can purchase one from places like Amazon.Com for around $10-$20.

Smart Card Readers: http://amzn.to/2wvTjKR / http://amzn.to/2vDkR4E

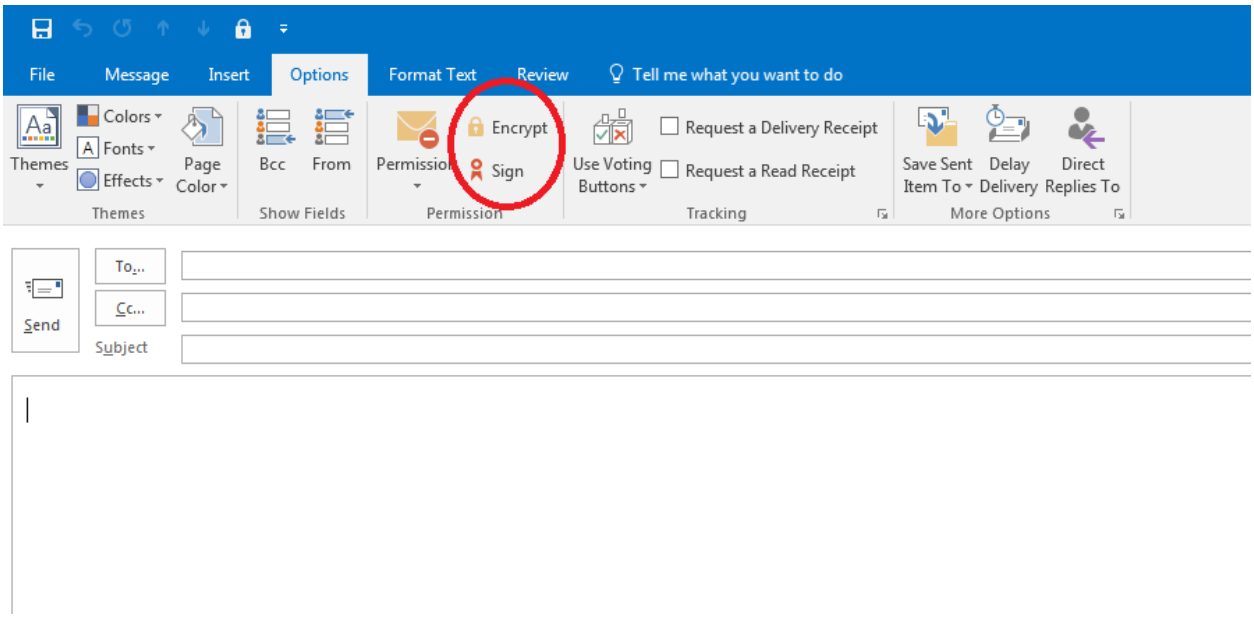
In many cases, your CAC reader will be plug-and-play, allowing you to access CAC restricted web-sites and send and receive encrypted e-mail without additional installations. However, if you have trouble getting your CAC to work from home, detailed instructions are available at https://militarycac.com/ that explain how to set up your home computer to work with your CAC.

If you don’t have a CAC or PIV you can still obtain a personal digital certificate from various non-government certificate authorities. Of course, a personal digital certificate won’t grant you access to government computer networks, but it does allow you to send digitally signed and

encrypted e-mail between yourself and anyone else using S/MIME certificates (such as those contained on the CAC and PIV card). Comodo offers a free personal digital certificate, while other companies such as Verisign and Entrust charge a few dollars per year to issue a personal digital certificate. (Comodo Link: https://www.comodo.com/home/email-security/free-email-certificate.php)

After installing a digital certificate on your computer, you will be able to digitally sign e-mail that you send to other people. Your digital signature also includes the part of your digital certificate (the public key) needed to allow others to encrypt e-mail they send to you. In order for you to send encrypted e-mail to someone, you must first obtain a copy of their public key. To do this, have them send you a digitally signed message and save it to your e-mail contacts list in MS Outlook, or to whatever e-mail client you are using. Note that you will have to be using an e-mail client on your computer, since you will not be able to save digital certificates to web-based e-mail (such as G-mail or Yahoo Mail).

