COMPLETE EXPERT OPSEC SETUP

BY BAILOPAN

BAILOPAN@EXPLOIT.IM

BASIC COMPUTER SECURITY

What if one day your computer was ever stolen from your home, hotel room or rental car? What if it was borrowed by a friend of yours/family relative and lost or forgotten at school or on the bus? What if you were robbed and your backpack stolen? What if the police ever raided your home and took control of your digital devices to conduct a thorough investigation, that could potentially leave you in a dire situation, where you could face years in prison? What if any of a thousand scenarios occurred that resulted in you losing physical control, whether permanently or temporarily, of your computer? In any of these instances the new "owner" of the computer may try to take a look at your data. What will they find there?

On my fully encrypted Windows, Mac, and Linux laptops they would find nothing but a blank screen prompting them for a boot password. My entire hard drives, including the operating system, are encrypted and the devices will not boot without the correct password. Replace my computer with that of most users, and the answer is likely to be credit reports, medical documents, resumes, family photos, saved logins, credit cards, financial information, internet browsing history, hobbies, sexual affinities, criminal evidence, and much more. All of this information, can be used to harass, blackmail, extort, or further exploit you. It could be used to steal your identity, open lines of credit, or commit crimes in your name, leaving you to clean up the mess.

For any of us committing fraud and other similar criminal activities online, this information WILL be used in court to put you in jail for many years. Unfortunately, the US government has a reputation for not going easy on cyber-criminals and if you ever get caught, be sure they will do everything in their power to land you in jail for as many years as they possibly can.

Although basic security is boring, without we cannot rely on the more "advanced" security measures we discuss later in this tutorial. This chapter should serve as a good review of your baseline digital perimeter.

All of the techniques that will be presented in this tutorial, rely upon the assumption that you have a desktop computer that is reasonably secure and free of malware. If your computer is in any way, infected with malware, or is at risk for malware infection, you should fix this before continuing. Some of the most common forms of malware are Spyware, Key Loggers, Ransomware, and Scareware. Simple Google searches will explain you further about each of these viruses if you so wish to read more about it, I will not get into that.

WHICH OPERATING SYSTEM SHOULD I USE?

This is probably THE most important aspect of your security. If you are using an OS, which is closed-source, full of exploitable bugs and easy to hack into, then you are in for a lot of headache. I see a lot of cyber-criminals working with Windows and Mac, and let me tell you, this is absolutely wrong. If you want to be a criminal, then do your homework. Both of these operating systems are closed-source, which means only the developers of Microsoft and Apple are able to look and modify the code of the operating system. This is really bad because we don't know what kind of backdoors there may be in these operating systems. Law Enforcement agencies could very well have easy access to devices running these OSs. This was the case with Windows 8 recently, where it was found that NSA had a backdoor into it, which in turn allowed them to control and monitor any machine running the operating system. See where I'm going with this?

This is not the only problem with these operating systems. Windows is full of zero-day exploits, bugs, and every single day THOUSANDS of new viruses and exploits are deployed for the Windows OS. The reason for that is because the majority of the world population uses Windows, which means hackers can infect a lot more computers, and earn much more money with Windows than with any other OS.

Mac is definitely much more secure than Windows, and Apple has been firm in their stance to not cooperate with authorities. We've seen this recently when the FBI contacted them so they could build a backdoor into the iPhone OS and open the terrorist's iPhone and Apple refused. However, one common misconception I see a lot is that people think Mac computers are simply immune to viruses, and

that is completely wrong. Mac computers are as vulnerable to viruses as any other OS. They just have a much smaller user base than Windows, and so developing viruses and exploits for the Mac OS, is not even close to being profitable like it is with Windows machines. Windows machines are used everywhere, Macs are not. There are exploitable flaws in all operating systems and OS X is no exception.

For us cyber-criminals, the best operating system BY FAR, is Qubes OS. This operating system allows us to run isolated environments. It is basically a giant virtual box. You can run different OSs in Qubes as different virtual machines. For example, we have a virtual machine for the Whonix OS, another for Fedora, Debian, and those are only the VMs that come pre-installed with the OS. You can install Kali Linux in Qubes, Windows, and all kinds of different OSs. If one of these VMs ever get compromised by a virus, we are okay. We simply delete the VM and create a new one. If you want to learn more about the Qubes OS, then navigate to the link below, it is full of tutorials and even videos about the OS so you can get a good look at what we'll be working with.

https://www.qubes-os.org/doc/

Qubes has a very small compatibility range and so will not work with most computers unfortunately. However, if you want to become truly a professional cyber-criminal, then I highly recommend you invest in a new computer. Don't be lazy or close-fisted with security, as that will lead to problems and much headache for you in the future, trust me on that. Below are the laptops I recommend, from best (most expensive) to worst (cheapest). All of them work perfectly with the current Qubes 4.0. All of the prices were taken from Amazon at the time of this writing, so keep in mind, you may get cheaper, or more expensive.

LENOVO THINKPAD X1 CARBON 5TH GEN ($1845): This laptop is absolutely amazing, and if you have money to buy it, then do it. It's totally worth it, as it will last you for many years to come. This was voted the best business laptop at CES 2018. The performance of this laptop is absolutely incredible and will make your work incredibly smooth and easy. This is the laptop that I currently use and the one I recommend to all my clients on top of every other one.

LENOVO THINKPAD T460P ($1350): Also works perfectly with Qubes 4.0 and the performance is amazing. The one above is much better, but if you want to get this one instead and save some money, I'd say go ahead.

LENOVO THINKPAD T450S ($530): This laptop is also very good, although the performance of the above one is much better, this one does boast some impressive features. You can get it on Amazon for very cheap. It comes with i7 processor, 8GB RAM, 256GB SSD (you may want to upgrade the SSD). I have tested this computer with Qubes 4.0 and it also works perfectly and smooth.

LENOVO THINKPAD X230 ($235): This is a last resort type of laptop, and you should only get it if you're really low on money. The performance will be terrible, but definitely usable. Qubes 4.0 runs perfectly with it, and everything works exactly as it should, just really slow due to the old processor and low memory. If you're thinking of buying this laptop, keep in mind you will most likely need to upgrade some of the components to make it run smoothly.

CAMERA AND MICROPHONE

You should seriously consider physically disabling the camera on your computer. On machines that permit opening of the case, I prefer to physically disconnect cameras and microphones to ensure they are not being eavesdropped upon. In the case of laptops, this means opening the case and physically severing connections to the camera and microphone. This may sound like an extreme measure, but software protections like disabling the microphone or turning on a light when the camera is on can be overridden by sufficiently sophisticated spyware. Disabling the hardware is the only sure defense, but I realize that the vast majority of individuals will not take it this far. At a minimum, I recommend blocking the camera with tape, a post-it note, or a dedicated sticker.

PHYSICAL SECURITY

With physical access to your device, there are a number of attacks that may be carried out successfully against your computer. This includes the “Evil Maid” bootloader attack to capture your full disk encryption password. USB or optical media attacks work by bypassing your OS password, or the installation of hardware key loggers that cannot be detected by antivirus applications. Though I will not get much in-depth into this, I will give you some basic suggestions to secure yourself against these type of attacks.

I strongly recommend that you carefully control the physical access to your computer, especially when traveling. Though it would be possible for someone to covertly enter your home and exploit your computer, it is not very likely. It is much more likely when traveling, so be especially cautious in hotel rooms. Even though you have locked the door, hotel doors and locks are susceptible to dozens of defeats, not to mention the fact that management, housekeeping, and maintenance all have operating keys to your room. Do not walk away from your computer to go to the restroom in a coffee shop. Do not leave it in your rental car, and do not leave it sitting in the conference room when you break for lunch. If you must leave it unattended in a hotel room or elsewhere, take the following physical security precautions:

- Turn off ALL interfaces including Wi-Fi and Bluetooth.
- Ensure your computer is full-disk encrypted and completely shut down
- Remove all external media including CDs/DVDs, SD cards, USB drives, external HDDs, etc. and take them with you.
- Take any transmitting devices, such as a wireless mouse and its dongle, with you when you leave
- Store your computer inside of a safe.

All of these precautions will give you a fighting chance. However, against a very skilled adversary, they cannot guarantee your computer’s security. Again, the absolute best practice is to avoid relinquishing physical control of your devices.

OS UPDATES

Keeping your operating system up to date is one of the most important steps in securing a computer. As software ages, security holes are discovered in it, and attacks are written to take advantage of these holes. Though software updates are occasionally released to add features and to deal with bugs, they are often written specifically to patch security holes. If your software is outdated, it is vulnerable to holes that are, in addition to everything else, well-publicized by virtue of the fact that a patch exists to fix them.

In Qubes OS, you should check for updates on all of your TemplateVMs and dom0 on a DAILY basis. This should take no more than 30 minutes if no major updates were released.

APPLICATION UPDATES

Just as vulnerabilities in the operating system may be exploited, security holes in your installed programs can be used as attack vectors. It is important to keep all software up to date. It is also extremely important to limit the number of installed applications on your device to an absolute minimum. Each application represents potential undiscovered security flaws. I recommend scrubbing your list of installed applications every three months and uninstalling anything you have not used during the previous three-month period.

