Digital Security: Basics & Best Practices

Digital media have made our lives easier and made our work more efficient. Data that would once have filled a library now fits on a thumb drive. Messages that would once have taken hours, days, or weeks to deliver are now transmitted instantaneously via email, text message or chat. Information that might once have been laborious or impossible to find is at our fingertips on the Internet.

But with this great convenience comes insecurity, especially for people working at odds with their government or other entrenched powers. Having so much information easily at hand means our information is also easily searched and indexed by those who can gain access to it. And in general, our data and communications are insecure by default—the tools we use most were not designed with privacy at their core.

Fortunately, by following a few best practices and using a few simple tools, we can be much safer online, even with a dedicated adversary seeking to undermine our security. This document will walk you through a few of the simplest steps you can take to improve your digital security.

Physical Threats

The simplest threat to your digital security is that someone will gain physical access to your computer or mobile phone. Think about it: how much of your sensitive information would be readily accessible to someone who seized or stole your computer, mobile phone, or other hardware? This is the first step toward physical security: thinking about where you keep your private data, who has access to it, and what you'll do if someone tries to take it.

Once you have done this initial assessment, you can start to think about ways to protect your information. One great tool for protecting your data is called **TrueCrypt**. This simple piece of software is totally free and will run on any operating system. It works like an electronic safe so that nobody can access or open your files without the correct password. TrueCrypt can run on a computer or as a portable application on a USB drive, so you can use it on shared computers like those at an Internet café.

There is a lot of information on your computer that you may not even need or want—but it is there anyway, and can reveal a lot about you if discovered. Two tools for helping to get rid of that information are **CCleaner** and **Eraser**. CCleaner will clear the history, cookies and cache from your Internet browsers, and will clean out many temporary files from your hard drive as well.

Even after you delete unwanted files from your computer and "empty" the Trash or Recycling Bin, these files can still be recovered. That's where Eraser comes in. This small piece of software will overwrite the blank parts of your hard drive, so that once files are deleted, they're gone forever, and cannot be recovered.

Your mobile phone contains a huge amount of information about you, maybe even more than your computer: your contacts, email, calendar, photos, and a lot more. If you find yourself in a situation where someone may be about to seize your phone, you might want to delete all that information as quickly as possible. **In The Clear** is a mobile application that you can set up to wipe all the data from your phone quickly and easily, and also send an alert message to a predetermined contact that your security has been compromised.

Most major browsers now include a feature called “private” or “incognito” browsing. It’s important to know that this feature will **not** make you anonymous on the Internet: all your communications will be exposed to your Internet service provider (ISP), the sites you visit, and to any other third party monitoring your traffic. This feature will, however, prevent any data from being stored within the browser, erasing any record of sites visited, cookies or cached files. It can be a useful tactic for preventing incriminating data from being created in the first place.

Malware & Spyware

One of the most treacherous and pervasive threats to our digital freedom is the danger of computer viruses. These pieces of software can invade our computers, mobile devices or other hardware and undermine our privacy completely. Some malware will slow down or otherwise incapacitate your hardware so as to make it unusable. Some Trojans are designed to trick you into sharing private data such as credit card information or passwords. Some spyware can even record every keystroke you enter on your keyboard, revealing all your passwords and communication to an unknown third party.

The best defense against malware and spyware is prevention, and there are a few vectors through which most infections are spread. Be careful with:

- **Email Attachments**: This is a very common way for viruses to spread. You may receive an email that looks like it’s from someone you know, asking you to open an attached file—and the file may even look real when you open it—but is actually a virus. A good rule is to **never** open an email attachment unless you are expecting to receive it from a trusted contact.

- **Links**: Links that appear in email messages or on the web can take you to websites that will attempt to install malicious software on your computer. A good rule is to **never** click on a link unless you are sure of where it will take you.

- **USB Drives**: Some malware is programmed to invisibly copy itself onto every USB drive that is plugged into a computer, and then install itself on every computer to which the drive is later connected. A good rule is to **never** plug USB drives into your computer unless they’re brand new or they’re set to be “read-only” (in other words, they’re locked so that no files can be saved onto the drive).

- **Online Software**: You may hear about a new plugin or tool that might even purport to be a “security tool.” A good rule is to **never** install software on your computer unless you’re sure you trust the author.