As a best practice, all of your e-mail communication should be encrypted. From the most mundane to the most sensitive, encrypt everything. If you only encrypt sensitive e-mail, even though the content of the message is protected by encryption, the fact that only some e-mail is encrypted can indicate when you are engaged in a sensitive conversation. When everything is encrypted mundane and sensitive communication appears the same.



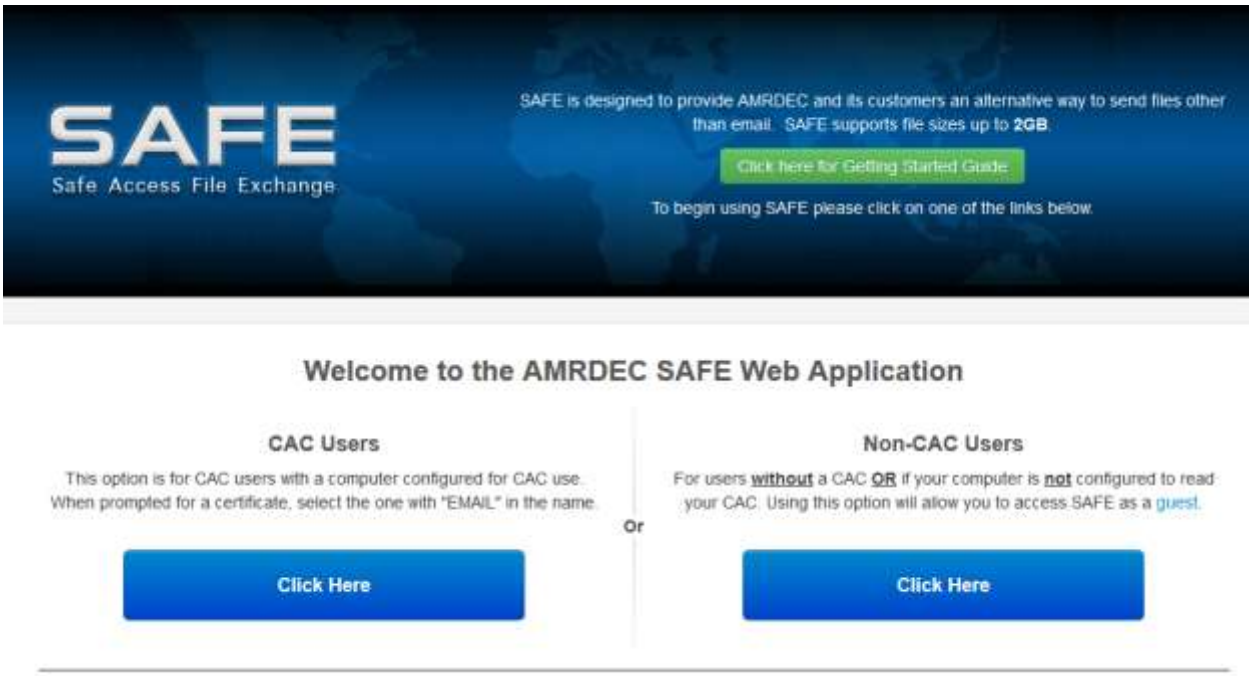
Once you have a digital certificate installed on your computer, and have obtained the public keys of others with whom you want to communicate, signing and encrypting messages is as simple as clicking a button on your e-mail toolbar. The installation of digital certificates and exchange of

encryption keys will most likely be handled by your IT Department for your official / business e-mail accounts. For your personal e-mail account, you will have to handle installation of your digital certificate and exchange of keys (often by exchanging digitally signed messages) yourself, but this is not overly difficult, and becomes quite easy after you have done it once or twice.

The goal is to ensure that everyone with whom you communicate by e-mail has a digital certificate, and that all of your e-mail communication is encrypted. It is important to understand however that your government provided encryption keys are archived and may be obtained under appropriate authority to decrypt anything encrypted with your digital certificate (i.e. CAC or PIV Card).