WEB BROWSER SECURITY

Your internet browser serves as your computer's ambassador to the internet. How it presents itself to the websites you visit and their third-party advertisers will, to some extent, influence how those sites and advertisers will behave in return. More importantly, the setup of your browser will certainly dictate what browsing information your computer stores. Setting up your browser is an important step in controlling your virtual security perimeter and protecting your personal privacy.

The first browser setup we will look at is for the protection of your privacy, and so we will try to limit as much as we can the information that is collected from your browsing sessions. If you wish to look at a browser setup for fraud related activities, then I will discuss that at the end of this chapter. I wouldn't skip this one though as it is very important for using the web normally, when you are not doing anything fraudulent.

THE THREATS

COOKIES: These are perhaps the most common means through which your browsing sessions are tracked. Cookies are small pieces of data placed on your computer by the websites you visit. They are placed there to be helpful. Cookies remember which links you have clicked, the products you have looked at, and sometimes your login information. You may be already logged in when you visit a page again. Accepting cookies is almost always required to complete a purchase or other transaction on a webpage. If your browser won't accept a cookie, the site you are visiting cannot remember what items are in your cart.

Unfortunately, cookies are capable of doing much more than remembering which videos you have previously viewed on a website. Cookies can also be used to spy on you. Third-party cookies are not placed on your machine by each site you visit, but by a third-party that is partnered with the "host" site. They are purely for analytical purposes and track your browsing from site to site. Some popular websites may allow as many as 40 third party cookies to be installed when you visit their site. Each one of these can record your username, account name, IP address (which can be resolved to your physical location), and each site that you visit. All of this can be used to create a comprehensive picture detailing your online activity.

Making matters worse, these cookies are also very persistent. Cookies are usually designed to last 90 days before they expire (some last longer). During the entire 90-day period the cookie may be used to track you. If you revisit the site where you got the cookie, a new one is installed and the 90-day clock resets. In this way cookies can be used to track users more or less over a lifetime.

I personally recommend clearing cookies frequently and never accepting third-party cookies.

BROWSER FINGERPRINTING: This is the process of identifying enough specific characteristics about a browser to make it unique or nearly unique. Though this fingerprint may not positively identify you, it can be used to create a very comprehensive picture of what content you frequent. If you have been, or subsequently are, positively identified, this information can be directly correlated to you.

The factors used to fingerprint a browser are many, and most of the reasons they are requested are legitimate. The sites you are visiting must know some of this information to allow sites to present and function properly with your device. These factors include your screen size and resolution, the fonts you have installed on your device, the time zone to which your computer is set, any add-ons that you have installed, cookie settings, and your browser and operating system details.

Browser fingerprinting is an extremely dangerous form of tracking because it is very difficult to defeat. While you can refuse to accept cookies it is very difficult to change your screen resolution. I will give you some advices to offer some light protection against this form of tracking. The EFF foundations has an excellent browser fingerprinting tool that will tell you how unique your browser is, as well as an excellent white-paper on the topic. I will leave the link to it below.

https://panopticlick.eff.org

WHICH BROWSER SHOULD I USE FOR PRIVACY?

If you wish to setup a browser for maximum security and privacy, I recommend Firefox. The reason for that is, Firefox offers the greatest control over security and privacy settings, and there are numerous add-ons for it that can harden the security of your browser.

The first and most basic step you should take is to ensure your browser is up to date. Outdated browsers with security holes are an extremely common attack vector. Browser updates are issued frequently to patch these vulnerabilities as they are discovered. Once you have ensured your browser is up to date, some settings must be modified to ensure the greatest possible privacy and security. Go to the Firefox Options and change the settings below.

- Change your homepage to https://google.com. Millions of people use this as their homepage and it is completely non-alerting.
- Change the downloaded files location from the "Downloads" folder to an encrypted location.
- Under Privacy, turn off do not track. Websites have absolutely no obligation to honor your requests, and in fact, they rarely do. We will take much more aggressive steps to ensure we are not being tracked. However, you may elect to tell sites that you do not wish to be tracked if you so wish.
- Under History, select "Use custom settings for history" from the pull-down menu. Then, uncheck "Always use private browsing mode" and "Remember my browsing and download history" and "Remember search and form history". This will prevent Firefox from remembering any history after your browsing session has closed.
- Next, still under History, check the box that says "Accept cookies from sites". This will allow cookies from the websites you visit. Without cookies, it is very difficult to make purchases, use online streaming services, or enjoy many of the other potential benefits of the internet. Though accepting cookies is not ideal, we will take steps to get rid of them upon closing Firefox. Next, under the "Accept cookies from third-party sites" drop-down, select "Never". Third-party sites are sites that you have not visited but that are still attempting to track internet usage for marketing purposes. There is no need to accept their cookies since you have not visited these websites. Under "Keep until" (which refers to how long cookies are retained), select "I close Firefox". By default, cookies may last 30, 60, or as long as 90 days, and may track your browsing sessions throughout that entire period. This option will ensure they are not saved after your browsing session has ended. After that, check the box that says "Clear history when Firefox closes".

- Before moving on click the “Settings” box to the right. This will bring up an entirely new dialogue that gives you very granular control of the items that Firefox clears upon closing. They are Browsing and Download History, Active Logins, Form & Search History, Cookies, Cache, Saved Passwords, Site Preferences, and Offline Website Data. Select all of them and click OK to close the dialogue. Finally, under “Location Bar” uncheck History, Bookmarks, and Open Tabs.
- Under Security check “Warn me when sites try to install add-ons” box. Next, deselect both the “Block reported attack sites” and “Block reported web forgeries” options. Both of these options could allow Firefox to track your web activity by sending the sites you visit to Mozilla for vetting against a whitelist. Though I don’t personally distrust Mozilla or Firefox, I still prefer to send them as little information about my browsing sessions as possible. Finally, deselect the “Remember passwords for sites” and “Use a master password”.

FIREFOX ABOUT:CONFIG

Go to the address bar, and type about:config. This will open a menu where power-users can make many adjustments to the application. Bypass the warning, and look for these values, change them accordingly.

media.peerconnection.enabled – SET IT TO FALSE
network.prefetch-next – SET IT TO FALSE
network.http.sendRefererHeader – SET IT TO TRUE
browser.send_pings – SET IT TO FALSE
beacon.enabled – SET IT TO FALSE
geo.enabled – SET IT TO FALSE
webgl.disabled – SET IT TO TRUE
pdfjs.disabled – SET IT TO TRUE
plugins.notifymissingflash – SET IT TO FALSE
security.cert_pinning.enforcement_level – SET IT TO 1
network.IDN_show_punycode – SET IT TO TRUE

FIREFOX ADD-ONS

Add-ons are small programs that can be added to Firefox. There are thousands of add-ons for Firefox and most of them are not designed to enhance your privacy or security. The add-ons listed here make Firefox more private and more secure, make it more difficult for your browsing history to be tracked, and reduce the possibility of certain types of malicious attacks successfully targeting you. I won't get much in-depth into each one of them, I will just list them here, if you wish to read more about each one of them and their features, look them up on Google. I recommend you install each one of these on your browser for maximum privacy. DO NOT USE THESE FOR FRAUD ACTIVITIES, AS THAT WILL 100% LEAD TO A DECLINED TRANSACTION. FRAUD BROWSER SETUP IS AT THE END OF THIS CHAPTER.

- NO-SCRIPT
- HTTPS EVERYWHERE
- UBLOCK ORIGIN
- COOKIE AUTODELETE
- USER-AGENT SWITCHER
- CANVASBLOCKER

TOR BROWSER

Though it is nearly impossible to be completely anonymous online, Tor is as close as you can get. No discussion of online privacy would be complete without a thorough discussion of Tor. Tor prevents your internet service provider, third-party advertisers and trackers, and even governments from seeing what you're up to online. Tor is typically demonized in the media as a tool for terrorists and criminals, but hypocritically enough, it was originally developed by the US Navy.

I will give you a brief explanation of the more technical aspects of how Tor provides the anonymity it offers. When using the Tor browser, the traffic you request is not sent straight to and from the website you wish to visit. Instead, Tor makes your traffic anonymous by routing it through three intermediary servers

(called nodes) prior to sending the request to the desired website. When you first open Tor Browser, a connection is made with a server (called a directory server) that receives your request. This server will then build your custom network. Traffic is encrypted from the user device, through the network, and is only fully decrypted when it leaves the network en route to its intended destination.

Your traffic is heavily encrypted within the Tor Network, which also contributes to your anonymity. When your request leaves your computer it is encrypted three times. The first node at which it arrives (called the “entry guard”) can see that it came from you. Upon removing the first layer of encryption, it can “see” the next node, it can see the node it was sent from and the node it will forward to, though it cannot tell that the request originated with you, or where the request is ultimately being sent. When your request arrives at the exit node the last layer of encryption is removed and your request is transmitted to its final destination. When your traffic is returned it is routed through the same network.

TOR DISADVANTAGES: Even though I believe strongly in both the philosophical mission of Tor and in the technical implementation of the browser bundle, I would be remiss if I did not mention the disadvantages of using Tor, and its vulnerabilities. The first disadvantage to most people is Tor is inconvenient. By routing all your traffic through three intermediate servers prior to sending it to its destination Tor traffic is much slower than “normal” traffic. Each of the computers through which your traffic is routed may be much slower than your own, and so may be their individual internet connections.