If you’ve been infected, there are good tools to discover and clean infections. If you have a PC, **Malwarebytes** one of the best antivirus programs available, and while a paid subscription will offer comprehensive protection, their scanner is totally free. Other antivirus programs, such as **AVG**, **Avira**, and **Avast!**, are free, offer good, proactive defense, and can clean infections from your hardware.

With any of these programs, it's important to install their updates regularly, so that you're protected against the latest threats. It's a good idea to scan your hard drive every couple weeks, and if you discover any malicious software, get the help of a trusted technical expert and get clean quickly!

Passwords

Every single one of your devices and online accounts is protected by a password. In many cases, your password is all that stands between your information and a malicious intruder. A good password is longer than ten characters, and complex: not just a word out of the dictionary, but a collection of letters, numbers and symbols that looks like gibberish. There are strategies to create passwords that are both impersonal and hard to guess, yet practical to remember.

For example, a good password might be made up of the first letters of the words of a sentence, with numbers and symbols inserted in place of certain letters. Or you might put multiple words together into a nonsensical phrase, possibly even using different languages for different words in the phrase, and including numbers or symbols in place of certain letters.

It is very important not to use the same password for many of your sensitive accounts: if someone successfully steals one password, they suddenly have access to all your accounts and data. Ideally, you should have different passwords for every account or device. If you have trouble remembering your different passwords, you can use the program **KeePass**, which is an open-source tool for encrypting and keeping track of multiple passwords. Then, the only password you have to remember is the password for KeePass—better make it a good one!

One other thing to remember: if you are using a computer with key-logging spyware installed, your passwords may be compromised as you type them. In an Internet café or other situation where you're using a computer that might be compromised by a key-logger, a good practice is to copy and paste your password from other text, rather than typing it in.

Communications Security

When you send data over the Internet or mobile networks, it's important to remember that all data is, by default, unencrypted. That means anyone who intercepts your communication will be able to read it in plain text. It's very easy for your Internet Service Provider (ISP) to intercept your traffic, and ISPs often work very closely with governments and law enforcement agencies. Skilled hackers, too, can access your communications at various points along the path of communication.

One of the most common defenses against interception of data is **HTTPS**. Most URLs (web addresses) start with "HTTP://"; some, however, start with "HTTPS://"—that "S" means secure. Some online services—such as Google Mail (Gmail), most banks and online payment systems, and others—always use HTTPS. Other services—such as Yahoo! Mail—use HTTPS on the login page (where you enter your password), but not for the sending and receiving of email. Still others—including Hotmail, Facebook, Twitter, and others—don't use HTTPS by default except on the login page, but allow you to activate it on all pages.

A useful tool to make sure you're browsing as securely as possible is **HTTPS Everywhere**, which you can install as a plugin for the Firefox and Chrome browsers. This plugin will ensure that you always use HTTPS when it is available. But remember: even with this plugin, some sites (like Yahoo! Mail) don't offer HTTPS at all, and you will be exposed.

As on the Internet, sending data via your mobile phone is, by default, very insecure. Your phone calls and SMS messages are unencrypted, as is any Internet data you send or receive. Even more so than on the Internet, on mobile networks, it is easy for network operators (MNOs), governments, or malicious actors to intercept your information. What's worse, your mobile phone tracks your location constantly, even when you're not using it, and the camera or microphone on your phone can be activated remotely.

To stay secure, it is best not to share any sensitive information via your mobile phone; it is better to communicate with your contacts using predetermined code words and pseudonyms. If you don't want your location tracked or your conversations recorded, it is best to remove the battery from your phone when undertaking sensitive activities, or just leave your phone at home.

In general, it is important to remember a few key points:

- **There is no such thing as 100% digital security.** In general, it is best to assume that your online communications are insecure, and operate accordingly, but by following a few best practices, you can make yourself much safer.

- **Digital security is a shared responsibility.** All tools and tactics for online security are only as good as their weakest link. If you are following all best practices, but your contacts or friends are not taking the same precautions, you may still be exposed.

Resources

Security in a Box: https://security.ngoinabox.org/en
CPJ, Journalist Security Guide: https://www.cpj.org/reports/2012/04/information-security.php
Floss Manuals, Basic Internet Security: http://en.flossmanuals.net/basic-internet-security/
Safer Mobile: https://safermobile.org/