It should also be noted that when you are conducting official government business there may be specific record-keeping and archiving requirements. Federal guidance released by the National Archives Records Administration in July 2015 updated the government's policies regarding newer forms of communications: Guidance on Managing Electronic Messages, Bulletin 2015-02 (https://www.archives.gov/records-mgmt/bulletins/2015/2015-02.html)

AMRDEC SAFE - Army SAFE (https://safe.amrdec.army.mil/safe/Welcome.aspx)



You may need to exchange information with someone who does not have a digital certificate, and thus you are unable to encrypt an e-mail to that person. You should still ensure that the content of your message is protected, and this is where AMRDEC SAFE comes in. AMRDEC

SAFE allows users to upload files to a secure web-site. Once the files are uploaded, the system sends an e-mail and password to your designated recipients allowing them one-time access to download the files.

CAC holders can upload files and makes them available to any e-mail address. If you don't have a CAC you can still upload files, but they can only be made available to .gov or .mil e-mail addresses. This allows non-DOD personnel to securely share information with personnel working for government and military agencies.

AMRDEC SAFE is a file transfer system, so it is not a direct replacement for e-mail. It is intended for transmitting what would normally be attachments to an e-mail, such as documents, photos, or spreadsheets. An advantage of AMRDEC SAFE is that it allows to transfer up to 2GB of files at a time, which is far more than can be attached to an e-mail.

Encryption Wizard (http://www.spi.dod.mil/ewizard.htm)

Encryption Wizard is an easy to use program, designed and distributed by the United States Air Force Research Laboratory / Software Protection Initiative, which provides the user with strong encryption to protect files and folders stored on a computer or transmitted across the Internet. Encryption Wizard comes in fully compatible government and public versions. The government version of Encryption Wizard contains a FIPS 140-2 validated RSA encryption module licensed for use by government employees. The public version of Encryption Wizard uses the AES algorithm supplied by the Java Runtime Environment on your computer. Encryption Wizard is a free program available to anyone who wants to download and use it.

By using Encryption Wizard, you can significantly improve the security of your information in transit (e-mail) and the security of your data at rest (information stored on your computer).

Because Encryption Wizard works across multiple platforms it is ideal for securing communication between separate agencies and organizations. Similar advantages exist for individuals who use Encryption Wizard for personal use, securing private e-mail and safeguarding personal files, exchanged with friends and family.

To use Encryption Wizard simply drag and drop the file or folder to be encrypted onto the Encryption Wizard window and click the 'Encrypt' button for a single file or the 'Archive' button to encrypt multiple files into a single archive folder. Enter your encryption password, or select an encryption certificate and your data is encrypted and protected. To decrypt a file or folder just drag and drop the encrypted information into the Encryption Wizard window, click the 'Decrypt' button and enter the correct password or choose the associated certificate. Additional features of Encryption Wizard, such as generating public/private key certificates, generating secure passwords, and creating keychains to manage encryption certificates and passwords, enhance the overall usability and security of the program.

Encryption Wizard is a free, easy to use, program that you should have on both your home and work computers. Encourage your co-workers and associates in external agencies download their own copy of Encryption Wizard and start securing your shared communications, files, and folders. Talk with your organization's systems administrator about using Encryption Wizard to enhance the security of your business records and how to use it to best secure communication with outside agencies and clients. Because Encryption Wizard is a small program (only 3.88 MB) and requires no installation or set-up it can be easily carried on a USB/Thumb drive for use when travelling. If you need strong, easy to use encryption then Encryption Wizard is an excellent choice.