Another major disadvantage is that some sites disallow logins, account creation, or other transactions from the Tor network. Further, many sites will require multiple captcha entries and are generally unfriendly to Tor. As I will say many times, CONVENIENCE AND SECURITY ARE INVERSELY PROPORTIONAL. I believe the slight inconveniences of Tor are more than made up for by the privacy and security it offers. Even though Tor is very secure, it is still not vulnerable.

Finally, Tor creates a very distinctive signature. Packets sent over the Tor network look very different from “normal” internet traffic. I believe this elevates your

profile and makes you more “interesting” than non-Tor users. You should seriously consider using a obfs4 Tor bridge to hide your use of the Tor network from your ISP, and even from your VPN provider as well.

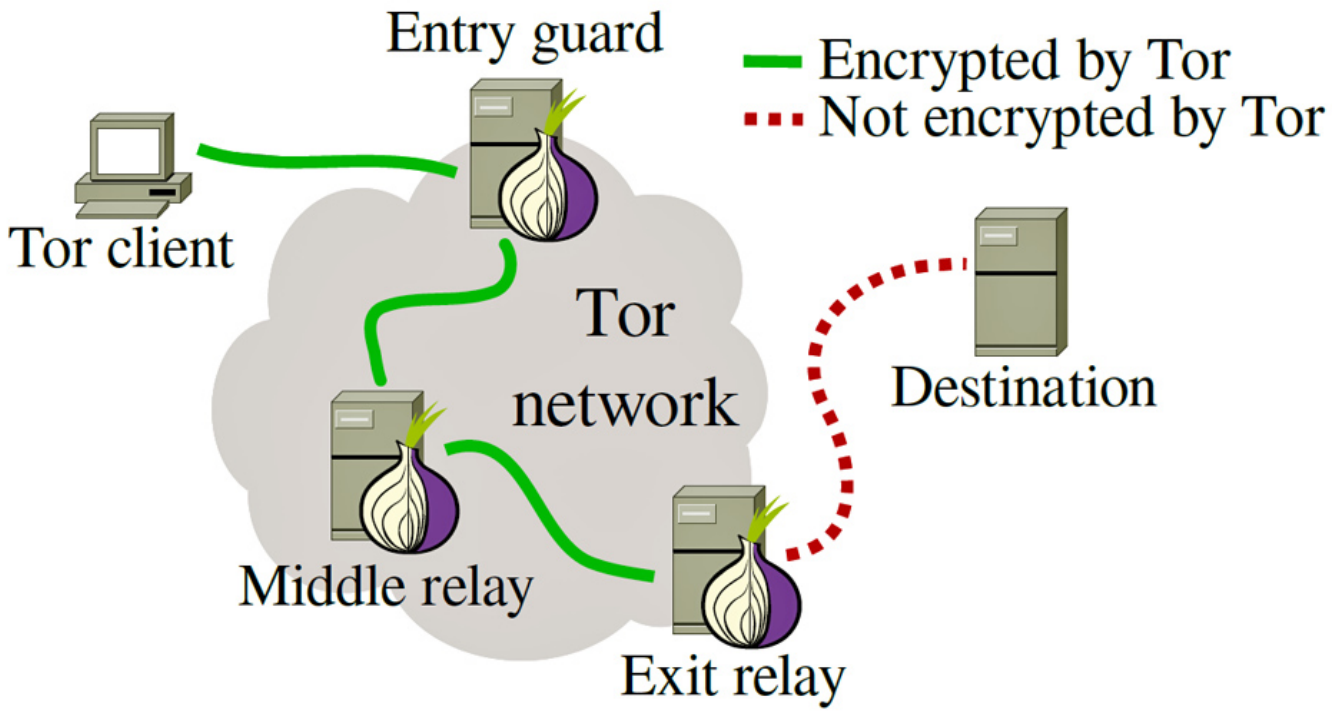


Figure 2.1: A typical Tor circuit. After the directory server creates the network the user’s traffic is routed through three intermediary servers, each of which can only see one node in either direction. This prevents any one node from seeing both the requested websites and the requestor and prevents the destination website from seeing who made the request.

TOR VULNERABILITIES: All the Tor servers used to re-route communications are hosted by volunteers. The host of the final server your communications are routed through can monitor any transmissions that exit Tor in plaintext though it would still theoretically be anonymous. This is why Tor places such emphasis on the HTTPS Everywhere add-on. When your traffic leaves the exit node it will still be encrypted with the TLS protocol if so supported by the website. This will prevent your traffic from being monitored by a malicious exit node.

You should also be aware that Tor is extensively monitored by law enforcement and intelligence agencies (both domestic and foreign) that may, under some circumstances, be able to observe your traffic. Tor is not a perfect solution and is vulnerable to some types of exploits. Your anonymity can be compromised on Tor in any of several different ways. For example, if you make a purchase on Tor using your credit card or other financial information that is linked to your true identity your anonymity will be breached. Further, Tor may also raise your profile.

Likewise, if you log into an email, social media, ecommerce, or other site that is associated with your name, your true identity will be associated with that entire browsing session. Opening a downloaded document while still connected to the internet is one of the most prevalent ways in which anonymity of Tor is broken.

Further, if you make any modifications to your version of Tor Browser it may be fingerprinted. This fingerprint can track you around the internet and eventually reveal your true identity. The default Tor Browser is designed to prevent browser fingerprinting. It discourages you from installing add-ons, and it makes all versions, regardless of download location, exactly the same. It even warns you not to maximize the browser which can reveal your computer's full screen size and resolution. Any modification can make your version of Tor Browser absolutely unique and make you trackable. There are many other ways that the veil of anonymity Tor provides can be pierced. To be truly anonymous takes extraordinary effort.

Even if you are using Tor "perfectly" and adhere to all best practices, your anonymity may still be compromised by adversaries with worldwide reach (US Government for example). Such adversaries can correlate the time between a Tor connection being established and the location from which it was established to determine a user's true identity.

BROWSING PRIVACY BEST PRACTICES

DON'T STAY LOGGED IN: When you are logged into your email or social media account, these services monitor everything you do on the internet. Not only do social media accounts log your "likes" and "tweets", they also record other sites you go to, accounts that you create, things you purchase, videos you watch, songs you download, appointments you make online, and a wealth of other information. Many people like to remain logged into their Gmail or other accounts constantly because of the convenience it affords. This convenience can be compromising to privacy.

While it is much more work (privacy is neither easy nor convenient), I recommend the following. If you need to check your Gmail, Facebook, or other account that is associated with your name, close your browser and clean it as described below. After you have done this, open your browser, log in, and conduct your business. While you are logged in do not visit any other sites or log into any other accounts. When you have finished, log out of the site, close your browser, and clean your system again.

CLOSE AND CLEAN: I strongly recommend closing your browser between sessions. It is especially important to close your browser after visiting a website to which you have logged in, such as an email or social media account so that all browsing history and cookies are deleted. Simply logging out of the website will not delete the cookies it placed on your computer, and the site will still be able to track your movements around the internet. Though this is not an absolute measure of protection from tracking it does break your data down into smaller pieces. If you never clear your system you are creating a month or year long record of every website you have visited on the internet, and sharing it with hundreds of other parties.

I recommend also cleaning your system between sessions. I recommend using Bleachbit and CCleaner if you are running Windows. These programs will thoroughly delete all browsing history including your internet cache, cookies, download history and location, session history, compact databases, and more.

BE CAREFUL WHAT WEBSITES YOU VISIT: The beauty of the internet is that it puts the world at your fingertips. Any interest you have can likely be explored and expounded upon on the internet. Many of these sites do not have your best interest in mind and care little about your security or privacy. Websites are commonly used as attack vectors for malware, to track your browsing habits, or to get personal information from you. Thoughtfulness is required when browsing the internet. Pornography websites are notorious as being attack vectors for malware. Clicking on the wrong link on a porn site can quickly lead to adware, nagware, ransomware, or worse. Porn websites are not alone in this. Be careful about the websites you visit. Pause and ask yourself two questions when any site is full of pop-ups. Does clicking a link on the site cause a new, unrelated window to open? Does the site cleverly conceal links that end up opening lots of new windows? If the answer to either of these questions is yes, the site is probably one you should avoid.

DO NOT CLICK ADS: Malvertising is an extremely sophisticated attack vector. This threat alone should be enough to dissuade you from clicking on online advertisements. If this isn't enough to convince you, also consider the fact that even the most benign of these ads will still track your browsing session.

DO NOT IGNORE WARNINGS: If you visit a website and receive a warning from your browser, or from a browser extension like NoScript, it is probably a good idea to skip that site.

DO NOT DOWNLOAD FROM UNTRUSTED SITES: Be very careful about the sites from which you download files and applications. Though torrent sites are fun and many people use them to get free media, they are also rife with malware.

USE CARE WHEN DOWNLOADING APPLICATIONS: When downloading applications, you should always use extreme care. Applications can contain extensive malicious payload, and attention should be paid to the quality of the download you are getting. If at all possible, attempt to download programs directly from their source, and check their signatures before running to ensure you are getting exactly what you want, and not some malicious file.

BROWSER SETUP FOR FRAUD ACTIVITY

Now to setup our browser to conduct fraudulent transactions, we must first take into account the fact that we want to appear as legit as possible. We want the website we are visiting to think we are a common browser user, with common browser settings and a common browser fingerprint. You don't want any under circumstances more than one or two of the most used add-ons, and not much should be changed on browser settings either.

