Secure Computing Basics for Targeted Individuals

TARGETED TECH TALK

WWW.TARGETEDTECHTALK.COM
TECHNICAL INFO AND SUPPORT FOR TI'S

Written by Frank S.
targetedtechtalk@protonmail.com
www.targetedtechtalk.com
Version August 16, 2025

image is creative commons public domain. Source: https://picryl.com/media/computer-laptop-in-the-workplace-computer-communication-b70300

Introduction -

This book focuses on the fundamentals of Cybersecurity that everyone should know. This book can be read and used by anyone and does not assume much prior computer expertise. The content and commentary in this book also includes highlights and useful insights for targeted individuals.

“Security is a Process, Not a Product” -- Bruce Schneier, security technologist

The best mindset to have when it comes to Cybersecurity is to recognize that security is a process, not a product. That means that to be successful you need to understand and apply security principles. We still need to do the right things even when we use the best products. There is not a product you can buy that will solve Cybersecurity for you. Don’t be fooled by any marketing making that claim.

I will share some of the key practices and processes in this book. I will also share some of the best in class software recommendations, including free and paid programs. While no tool or program is a fix for everything, the best programs are still a good starting point.

Types of Security Controls

Before getting too far into security specifics, lets examine the big picture concept of the types of security controls. In other words, why should you be concerned about Cybersecurity and some of the types of security.

Preventative Controls. (Keep them from getting in) These are things you do in order to prevent a Cybersecurity threat. A good example of this would be using a firewall on your computer. A firewall creates a barrier against network attacks. Another example is using encryption. This protects your data by making it unreadable to those who don’t have proper access.

Detective Controls. (Find them when they try to get in) These are things that identify suspicious activity as it is occurring. A good example is an antivirus or anti-malware program that detects and blocks suspicious files or activity.

Corrective Controls. (Get you back on your feet). These are things that allow you to recover if you have a disaster, accident, or Cybersecurity incident. A good example in this category is keeping external backups of important files on a storage drive.

Deterrent Controls. (Discourage them from attempting). These are things that may discourage potential threats from making an attempt. Example could include warning signs, or the threat of legal repercussions.

Firewall and Anti-malware programs

Most computers are going to come with a firewall program and I would recommend you enable it and leave it turned on. Most computers also come with a default antivirus program, which I would also recommend you enable. On Windows it is Windows Defender and on Mac it is Xprotect. I think these programs are fine to start with. They are built-in free options that provide a basic starting point. Make sure you have regular updates enabled.

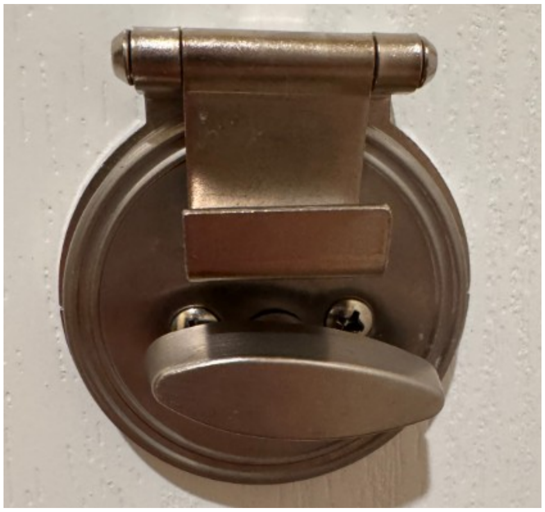
My current recommendation for the best paid anti-malware program is Bitdefender. You can buy an annual subscription which includes a certain number of devices. You can use the software on both computers and phones. https://www.targetedtechtalk.com/2024/12/16/best-paid-anti-malware-programs-for-computers-and-phones/

Physical Security and Home Security Systems

The first step on your checklist would be to verify the physical security of the place you live. If someone can get physical access to your home or apartment, there is really no software to protect your devices.

Doors. A good physical security measure for doors would be to get deadbolt blockers. These are metal inserts which physically prevent the deadbolt from turning. So even if someone were to have a key or be able to pick a lock, they would have no way of getting in short of breaking the door down. Of course you will still have to secure one door with a regular lock when you leave your house or apartment. An exterior padlock with exterior metal hinges in addition to your regular door lock on your exit door is probably the best physical security you can get.

Pictured is a deadbolt blocker. To install you loosen the screws of your deadbolt slightly and insert the metal blocker piece. You can purchase these for typically $20 or less and can be installed in a couple minutes.