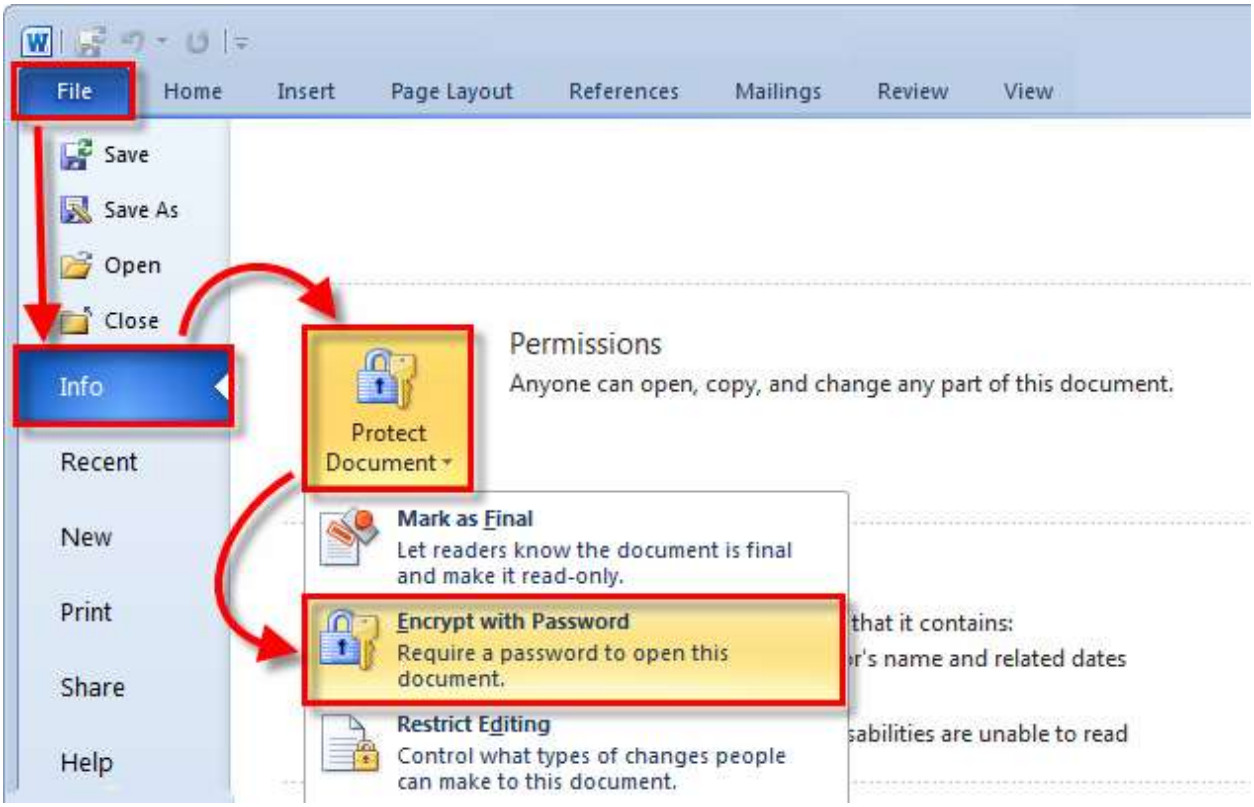
MS Office Encryption

MS Office allows you to protect documents (Word), spreadsheets (Excel), databases (Access), and presentations (PowerPoint) with a password. When MS Office products are protected, they are encrypted and a password is required to open and read them.

The default encryption values for MS Office 2013 are AES (Advanced Encryption Standard), 128-bit key length, SHA1, and CBC (cipher block chaining). This provides good security for the content of your products, but you must ensure that you are using a strong password.

Programs like Elcomsoft's Advanced Office Password Recovery and Elcomsoft's Distributed Password Recovery tools can use a variety of attacks to defeat MS Office password protection if you use a weak password to protect your products. According to the Elcomsoft web-site: "If your documents don't fall into the instant recovery category, their protection may be removed automatically in less than 10 minutes... Advanced Office Password Recovery performs a preliminary attack on the password, attempting to unlock the document with commonly used

passwords and passwords based on dictionary words. Your document may be recovered without any extra effort in just a few minutes!" (https://www.elcomsoft.com/aopr.html)



To add a password to an MS Office product, click on the 'File Tab', choose the 'Info' Menu, and then click on the 'Protect Document' ('Protect Workbook', etc.) Button, and choose "Encrypt with Password' from the drop-down menu. Add a password to the open dialog box, confirm the password, and now your MS Office product will require a password the next time it is opened.

Trusted End Node Security (https://www.spi.dod.mil/lipose.htm)

Trusted End Node Security (TENS) creates a secure end node from trusted media on almost any Intel-based computer (PC or Mac). TENS boots a thin Linux operating system from removable media without mounting a local hard drive. Administrator privileges are not required; nothing is installed. TENS 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.