Our solution to all of this is using a clean hacked RDP. We simply install Firefox or Chrome on that RDP, don't change any settings, go to the website we want to conduct the fraudulent activity in, and do our magic. That is it. If you want an extra security measure, then just go to about:config and change these 2 settings below.

media.peerconnection.enabled – SET IT TO FALSE
webgl.disabled – SET IT TO TRUE

Once you are done carding 1 specific website, don't ever use that same RDP again for the same website, trash the RDP and move on to another clean hacked one if you want to card the same website. You can use the same hacked RDP for multiple websites, but not more than once if you want your success rate to be high.

With hacked RDPs, we do not have to worry about canvas or browser fingerprinting, since that is not our real machine and any data the website is able to get about that machine will be useless in an investigation. Unless you are connecting to that RDP using your REAL IP. In that case, you are extremely dumb and will most likely get caught. ALWAYS USE A VPN, OR EVEN BETTER, A CHAIN OF 2 VPNs, Tor and Socks5.

Now let's move on.

ONLINE ACCOUNT SECURITY

It has been suggested that the strongest password is the one you don't know. Humans are notoriously poor at developing effective passwords because we are limited largely by the constraints of memory and the desire for convenience. Later in this chapter I will teach you how to create effective, difficult-to-crack passwords that are still memorable and usable. I recommend you use a different username and password on all of your online accounts. This may seem terribly difficult, exceedingly inconvenient, and impossible to remember, and generally I would agree. With only the benefit of human memory it would be nearly impossible to remember and use more than just a few passwords of the recommended length and complexity. For that reason, I've chosen to begin this chapter with a discussion of password managers, one of the single biggest and most important tools you can employ to strengthen your digital security posture.

I have been using password managers for years, and there's no way I'd even consider the possibility of going back to not using one. A password manager is a purpose-built application that creates an encrypted database for storing and organizing your usernames and passwords. Password managers solve many of the problems inherent in password development and use by "remembering" your passwords for you so that you don't have to. This allows you to easily implement the online account best practices of using a different username and password on every one of your online accounts, using passwords that are randomly generated and of the maximum allowable length and complexity, and changing them as often as you deem prudent without fear of forgetting them.

Because password managers store all your passwords in one place, they create an "eggs-in-one-basket" situation. It should go without saying that a password manager should be protected by an extremely strong password, and if at all possible, two-factor authentication. If you can only take the time to remember one very strong, very complex password, you should do so for your password manager. Be especially careful not to lose or forget this password.

Password managers are designed to not let you back in without the correct authentication credentials. This could result in the loss of all passwords for all your accounts, an unenviable situation in which to find yourself. It should also go without saying that your password manager should be backed up, frequently. If you are using a host-based manager and your computer crashes, you must have a way to recover the information the password manager contained. Otherwise you risk being locked out of, and potentially losing, hundreds of accounts.

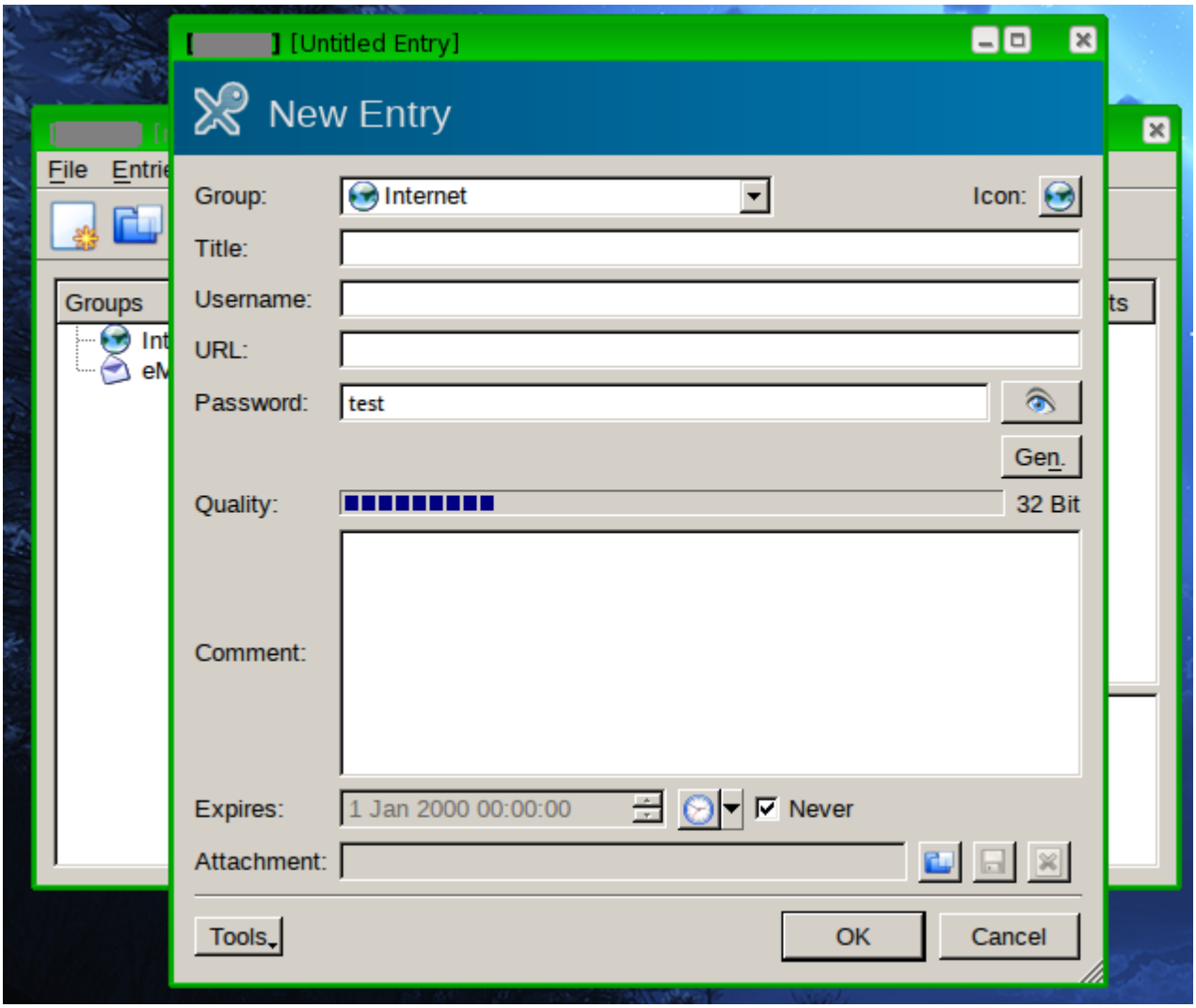
There are two basic categories of password managers, host-based and web-based. Although I will discuss both, my recommendation is to only use host-based password managers. While web-based password managers are strongly encrypted, they are significantly riskier because they store your passwords in the cloud on machines that you do not personally control. Further, online password databases are a natural target for hackers because of the wealth of information they contain. Though a certain amount of confidence is placed in all online account providers, an extraordinary amount is required to entrust your passwords to all your accounts to an online service. I have not found yet an online service to which I am ready to give this level of trust for my extremely sensitive accounts, and frankly don't believe I ever will.

HOST-BASED PASSWORD MANAGERS

A host-based password manager is an application that runs locally on a single device. All the information that is stored in a host-based password manager is stored only on that device and is not sent to the cloud or otherwise transmitted. This is somewhat less convenient than a web-based password manager as your passwords are only available on your computer or device. As a result, you may not be able to log into your online accounts from computers other than the ones you own and that store your password database. This is not an issue for me since I'm reluctant to log into an account from a computer that I don't control and therefore don't trust. However, there are good reasons to use a host-based password manager. The biggest advantage host-based managers enjoy over web-based password managers is security. I have an instinctual, inherent distrust in cloud storage, and prefer to keep all my password, stored safely on my own devices.

QUBES OS: KEEPASSX

KeePassX is by far my favorite open-source host-based password manager for Linux machines, and it comes pre-installed on Qubes, on the Debian VMs. I recommend you create a new database on a VM labeled “vault” with KeePassX, and to further enhance your security, store that database inside a hidden veracrypt container with a strong password. It’s as simple as downloading the .tar.bz2 file from the veracrypt website, decompressing it, and running a bash command on the folder to install veracrypt. If you’re having difficulty doing this, feel free to contact me and I will help you with that.



Picture 2.1: KeePassX has a very friendly and easy-to-use user interface. It allows us to create passwords of up to 1000 characters, add URL, and comments to entry.

GLOBAL PASSWORD POLICIES

Regardless of which password manager you choose, I recommend defining global password policies. These policies allow you to quickly choose from a predefined length and character set for given websites. There may still be occasions when you have to build a custom, per-entry policy but these instances should be rare. I recommend building the global policies listed in the table below.

Policy	Length	Character Set	Uses
Standard Policy	60+	ALL	Most websites and logins
Long Policy	99+	ALL	Sites allowing very long passwords
Short Policy (or policies)	12-32	Customized to site restrictions	Sites disallowing very long passwords; sites disallowing the use of certain characters in passwords. I recommend creating a custom policy for each site with such restrictions and using it ONLY on that site
Username Policy	24	Uppercase letters and numbers only	Creating random usernames for sites where user-selected usernames are allowed (see section below on Usernames)

USERNAMES

With password managers to keep up with all of your login information, it is now possible to elevate your security posture significantly without a corresponding increase in the amount of work required. Generally, usernames are completely overlooked in the discussion of online security. I think this is a huge mistake. I believe that usernames should be considered the very first line of defense for such accounts. Most websites require at least two things to log in: a username and a password. If the attacker cannot find your username, your account I significantly

more secure. To launch an attack against your account would require first finding your account and an obscure username greatly reduces the chances of this happening.