Windows. If you search for window locks you can find many options. Typically these are clamps that attach to the window sill and physically prevent someone from opening the window from the outside. Someone would generally have to break the window to get past one of these devices.

Garage Door. When you are inside your house you can secure your garage door in a couple different ways. Garage doors have an outer and inner track, so you typically just need a way to keep the garage door from being pushed open from the outside. You can find sliding deadbolts that can work well and be installed on garage doors as well as simpler options such as security the two tracks together with pliers.

Putting all of this in place for an average size home or apartment can be done for under $100. Even if you don't experience overt break-ins, this level of physical security may bring you peace of mind. These types of locks can't be hacked, so starting with physical security is often a good idea.

Should you invest in a home security monitoring or camera system? Home security services that charge a monthly fee will be useless for targeted individuals. These organizations are too easily compromised both from the people side and from the technology side.

Likewise expensive camera systems are too easily compromised. Some targeted individuals have spent a lot of money on comprehensive camera systems only to find they are easily hacked and leave no evidence. Making an investment like this is often a form of so called 'asset stripping', separating you from your hard-earned money. Hard wired cameras would be more secure than wireless cameras but again I would not make a large investment in these cameras for the same reason, ultimately they are highly unlikely to leave you with any usable evidence.

Referring back to the previous section on control types – camera systems almost always fail as detective systems, leaving little usable evidence. Still a cheaper setup may still be a good option for some. You should not have the expectation that you will be getting great evidence, but by having a basic system in place you are forcing intruders to take the time and resources to jam or interfere with your system. You may notice a lessening in some activity with a basic camera as opposed to no camera system. So it may be slightly effective as a deterrent because they need to take action to make sure they don't give you any usable evidence.

If you have a car, a basic dash cam may also be a good idea. Having some footage may help you in the event of some kinds of accidents, etc. Again, go with something basic and functional.

Device Hardening

Now lets begin our discussion of computer and phone Cybersecurity. Device hardening refers to the process of making your device (phone or computer) harder to hack or break into. The best practice for device hardening is ***1) if you need it, keep it up to date, and 2) if you don't need it, uninstall it or turn it off.***

The reason this is important is that it reduces the surface area exposed to potential attackers. If you have Wi-Fi turned off for example, then there are hundreds of different wireless attack methods that you won't be subject to. Likewise with applications, don't keep applications installed on your phone or computer just in case. If you don't need it uninstall it. A potential vulnerability in an unused application could be the way an attacker gains access to your device.

I would also include your computer and phone's operating system as part of the list that you should keep up to date. Make sure to check for and apply updates regularly. Most software updates include at least some security fixes, so it is important to stay up to date.

Secure Email and Services

In considering an email provider and other online services targeted individuals should consider company location, ownership, and behavior in addition to the online service itself. For example, many United States based tech companies participated in the NSA PRISM program as revealed by Edward Snowden. This program involved many private companies providing the content of users and email directly to US intelligence agencies. So you should consider that security and privacy threats can come not just from someone breaking into your phone or computer.

Proton (https://proton.me) is one of the better choices currently because they are based in Switzerland which is not subject to direct action by US or western government entities. They offer email, online drive storage, VPN, and password management programs. They offer free versions of all of these services and you can also upgrade to a paid version for additional storage and features.

We should note that Proton does respond to warrants and orders that go through the Swiss court system. So using Proton does not guarantee your information will never be subject to a warrant, it just ensures that to do so would require a visible paper trail that is not in the hands of government / military interests.

I can also recommend the program 'Wire' for secure messaging. See this article for a full write-up. https://www.targetedtechtalk.com/2025/03/03/wire-end-to-end-encrypted-messaging-app/

A secure service will also use a modern encryption method. This article has a full explanation for of certain types of encryption now considered weak or obsolete. https://www.targetedtechtalk.com/2024/12/25/avoid-weak-encryption/

Benefits of VPNs – (Virtual Private Network)

In selecting a VPN, you will want to choose one that supports what is called 'full tunnel encryption'. Some VPN's such as Proton support this feature by default. A full tunnel VPN encrypts all traffic, which is important for protecting your privacy and security. One of the biggest benefits of VPNs for targeted individuals is that encrypts you traffic so that your internet service provider does not have a record of your internet activity.

This article provides a full description on VPNs. https://www.targetedtechtalk.com/2024/06/04/why-is-a-vpn-important-for-targeted-individuals/. This article also provides some additional details on VPN technology as well as a comparison with the Tor browser https://www.targetedtechtalk.com/2025/08/07/tor-versus-vpn/

Affordable Computing and Community Resources

Often targeted individuals face financial pressure that the general public does not face. Therefore it can be useful to identify strategies for obtaining affordable devices as well as free or cheap resources.