TENS differs from traditional operating systems in that it isn't continually patched. TENS is designed to run from read-only media and without any persistent storage. Any malware that might infect a computer can only run within that session. A user can improve security by rebooting between sessions, or when about to undertake a sensitive transaction. For example, boot TENS immediately before performing any online banking transactions. TENS should also be rebooted immediately after visiting any risky websites, or when the user has reason to suspect malware might have been loaded. In any event, rebooting when idle is an effective strategy to ensure a clean computing session.

TENS is updated on a regular basis. Be sure to update to the latest version to have the latest protection and most recent drivers.

Editions

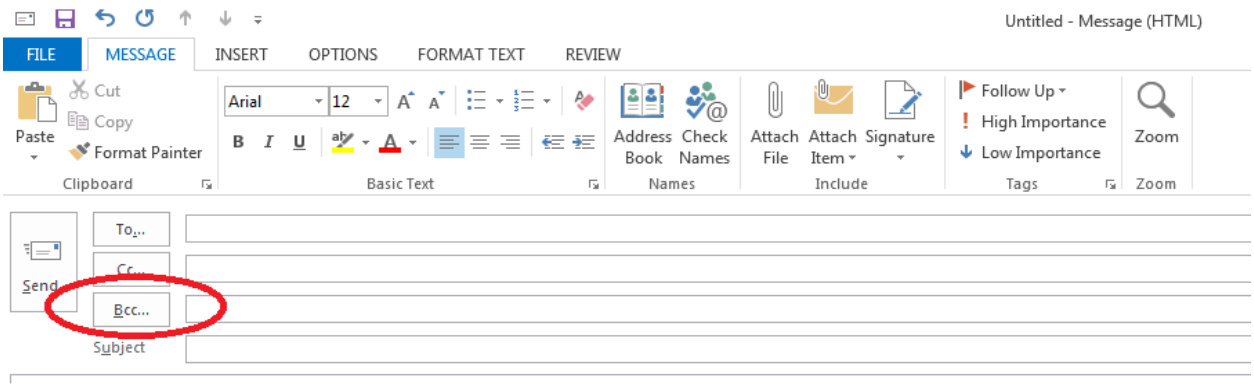
Each of the TENS products (TENS-Public, TENS-Professional, and Bootable Media) was created to address particular use cases.

TENS-Public is a safe, general-purpose solution for using web-based applications and accessing CAC and PIV-enabled web pages. TENS-Public Deluxe includes the open-source LibreOffice software suite. Both operating systems are available to download for free on the TENS website, as we contribute to the open source community. CAC middleware is integrated into the TENS operating system. TENS-Public is not intended to be an obfuscation tool; it is designed to be a safe operating environment for web-based activity. Encryption Wizard Public Edition is included in TENS-Public. Customizations are not available for this product.

TENS-Professional is similar to TENS-Public but is offered exclusively to non-DoD federal organizations. It is customized by TENS engineers. Customization options include selecting specific applications, pre-configured settings for VPN and/or VDI, firewall configuration, web proxy, time zone, desktop background, browser bookmarks, etc. Encryption Wizard Government Edition is included in this build. TENS-Professional is currently used by several Federal organizations, primarily to help remote users securely connect to their organization's private networks.

Bootable Media is the secure, DoD version of TENS. Bootable Media has a strong legacy of providing secure remote access to DoD civilian, military, and contractor personnel. Bootable Media is the TENS flagship product and has a supported user base numbering in the hundreds of thousands. Development, sustainment, and configuration is centrally funded by DISA, so each DoD organization doesn't need to pay for this product. Customization is available and completed for all the features included in TENS-Professional, in addition to including DoD-specific accreditation controls. Bootable Media has an Authorization to Operate (ATO) for DoD networks.

Blind Carbon Copy (BCC)



While encryption protects the content of your messages, it does not protect other data associated with the messages such as the e-mail addresses to which you send your message. Someone

obtaining a copy of your e-mail might not be able to read its content, but that person would be able to assemble a detailed list of the people with whom you are communicating.

Large e-mail lists are often developed when sending out newsletters, bulletins, or daily announcements. If you send an e-mail to multiple people, a security best practice is to place all of the e-mail addresses on the Blind Carbon Copy (BCC) line of the message. Addresses on the BCC line are not visible to recipients of the e-mail, unlike addresses on the To: and Cc: lines which everyone can see. Everyone listed on the BCC line will receive a copy of the e-mail, but their e-mail address will remain invisible to other recipients of the message.