A predictable username has several problems, the first of which is susceptibility to guessing. If an attacker is targeting an attack against a specific individual, he or she will attempt to guess the target's username(s) to various sites. The attacker will base guesses on known information about that person. This information can be gathered online from social media sites, personal blogs, people search sites, and public records. Predictable usernames are most commonly generated from a combination of first, middle, and last names. For example, if your name is Amy Schumer your username might be "ABSchumer". Sometimes they are combinations of monikers or initials and dates of birth such as "chumer81". Once the username has been discovered the attacker can now target that account and attempt to break the password. Conversely, the attacker can never begin targeting the account if it cannot be located.

The second problem with predictable usernames is that they are typically used across multiple websites, especially when the email address associated with the account is used as the username. Using the same username across several of your accounts correlates those accounts. This makes them easier to locate and leaks information about you such as your social media presence, interests, the online services and commerce sites you use, etc. This can expose a great deal of information about you. After locating your username, the attacker in this scenario may use a service like KnowEm (http://knowem.com/) to locate other accounts you have. If a common username and password combination are used across multiple accounts, hacking one account can very quickly lead to the compromise of multiple accounts with disastrous consequences. Though you may not care if your throwaway email account or an old social media profile is hacked, it could lead to your bank account or an active e-commerce account being hacked if they share a username and password.

The third major problem with predictable usernames is that when breaches occur, the username and password combinations are usually sold or posted online in

massive databases. If you use a username or email address that correlates to your name, a breach can reveal personal information about you, especially if you have an uncommon name. As an example, let's assume your name is Harrison Tang and your username to a site is harrisontang83, an obvious and easily guessable username based on your name and year of birth. Let's also assume that a large password breach occurs at a given site, and the usernames and passwords are posted online (which is very common by the way). Anyone seeing this database would easily recognize your name and with some research could probably confirm the user is you. This reveals information about you and your personal interests. This could be a dating site (like Adult Friend Finder or Ashley Madison), a bank, an ecommerce site, or an online service of some sort. This would reveal to anyone seeing this database that you use this dating site, bank, online retailer, or service, leading to further avenues of exploitation.

To combat this, you should consider the username a security measure. If the usernames on your accounts happen to be obvious, change them immediately. If a particular site does not allow you to change your username, consider closing the account and opening a new one using a non-obvious username. I'd personally consider a random-generated username for maximum anonymity. An ideal username would look something like this: 532T4VYL9NQ54BTMDZI1.

PASSWORDS

Though password managers provide most of the memory you need, there are still a handful of passwords that you will need to manually enter on a day-to-day basis. Not only do you want these passwords to be memorable, you also need them to be incredibly strong as the compromise of these passwords could lead to the compromise of all of your sensitive data. For this reason, you need to know how to develop a strong password that you can remember and enter manually.

PASSWORD BASICS: Before I discuss how to build a good, strong password it is critical to understand what comprises one. There are two factors that make (or break) a password: length and complexity. Added length and complexity both exponentially increase the difficulty in breaking a password.

Password length is uncomplicated. With today's computing power, 20 characters is a prudent MINIMUM length (if your site does not allow a longer password). When passwords are cracked using brute force techniques, powerful processors run through hundreds of millions or billions of possible passwords per second. Every possible combination of a very short password could be tested in a matter of minutes with strong enough computing power, and computers are growing faster every day. Password length is the single most important factor that increases the strength of a password.

When using a password manager, we will use passwords that are much longer than 20 characters, sometimes exceeding 100. If this seems like overkill, consider the following. Regardless of whether a password is 1 character or 100, both require the exact same amount of effort when using a password manager. Why not go with the longest allowable password? If a site with which you are registering does not allow a longer password, think twice before registering with that service.

Complexity can be a bit trickier. Password complexity is created by following some basic rules. Ideally a password will contain characters from the full ASCII suite, including upper and lower-case letters, numbers, special characters (!@#$%^&* +=-/.,<>?;"":[]}{\|), and spaces. Spaces are very important as they are not commonly used in passwords, and as a result are not commonly searched for by password-cracking programs.

PASSWORD VULNERABILITIES: You may be wondering why such extreme measures are needed to develop an effective password. The reason complexity is desirable is that passwords are not typically cracked by "dumb" brute force methods alone, like starting at lowercase "a" and going all the way through "ZZZZZZZZZZ", and testing everything in between.

Though brute-force attacks exist, they are not the most popular or effective method of cracking a password, as they can take an immense amount of time. Time is the enemy of the password cracker, and your goal in designing a password should not be to make it unbreakable. Nothing is truly unbreakable given enough time, but you should aim to make it take an unacceptable length of time. Passwords are usually cracked in a much timelier manner by understanding how people make passwords and designing a dictionary attack to defeat it. Dictionary attacks rely on specific knowledge of the target and heuristics.

Knowledge of the target is useful when cracking a password because personal information is frequently used as the basis for human-generated passwords. An individual may use his or her birthday (or birthdays of a spouse, or children, or a combination thereof), favorite sports team or player, or other personal information or interests. This information can be input into programs like the Common User Password Profiler (CUPP). This application takes such tedious personal data as birthdays, names, occupation, and other keywords, and generates thousands of potential passwords based on the data. This list of passwords can then be programmed into a custom dictionary attack against the target machine or account.

Dictionary attacks work through a trial and error approach. First, a list of passwords is entered into a password-cracking program. This list might be customized against the target (through applications like CUPP as described above), or it may be more generic. Even though “generic” lists are not tailored to a specific target, they are still far more successful than they should be. These lists are based upon the heuristics of how people develop passwords. These lists are developed with the knowledge that many people use the techniques explained in the following list of password pitfalls.

- Never use a dictionary word as your password. Almost all dictionary attacks will include a list of dictionary words in a number of languages.
- Do not use a dictionary word with numbers/characters at the beginning or end (e.g. password11 or 11password), and do not use a dictionary word with simple obfuscation (p@ssword). These are the most common methods of

adding complexity to a dictionary word-based password, and combinations such as these would be tested in any decent dictionary attack.

- Never leave the default password on your devices (Bluetooth devices and wireless routers are notable offenders in the retail market). Default passwords for any device imaginable are available through a simple web search and would absolutely be included in an attack against a known device.
- Never use information that is personally relatable to you. As I have discussed, information that is personally relatable to you can be used in an attack that is customized to target you specifically.

The inherent problem with complexity is that it makes our passwords difficult to remember, though with creativity it is still possible to create passwords that are very long, very complex, yet still memorable. Below are two of my favorite techniques to develop strong (and memorable) passwords.

THE PASSPHRASE: A passphrase is a short phrase instead of a single word and is my preferred technique. Passphrases work like passwords but are much more difficult to break due to their extreme length. Additionally, if appropriate punctuation is used, a passphrase will contain complexity with upper and lower-case letters and spaces. A shrewd passphrase designer could even devise a phrase that contains numbers and special characters. An example of a solid passphrase might be the following.

“There’s always money in the banana stand!”

An even better example might be:

“We were married on 07/10/09 on Revere Beach”.

Both of those passphrases are extremely strong and would take a long, long time to break. The first one contains 43 characters, including letters in upper and lower-cases, special characters, and spaces. The second is even longer at 46 characters, and it contains numbers in addition to having all the characteristics of the first. Additionally, neither of these passphrases would be terribly difficult to remember.

DICEWARE PASSPHRASES: Diceware is a method of creating secure, randomly-generated passphrases using a set of dice to create entropy. To create a diceware passphrase you will need one dice and a diceware word list. Numerous diceware word lists are available online. Because of the way passwords are created, these lists do not need to be kept secret. These lists consist of 7,776 five-digit numbers, each with an accompanying word and look like this:

43612 noisy
43613 nolan
43614 noll
43615 nolo
43616 nomad
43621 non
43622 nonce
43623 none
43624 nook
43625 noon
43626 noose

After you have acquired a dice and a word list, you can begin creating a passphrase by rolling the dice and recording the result. Do this five times. The five numbers that you recorded will correspond with a word on the diceware list. This is the first word in your passphrase. You must repeat this process for every additional word you wish to add to your passphrase. For an eight-word passphrase you will have to roll the dice 40 times. Diceware passwords are incredibly strong but also enjoy the benefit of being incredibly easy to remember. A resulting diceware passphrase may look like the following.

puma visor closet fob angelo bottle timid taxi fjord baggy

Consisting of ten short words, this passphrase contains 58 characters including spaces and would not be overly difficult to remember. After you have completed this and compiled the words from the list into a passphrase you can add even more entropy to the passphrase by capitalizing certain words, inserting numbers

and special characters, and adding spaces. Experts currently recommend that six words be used in a diceware passphrase for standard-security applications, with more words added for higher-security purposes. You should NEVER use a digital or online dice-roll simulator for this. If it is compromised or in any way insecure, so is your new passphrase. Wordlists are at http://world.std.com/~reinhold/diceware.html

THE "FIRST LETTER" METHOD: This method is a great way to develop a complex password, especially if it does not have to be terribly long (or cannot be because of site restrictions on password length). For this method select a phrase or lyric that is memorable only to you. Take the first (or last) letter of each word to form your password. In the example below, we use a few words from the Preamble to the Constitution of the United States.