If you are looking for a discounted second hand computer or laptop, I have an article providing some good resources. https://www.targetedtechtalk.com/2025/02/24/guide-to-purchasing-a-budget-laptop-or-desktop/ To briefly summarize the article, recommended sites for refurbished computers would include BestBuy and Newegg. And you can often get a very good deal at your local thrift store. Often you can find deals starting as low as $150.

Another good resource in general is your local library. Often you can get free access to computers as part of a computer lab just by having a library card. Also review the resources available on their website, in addition to checking out books, libraries often also offer online services with your library card. This could include access to online training sites such as LinkedIn Learning, the ability to check out ebooks, electronic audiobooks and the ability to view some types of online shows and movies. Libraries often also have free or cheap classes that can be valuable such as basic computer skills. If you have a local community center, you may also want to check with them to see what classes and resources they offer.

Open Source Software

If you do a web search for “free software” you are often flooded with results that send you to sites filled with adware or otherwise sketchy results. But there are many legitimate sources of free software and most of the best are called “open source software”. This means that the source code, which is the computer code that makes up a program is available to everyone to use and extend. Often people volunteer their own time to develop and maintain these programs. But you don’t have to be a computer programmer to use an open source program. The finished programs are available for anyone to download.

So instead of looking for “free program x”, look for “open source x”. One example of an open source program I recommend would be Libre Office, which provides a desktop word processor, presentation tool, and spreadsheet tool, all of which can open files and save back to Microsoft Office format. https://www.targetedtechtalk.com/2025/02/17/libreoffice-free-open-source-office-suite/ I also did an article previously on the Tails operating system which is also open source. https://www.targetedtechtalk.com/2025/04/06/tails-operating-system-for-increased-online-privacy-and-security/

Password Managers

A simple 8 character password can be cracked in less than a couple hours. A complex 16+ character password could take a single computer millions of years to crack. This example highlights the importance of using a password manager. A password manager allows you to generate a unique complex password for every password you need. And I would strongly recommend that you create a unique password for each site. If a site’s passwords are exposed to hackers, you don’t want that one password in use with all of your accounts.

If you would like a good online password manager, I think the one included with Proton is fairly good, Proton pass. If you want a good offline password manager, I recommend KeePass. You can also find mobile apps compatible with KeePass. There are other password managers available , but these are my top picks currently.

External Backups

A good practice to get in would be doing a regular backup of external files. Many people choose to use an offline storage device. Having the ability to recover files from a backup can be important for many reasons. First, no computer lasts forever, so eventually one or more hardware components will fail and having a backup of important files can be very important. Also, computer and phones can be damaged intentionally or unintentionally by water damage, dropping, fire, theft or many other reasons. And your files or accounts could be hacked. With a ransomware attack they try to encrypt your entire hard drive and demand a ransom to unlock it. If you had a backup, you could recover. Likewise any sort of hacking attack could modify or delete files you need.

There are some pros and cons to offline backups. If you experience break-ins someone could gain a copy of your files from your backup. However in many instances of hacking, offline backups were the only effective way to protect important files from being damaged or altered.

If you’re interested in getting started with encryption for your files, I have additional details and recommendations in this article. https://www.targetedtechtalk.com/2024/08/06/drive-encryption-recommendation-veracrypt/

Hardwired Over Wifi

Where possible I would recommend the use of hardwired connections over the use of wireless connections such as Wifi and Bluetooth. This is really a continuation on the discussion of hardening. If you don’t use wireless connections then a wide range of wireless attacks cannot be used against your devices.

If you need to use wireless you might thing about separating your devices. For example, some targeted individuals find that Bluetooth based bone conduction headphones work well with the Dave Case audio therapy, so you might think about getting a cheaper stand-alone mp3 player rather than using your phone or computer. That way you isolate your Bluetooth usage to a stand-alone device rather than connect it to your primary devices.

Purchasing Electronics In Stores

One recommendation for targeted individuals is that where possible you can purchase electronics in stores. https://www.targetedtechtalk.com/2024/06/05/why-tis-may-wish-to-purchase-electronics-in-a-retail-store/ Making purchases in person very challenging for someone to alter or tamper with your electronics. It’s not always possible to avoid online purchases, many targeted individuals have reported problems with their purchases from Amazon.com.