If a message is forwarded, addresses on the To: and Cc: lines are sent with the forwarded message, but addresses on the BCC line remain invisible and are not included with the forwarded message. If someone selects 'Reply All' in a message, the sender and everyone on the To: and Cc: lines receive the reply, but addresses on the BCC line do not receive the reply because they are not visible to the system. Of course, everyone on the BCC line is still able to reply to the sender of the message. In general, when using BCC to send e-mail to large groups there should be no addressees listed on the To: and Cc: lines. If your e-mail client will not send without an address on the To: line, put your own e-mail address there since everyone will know the message is from you anyway.

Keep in mind that many people do not want their e-mail address and other personal information disclosed to someone that they do not know. BCC helps to reduce Spam since BCC addresses cannot be seen and harvested by Spammers and BCC messages cannot not be used to develop lists of names of the employees of a company or members of an organization since, again, the names and e-mail addresses of the recipients are not visible. It should also be noted that NIST Special Publication 800-122, *"Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"* lists e-mail addresses as one type of PII. You may have specific legal requirements to safeguard PII, especially if you send information to people in multiple businesses, organizations, or government agencies.

BCC protects the privacy of individuals included in large e-mail groups. It also helps protect you (the sender) since someone monitoring your e-mail is unable to see with whom you are exchanging messages. BCC is a simple technique to improve security of your e-mail. Remember, however, that the e-mail addresses are not completely invisible. BCC e-mail addresses are visible on the Exchange Server as this is necessary in order to route your message to the addressee.

Information Sharing

Information sharing between agencies and organizations is useful for maintaining situational awareness of security threats, trends, tactics, techniques, and procedures. However, it is essential to note that "*the popularity and availability of a variety of Internet-based services (social*

networking sites, photo sharing, Web log (blogs), and so forth) have greatly increased the risk of inadvertent disclosures of sensitive and/or critical information and possibly Classified information (alone or through compilation). The fact these capabilities can be accessed from an ever-increasing number of mobile devices in addition to the traditional desktop workstation reduces the amount of reaction time available and also increases the risk to sensitive and/or critical information." (AR 530-1 OPSEC, 26 September 2014)

Information should never just be copied from open sources and reported as found. In all cases, prior to posting or sharing open source information, that information must be reviewed to ensure that it is in compliance with information security policies, and that the content is relevant and appropriate and void of critical and/or sensitive information.

It is also important to understand that information is not intelligence. Intelligence is the product that is produced from the collection, processing, and analysis of information as part of the intelligence cycle - https://www.fbi.gov/about/leadership-and-structure/intelligence-branch.

One way to help protect the content of shared information is to only make it available on secure web-portals. Personnel using these portals generally must have some type of official status, and may be subject to additional vetting before being granted access. However, posting to a web-portal alone does not ensure security of your communications. You must choose a web-portal that is appropriate to your activity, and recognize that while secure web-portals help secure the content of the information posted, they do not necessarily safeguard distribution lists, user names, and e-mail addresses. Also, ask yourself, what do you have to gain from posting? If you stand to lose more than you stand to gain - Don't Post It!

Some examples of secure web-portals can be found below.

milSuite (https://www.milsuite.mil/)

milSuite is a collection of online tools and applications produced for the purpose of bringing online collaborative methods and secure communities to the entire Department of Defense. milSuite is the preferred and recommended information sharing portal for DOD personnel and agencies.

Homeland Security Information Network (HSIN)
(https://auth.dhs.gov/oam/hsinlogin/HSINLogin)

The Homeland Security Information Network (HSIN) is the trusted network for homeland security mission operations to share Sensitive But Unclassified information. Federal, State, Local, Territorial, Tribal, International and Private Sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and in general, share the information they need to do their jobs.