We the people of the United States, in order to form a more perfect union, establish Justice, insure domestic Tranquility

WtpotUSiotfampueJidT

This password contains 20 characters, upper and lowercase letters (the letters that are actually capitalized in the Preamble are capitalized in the password), and does not in any way resemble a dictionary word. This would be a very robust password. The complexity and length of this password could be increased greatly by spelling out a couple of the words in the phrase, and more complex still by replacing a letter or two with special symbols as in the following example.

We the People of the United States, i02famPu,eJ,idT

Containing 51 characters, this is the strongest password yet, but would still be fairly easy to remember after taking some time to commit it to memory. The first seven words are spelled out and punctuated correctly, and the last fifteen words are represented only by a first letter, some of which are substituted with a special character of number. This password is very long and very complex, and would take EONS to crack with current computing power.

OTHER PASSWORD ISSUES

Even if all your passwords are strong, there are some other issues to be aware of.

MULTIPLE ACCOUNTS: Though this is covered elsewhere in this book it is worth reiterating. Each of your online accounts should have its own unique password that is not used on any other account. Otherwise the compromise of one account can lead quickly to the compromise of many of your accounts. If a password manager is doing all the work for you there is no reason not to have different passwords on every single online account.

PASSWORD RESET MECHANISMS: Most online accounts feature a password recovery option for use in case you forget your password. Though these are sometimes referred to as "security" questions, in reality they are convenience questions for forgetful users. Numerous accounts have been hacked by guessing the answers to security questions or answering them correctly based on open source research, including the Yahoo Mail account of former Vice Presidential candidate Sarah Palin. The best way to answer these questions is with a randomly generated series of letters, numbers, and special characters (if numbers and special characters are allowed). This will make your account far more difficult to breach through the password-reset questions. If you use a password manager, the answers to these questions can be stored in the "Comments" section of each entry, allowing you to reset your password in the event you become locked out of your account.

If you are prompted to enter a password "hint", I recommend using purposely misleading information. This will send the attacker on a wild goose chase if he or she attempt to discover your password through the information contained in the hint. You should never use anything in the hint that leaks any personal information about you, and if you are using a strong, randomly generated password, the hint should have nothing at all to do with the password itself. Some examples of my favorite purposely misleading hints might be: My Birthday, Miami Dolphins, Texas Hold'em, or Password, none of which have anything at all to do with the password at which they "hint".

PASSWORD LIFESPAN AND PASSWORD FATIGUE: Like youthful good looks, architecture, and perishable foods, passwords are vulnerable to the ravages of time. The longer an attacker has to work at compromising your password, the weaker it becomes in practice. Accordingly, password should be change periodically. In my opinion, they should be changed every six months if no extenuating circumstances exist. I change all of my important passwords much more often than that, because as a security professional, I am probably much more likely than most to be targeted (not to mention much more paranoid, as well). If you have any reason to suspect an online account, your wireless network, or your computer itself has been breached you should change your password IMMEDIATELY. The new password should be drastically different from the old one.

If you are using a password manager, a practice I strongly recommend, changing passwords is not difficult at all. Remembering them is a non-issue. If you choose not to use a password manager, or you have more than one or two accounts for which you prefer to enter the password manually, you may become susceptible to password fatigue. Password fatigue is the phenomenon of using the same four or five passwords in rotation if you change them, or are forced to change them, frequently. This impacts security negatively by making your password patterns predictable, and exposes you to the possibility of all the passwords in your rotation being cracked.

With modern password hashing techniques, changing passwords frequently is typically unnecessary. The corporate practice of requiring a new password every 30, 60, or 90 days is a throwback to the days when passwords were predominantly stored in plaintext and there was significant risk of the entire password database being hacked. If passwords are being stored correctly, they should be secure even when the database is breached. With that being said, I am more paranoid than most and regularly change my passwords on all of my important accounts. Though it takes a bit of time and patience to update passwords on multiple sites, doing a few each week in a constant rotation can ease the tedium a bit and ensures that if one of your passwords is compromised it will only be good for a few weeks at most.

TWO-FACTOR AUTHENTICATION

These days, one does not have to specifically follow security news to know that password compromises happen with shocking regularity. The Wired cover story about the hack on Mat Honan in late 2012 fully underscores the weaknesses in passwords. Mr. Honan is also an excellent case study in the folly of using the same password across multiple accounts. When one of his passwords was hacked, it led to the compromise of several of his accounts. Passwords are becoming a weaker method for securing data. Passwords can be brute-force, captured during insecure logins, via key-loggers, via phishing pages, or lost when sites that do not store passwords securely are hacked.

There is a method of securing many accounts that offers an orders-of-magnitude increase in the security of those accounts: two-factor authentication (2FA). Using 2FA, each login requires that you offer something other than just a username and password. There are several ways 2FA can work, and there are three categories of information that can be used as a second factor. The three possible factors are something you know (usually a password), something you have, and something you are (fingerprint, retinal scan, voice print, etc.). A 2FA scheme will utilize at least two of these factors, one of which is almost always a password.

PGP KEY MESSAGE DECRYPTION: With your account setup with a PGP key that you control setup as a second factor, you will enter your username and password to login. Before being allowed access to the account, you will be presented with an encrypted message, that was encrypted with your own PGP public key. Once you decrypt the message, a code will be given to you. Upon entering the code, access to the account will be granted.

Sadly, I have yet to seen a Clearnet website deploy this kind of security measure. The only websites that have this kind of protection in place are darknet websites and markets. Most likely because of the fact that most people don't use PGP to communicate, if not on the darknet, so it is not a very popular security measure. This is very unfortunate, as PGP key message decryption, is most likely the single best method to secure your account from hackers, and currently, my favorite.

With Qubes OS, we can create an isolated VM, with no access to the internet, especially designed for the use of PGP, which makes things extremely more secure. I recommend you clone the fedora-26 TemplateVM into fedora-26-pgp and then simply create a new AppVM based on that template, to which you will then label it "pgp" and give it no access to the internet. From there, to use PGP it is as easy as setting up a new key pair and knowing the command line commands to encrypt/decrypt messages. You can follow the tutorial in the link below to accomplish so.

https://apapadop.wordpress.com/2013/08/21/using-gnupg-with-qubesos/

TEXT/SMS: With this method, a code will be sent via text/SMS message to your mobile phone. Upon entering the code, which is typically 6-8 digits, access to the account will be granted.

Using the text/SMS scheme of two-factor authentication is a major security upgrade but is not as good as the next option we will discuss: the dedicated authenticator app. Text/SMS can be defeated if your phone's texts are forwarded to another number. This may happen if your service provider account is hacked, or if a phone company employee is a victim of social engineering and allows an unauthorized person to make changes to your account. This may seem like a very sophisticated and unlikely attack vector, but several well-documented cases of this attack have occurred.

APP: Another option for smartphone owners and Qubes OS users is a dedicated two-factor authentication app. One such app is the Google Authenticator. With the app installed, you will visit the website and enter your username and password. Then, you will open the app, which will display a six-digit, one-time code for that account (this code changes every 30 seconds). You will enter the one-time code to login. Setup for the app is slightly more complicated than setting up text/SMS, but it is far from difficult.

Once the app is installed on your computer/phone, you visit the site for which you wish to setup 2FA. The site will give you a code that you can input on the app,

which links your phone/computer to the account, and adds an entry for the account into the app. Google Authenticator works for a number of sites, including Amazon Web Services, Dropbox, Gmail, Facebook, Microsoft, Wordpress, and more.

Though I generally consider app-based tokens more secure than text/SMS systems, it is important to be aware that they are not invulnerable. While an attack on your phone could get some of your login tokens, the capture of the token that is transmitted to your app could allow an attacker unlimited access to all your two-factor codes indefinitely. This is very unlikely however. In Qubes, you should create a VM specifically for this purpose ALONE, don't use for nothing else, and don't download or navigate the web in that VM. There are other VMs you can create specifically for those other purposes. Below is the link to a tutorial in setting up a VM on Qubes for this purpose. If you are having problems, feel free to contact me and I will help you.

https://www.qubes-os.org/doc/multifactor-authentication/

COMMON TO ALL: BASIC BEST PRACTICES

DO YOU REALLY NEED AN ACCOUNT? Many online accounts that you are asked to create are unnecessary and time-consuming. Some services require an account. Before you set one up, I strongly recommend considering the potential downsides. You should also carefully consider what data you are willing to entrust to a website. An online dating site may request a great deal of data and periodically invite you to participate in surveys. Of course, it will also ask you to upload photographs. I urge you to use caution when doing so because it is a near certainty that any information you put on the internet will one day be compromised in some manner.

USE ACCURATE INFORMATION SPARINGLY: When signing up for a new online account, consider what information is really important and necessary to the creation of the account. When you sign up for an email account, does it really need your true date of birth? Obviously not. E-commerce sites require your address to

ship packages to you, but do they need your real name? Perhaps they do. When you create an online account with your bank, do you need to use complete and accurate information? Yes, you most likely do, unless you are conducting any type of fraudulent activity.