Intelink (https://www.intelink.gov/)

Intelink is a group of secure intranets used by the United States Intelligence Community. Intelink-U (Intelink-SBU) is a sensitive but unclassified (SBU) variant of Intelink which was established for use by U.S. federal organizations and properly vetted state, tribal, and local officials so sensitive information and open source intelligence could be shared amongst a secure community of interest. Personnel assigned to DOD law enforcement agencies (i.e. PMO, DES, CID) should avoid using Intelink as an information sharing portal to avoid potential intelligence oversight violations, and the perception of violations of Posse Comitatus.

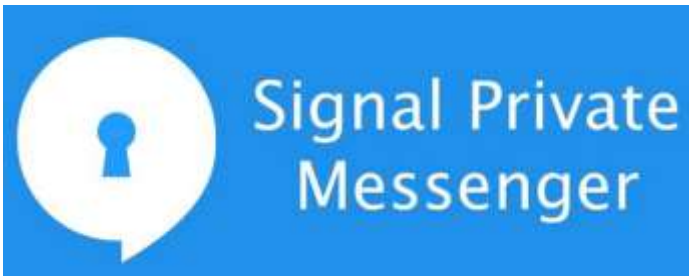
Law Enforcement Enterprise Portal (LEEP) (https://www.cjis.gov/)

The FBI's Law Enforcement Enterprise Portal (LEEP) is a gateway providing law enforcement agencies, intelligence groups, and criminal justice entities access to beneficial resources. These resources will strengthen case development for investigators, enhance information sharing between agencies, and be accessible in one centralized location.

Regional Information Sharing Systems (RISS) (https://www.riss.net/)

The mission of the Regional Information Sharing Systems (RISS) Program is to assist local, state, federal, and tribal criminal justice partners by providing adaptive solutions and services that facilitate information sharing, support criminal investigations, and promote officer safety.

RISS is composed of six regional centers and the RISS Technology Support Center (RTSC). RISS works regionally and on a nationwide basis to respond to the unique crime problems of each region while strengthening the country's information sharing environment. More than 9,000 local, state, federal, and tribal law enforcement and public safety agencies are members of RISS. RISS is used and trusted by hundreds of thousands of law enforcement officers and criminal justice professionals in all 50 states, the District of Columbia, U.S. territories, Canada, England, and New Zealand.



Signal Private Messenger (https://whispersystems.org/)

Generally speaking cellular telephone communication is not secure. While there are some exceptions, such as iPhone's Facetime and iMessage, this security isn't available when communicating with someone who uses a non-iOS cellular telephone. As a best practice, use cellular telephones only in exigent circumstances. Cell-phones and Blackberries will be used only when the mission clearly demonstrates a critical need for immediate communication and government / military telephone service and/or e-mail is not reasonably available. Government issued cell-phones will NOT be used in lieu of established land-line telephone service. Official calls should be made from official government land-line telephones when available. Government issued cell-phones and Blackberries will only be used to communicate UNCLASSIFIED information.

According to the American Bar Association (2015): 'While text messages have increasingly replaced phone calls, users do not always stop and realize that individually identifiable information, once captured in a traditional text message or third-party messaging system, likely becomes a PII record.' Consumer text messaging services also offer little protection from sending messages to an unintended recipient. Texting a personal message to the wrong recipient can be embarrassing, but text messaging PII to the wrong person potentially carries significant consequences. Indeed, a single text message including PII sent to the wrong number or wrong person would likely constitute a PII breach and Privacy Act Violation, subject to mandatory reporting and investigation by the Defense Privacy and Civil Liberties Office.

There are a number of cross-platform encrypted communication apps available, but one of the most secure is Signal Private Messenger. It is important to note that Signal Private Messenger is not government produced / approved software. However, Signal Private Messenger is widely considered the gold standard of encrypted messaging apps, is open source, security reviewed and audited, and available for free. If you are going to use your cellular telephone to communicate sensitive or private information, then it is essential that you have a secure communications application on your phone.

The Electronic Frontier Foundation (EFF) (https://ssd.eff.org/en/index), the leading nonprofit organization defending civil liberties in the digital world, provides guides for using Signal Private Messenger with both Android and iOS devices.

How to: Use Signal for Android - https://ssd.eff.org/en/module/how-use-signal-android

How to: Use Signal on iOS - https://ssd.eff.org/en/module/how-use-signal-ios

Michael Chesbro

http://www.chesbro.tech