CHECK THE STATUS OF EXISTING ACCOUNTS: An early step in securing online accounts is to ensure they have not been breached. There are a couple of services that will offer you a bit of insight into this by allowing you to cross-reference your email address against lists of hacked accounts. Breachalarm.com allows you to input your email address, which it then cross-references against a list of hacked accounts. If your account has been hacked, change the password immediately.

Haveibeenpwned.com is a similar website that checks both email addresses and usernames against lists of known-hacked accounts. The site is relatively new and maintains a database of breached accounts.

GET RID OF UNUSED OR UNTRUSTED ACCOUNTS: If you have old online accounts that are no longer used, close them down if possible. Some websites can help you do this such as KnowEm (www.knowem.com), AccountKiller (www.accountkiller.com), WikiCancel (www.wikicancel.org), and Just Delete Me (www.justdelete.me). Before closing an account, I highly recommend you get rid of as much personal information as you can in the account. Many services will continue to harvest your account for personal information, even after it has been closed. Before closing the account, login and replace the information in as many data fields as possible. Replace your name, birthday, billing information, email and physical addresses, and other fields with false information.

SOCIAL NETWORKS

With the explosion of social networks, many data mining companies are now collecting content from public profiles and adding it to a person's record. Overall, society has made it acceptable to provide ever level of personal detail to the corporations that own these networks. We have been trained to "like" or "favorite" anything that we find enjoyable or feel pressured into identifying with. These actions seem innocent until we discover the extent of usage of this data. Think about your online actions another way. Would you ever consider spending time every day submitting personal details to online survey websites? Further, would you consider doing this for free? Would you sit down for an hour each day with a complete stranger and answer invasive questions about the details of your life and your likes and dislikes, knowing that he was going to sell this information? Not to mention the fact that all of this information, is gold in the hands of private investigators and police officers when conducting an investigation and MANY people have been caught because of data found on social networks, and consequently that data was used in court to further persecute their actions.

Essentially, when you create a Facebook account you are agreeing to work as unpaid survey-taker, photographer, and writer. When you "like" a site you are adding to Facebook's trove of data about you. When you install the Facebook app on your phone you give Facebook permission to access your location data, letting the service track you everywhere you go. When you upload photos to Instagram you are actually giving them, in perpetuity, to Facebook who can use them for almost any purpose whatsoever. When you update your status, submit a photo, or comment on Facebook you are voluntarily giving them data they can resell or reuse in almost any legal way. This in addition to the fact that all your posts, status updates, likes, and other actions are used to build an incredibly accurate profile about you. Your photos are used in facial recognition software so accurate that Facebook could even build a near-perfect 3D model of your body. You aren't the customer, you are the product.

The other danger of social networks and other services that rely on data collection is that they never forget. While you can delete your Facebook or Google account, the information that you have submitted to the service will always be retained in some form. While Google may not keep the entirety of your emails, your profile will be saved for potential future use. While using some of these services, teenagers and adults are making IRREVERSIBLE decisions.

I personally recommend deleting and removing all of your social networks. It is very important that you first replace every single information with fake info, before actually deleting your account.

EXIF DATA

Every digital photograph capture with a digital camera possesses metadata known as Exif data. This is a layer of code that provides information about the photo and camera. All digital cameras write this data to each image, but the amount and type of data can vary. This data, which is embedded into each photo "behind the scenes", is not visible within the captures image. You need an Exif reader, which can be found on websites and within applications. Keep in mind that most social network websites remove or "scrub" this data before being stored on their servers. Facebook, for example, removes the data while Flickr does not. If the image has been compressed to a smaller file size, this data is often lost. However, most photo sharing websites offer a full size view. The easiest way to see the information is through an online viewer.

JEFRREY'S EXIF VIEWER: I consider Jeffrey's Exif Viewer (www.regex.info//exif.cgi) the online standard for displaying Exif data. The site will allow analysis of any image found online or stored on a drive connected to your computer. The home page provides two search options. The first allows you to copy and paste an address of an image online for analysis. Clicking "browse" on the second option will open a file explorer window that will allow you to select a file on your computer for analysis. The file types supported are also identified on this page.

The first section of the results will usually provide the make and model of the camera used to capture the image. Many cameras will also identify the lens used, exposure settings, flash usage, date and time of capture and file size. This is a lot of data to share with the world.

Scrolling down the analysis page will then identify the serial number field. This is most common in newer, costlier digital cameras and may not be present in less expensive cameras. These cameras will identify the make, model, and serial number of the camera inside every photo they capture.

EXIFTOOL: As I express constantly on these pages, I typically prefer local solutions over cloud-based solutions. ExifTool is a simple, lightweight tool that will quickly and easily display the Exif data contained on photographs. It runs in portable mode and does not require you to permanently install the application. To view Exif data for a photo simply open ExifTool and drag the photo onto the command line interface. A list of all available Exif data will be displayed. This tool can be used to see what metadata needs to be removed from the photo, and to verify that it has been removed before uploading. ExifTool is free and available by visiting https://owl.phy.queensu.ca/~phil/exiftool/. A graphical user interface (GUI) that makes ExifTool easier to user, especially for bulk photos, can be downloaded at http://u88.n24.queensu.ca/~bogdan/.

A serial number of a camera associated with an image can be valuable data. This can help someone associate photos that you "anonymously" posted to the internet directly to you. For example, if a stalker found a photo that you posted on your Twitter feed that you took with your camera, he or she may be able to identify the serial number of your camera. If the stalker then finds a photo and suspects that you took it but posted anonymously, he or she can see if the serial numbers match. I bring this up to explain the next threat.

STOLEN CAMERA FINDER

This site (www.stolencamerafinder.co.uk) was designed to help camera theft victims with locating their camera if it is being used by the thief online. For that use, you would find a photo taken with the stolen camera, and drop it into the site for analysis. This analysis identifies a serial number if possible. If one is located, the service then presents links to photo-sharing websites, such as Flickr, that contain photos with the same serial number. This can locate photos that you may not want to take credit for.

CAMERA TRACE

An additional site that provides this service is called Camera Trace (www.cameratrace.com/trace). Type in the serial number of a camera and the site will attempt to locate any online photographs taken with the camera. This service claims to have indexed all of Flickr, Twitter, Twitpic, Panoramio, and 500px.

GPS

Many new SLR cameras, and almost all cellular telephone cameras, now include GPS. If the GPS is on, and the user did not disable geo tagging of the photos in the camera settings, you will get location data within the Exif data of the photo. This field will translate the captured GPS coordinates from the photo and identify the location of the photo. Further down an Exif results page, the site will display an image from Google Maps identifying the exact point of the GPS associated with the photo. All Android and iPhone devices have this capability.

CROPPED PHOTOS

Another piece of information that can be located from the Exif data is the presence of a thumbnail image within the photograph. Digital cameras generate a small version of the photo captured and store it within the Exif data. This icon size image adds very little size to the overall file. When a user crops the image, this

original smaller version may or may not get overwritten. Programs such as Photoshop or Microsoft Photo Editor will overwrite the data and keep both images identical. Other programs, as well as some online cropping tools, do not overwrite this data. The result is the presence of the original and un-cropped image within the Exif data of the cropped photo. You can now see what the image looked like before it was cropped.

If you have a situation where it is necessary to upload photos to the internet, you may want to consider removing this metadata.

EXIF REMOVER

This website (www.verexif.com/en/) allows you to upload a digital image and either view or remove the metadata attached to it. Click on the "Browse" button, locate the photo you want to edit, and click "Remove Exif". You will be presented with a new download that will contain your image without the Exif data embedded. ExifTool will also allow you to remove this data without touching the internet.

QUBES – WHONIX MAT SOLUTION

This is by far my favorite method to scrub any Exif data from my pictures, and any metadata from my documents.

Whonix-workstation comes with a pre-installed application called MAT (Metadata Anonymization Toolkit). You can follow the steps in the Whonix website to use this program, but it is fairly straight forward and easy.

https://www.whonix.org/wiki/Metadata

ANONYMOUS PURCHASES

In this chapter, I will explain various ways to protect your privacy while maintaining the convenience of making non-cash purchases online and in person. Before outlining these techniques, I feel obligated to examine how convenience is inversely proportional to privacy and security. The more convenient something is the more personal privacy and control of your identity you are probably sacrificing. Credit and debit cards are one such convenience. With cash you have to make time to visit an ATM, carry bills, and manage change. All of these inconvenience factors are compounded if you make multiple small purchases throughout the month.

Despite its inconveniences, making these multiple small purchases routinely is precisely the reason you should use cash when available. Though it is certainly more convenient to swipe a credit card for purchases than it is to use cash, it also creates a tangible, searchable record of each transaction. Your purchases record a wealth of data about you including your location and movement, interests, hobbies, and a plethora of other information. Some will say this data is protected and only visible to those with proper authority. I counter that argument with whatever data breach is in the headlines while you read this chapter. Further, history has proven that those with proper authority often abuse their power.

Ideally, you want your bank statements to always look something like this.

DATE	TRANSACTION DESC	AMOUNT
07/01/15	ATM WITHDRAWAL	$500.00
07/08/15	ATM WITHDRAWAL	$500.00
07/20/15	ATM WITHDRAWAL	$500.00

This type of bank statement, does not raise any kind of suspicion, and will keep you in a low-profile, which is what we want. If you are a cyber-criminal, you do not want any kind of attention to yourself, especially from the IRS or police.

This kind of statement also reveals very little about you. It does not reveal where you buy your groceries, where you eat lunch, dinner, etc... This does not associate your name with any kind of purchase.

I attempt to use cash as much as possible but realize that I will never be able to fully eliminate credit cards from my life. Air travel, rental cars, and hotels all require credit cards. I still find myself in locations where I don't want to pay exorbitant ATM fees and end up using a credit card. But I use it a lot less, which is what I am truly advocating. Use more cash and less plastic. This reduces the amount of information about yourself that you give over to your bank, your lenders, or anyone curious enough to swipe a statement out of your mailbox.

There are significant and compelling reasons to keep your purchase history anonymous. Especially for us criminals. Your purchases will reveal almost everything about you. The sporting goods you buy (or don't buy) probably say a lot about your level of physical activity and fitness. The books you read reveal a lot about your personality including your religious beliefs, your political leanings, your sexuality, and the things you are passionate about. The foods you buy, the restaurants at which you eat, the frequency with which you eat at them, and the alcohol and tobacco products you consume reveal a LOT about your life. This may one day very soon be used against in one way or another.

Using cash isn't bulletproof, and it won't make you totally anonymous. But it will lower your digital signature, offer you a lot more anonymity, and make an attacker's job a bit harder. Every little bit helps. For those situations that do not allow cash purchases, I have some ideas that will decrease the invasive tracking of your buying habits.

AMAZON

I begin with Amazon because it is one of the largest online retailers. I place orders through Amazon weekly and never jeopardize my privacy during the process. If you are already using Amazon and have an account created, I recommend that you stop using that account and create a new one. The details that you provide are

extremely important. Before discussing the appropriate methods, please consider an actual scenario.

A friend had recently moved to a new rental house to escape a dangerous situation. She had nothing associated with her real name at the address. The utilities were still in the name of the landlord. She used a PO Box in a different city for her personal mail. She was doing everything right. She created a new Amazon account and provided the name of her landlord and her home address for shipping purposes. This way, her packages would arrive in the name of the property owner and she would stay invisible. She made sure that her name was not visible in any part of the order.

When prompted for payment, she used her real credit card in her name. She verified one last time that her name was not present anywhere within the actual order or shipping information. Her item, a pair of hiking shoes, arrived in the name of the landlord. Her real name was not referenced anywhere on the package. Within 30 days, she received a piece of mail that made her stomach drop. It was a catalog of hiking equipment addressed to her real name at her address. The company had accepted the order through Amazon and was given her name as attached to the credit card. Therefore, the company added her to its catalog delivery list.

All of her hard work was ruined from this one mistake. The lesson here is that you can never tie your real name to your address if you do not want that association to be public.

The following steps will mask your real identity from your Amazon purchases. This technique can also apply to other online retailers. Create a new account with the following information.

- **Name**: Use the name that you want your packages shipped to. This could be the former resident or landlord at your address, or a complete alias.
- **Email Address**: You must provide an email address for your new Amazon accounts. I recommend you use Protonmail for this. Do not use your name.

- **Credit Card**: I personally recommend you head to https://dnt.abine.com/#register and create a new account with them. They allow you to create masked cards and masked cell phones with your real credit card. Supply Amazon with the masked card and provide an alias name that you want to use for deliveries. If you don't want to get a Blur account, you can simply buy a BTC debit card, and attach that to your account. But make sure the BTCs in the debit card are extra clean.
- **Address**: This could be your home address if you do not have a better place for deliveries. You can alter this information once the account has been verified. I personally recommend you get a PO box in a different city, and use that as your delivery address. Because the name on the shipment is not a real name, I do not see this as a privacy concern (for your house, do not use a alias for a PO Box you opened with your real ID). I believe it actually helps establish that someone else lives at your residence, and provides great disinformation. You should scrutinize any option that you choose and make sure that it is appropriate for your scenario.

This method should protect you from any association between your name, your purchases, and your home. You could likely use this new Amazon account for all of your purchases and have no problems. However, I encourage you to take things a step further and apply a bit more paranoia to your plan. I create a new Amazon account after each Blur card has been depleted. If I add a $200 Blur masked card to my account, and then use those funds over a period of five orders, I do not add a new masked card to my Amazon account. Instead, I close the account and create a new one. Same thing with BTC debit cards and Amazon gift cards. I create a new account after each purchase. This way, Amazon does not have a single record of all transactions. It will add disinformation to your address and will confuse your delivery person. The only drawback to this is if you subscribe to their Prime membership. You may want to create an account to be used with those benefits.

AMAZON GIFT CARDS

An alternative strategy for purchasing anonymously on Amazon is to use their gift cards. These are available for sale at many retailers including drug stores such as CVS and Walgreens, grocery store, and even hardware stores such as Home Depot and Lowes. They can also be purchased directly with Bitcoin through a website called PayBis (https://paybis.com/buy-amazoncom-gift-card-with-bitcoin/). Many people used to use eGifter and Gyft, however, they no longer support Amazon gift cards.

These can be purchased in amounts up to $2,000.00, require no additional activation fee as prepaid credit cards do, and some retailers require that you pay cash for them. Using these cards is incredibly simple. Create a new Amazon account, navigate to your payment settings, and add the gift card. When you have used up your gift card balance, open a new Amazon account providing your real shipping address and a false name. Now order items from Amazon as you normally would. This creates disinformation rapidly. Within 30 days of making a purchase on an alias account, you might begin receiving junk mail at your home address in that name.

Taken to the extreme, you could use this technique to make a new Amazon account, complete with a new name at your shipping address, for every purchase you make.

MONERO

No discussion of anonymous purchases would be complete without mentioning the infamous cryptocurrency Monero (XMR). Monero is currently the most anonymous cryptocurrency in existence.

The unfortunate disadvantage of Monero is that almost no retailers accept it as a form of payment. However, you can easily purchase BTC with Monero through services such as xmr.to. In fact, I strongly recommend you do this before purchasing an Amazon gift card, to ensure your maximum anonymity.

MONERO ANONYMOUS DEBIT CARD

UQUID (https://uquid.com/uquid-card) is a service that will allow you to get a Monero reloadable debit card, of which you can use as you normally would a bank debit card. The huge advantage to this is the fact that we can remain completely anonymous, and not depend on banks to spend our hard-earned money. These cards also allow for easy withdrawals at any functional ATM. The service is completely free and you can provide them fake information to sign up with them. They do not ask for any kind of ID verification, and even if they do in the future, you can simply send them a scan of somebody else's ID. I highly recommend you get this card shipped to an anonymous drop that can't ever be connected to you. Preferably even in another country other than the United States, if you're a US resident as they don't ship to the United States. Simply team up with someone and pay them a small fee to reship the card for you.

BITCOIN ANONYMOUS DEBIT CARD

There are many services online that will allow you to get anonymous bitcoin debit cards. I will list some of the services I've used myself and can vouch for their reliability below.

1. https://spectrocoin.com/ (WORKS FOR US RESIDENTS)
2. https://wirexapp.com/ (WORKS FOR US RESIDENTS)
3. https://coinsbank.com/

ANONYMOUS TELEPHONES

Cellular telephones are digital trackers in our pockets monitoring and recording every move we make. They are beacons announcing our locations, conversations, contacts, and activities to companies outside of our control. Do we use cell phones? Absolutely. Can we reclaim our privacy without ditching the convenience of a computer in our pocket? Yes, and I will explain my methods in this chapter.

I believe that having an anonymous cellular telephone is very high on the list of vital steps to take in order to obtain true privacy. Even if you implement every tactic explained in this chapter about phone security, your device is always tracking you. If the device is on and connected to either a cellular tower or Wi-Fi connection, it is collecting and sharing your location information. The moment you place a call or send a text, you have updated a permanent database of these details attached to your account. Some will argue that these details are not publicly visible and only obtainable with a court order. While in a perfect world this is true, we do not live in a perfect world. There are many scenarios that could leak your entire communications history to the world. Not to mention law enforcement has been known to break the law to go after people.

The most common scenario would be a data breach. I hear every day that a new database of customer information has been stolen and released to the wild. What is to prevent that from happening to a cellular provider? We also know from widely publicized reports that some government agencies overstep the scope of data collection from both Americans and non-Americans, often including telephone records. We have seen several civil legal battles incorporate cellular records into the case after submitting a subpoena to a provider. I have even heard of rare instances where a Freedom of Information Act (FOIA) request was submitted for cellular records of government employees.

Regardless of the situation, I believe that you have a great deal of data to lose by using a standard cellular telephone setup. In this chapter I will explain many ways of maintaining privacy while remaining connected to the world.

The most common way to possess a cellular telephone is through a contract with a major provider. This typically happens when you visit a provider's kiosk or store and are given a free phone. While this sounds like a great excuse to upgrade, you are committing to multiple years of service through this carrier. Privacy through this method is practically impossible since the provider will mandate a financial check on you using your Social Security number. Your phone, bill, and call details will be stored forever and connected to your name. This can all be avoided, but at a cost.

THE DEVICE

First of all, you will need a proper telephone. I never recommend any devices that are marketed toward pre-paid buyers. These are always unpopular models that no one else wants. They are slow, have poor battery performance, and will only meet the minimum hardware requirements to function. Additionally, they are overpriced. At the time of this writing, a local grocery store was selling an Android smartphone for $149 that was available on eBay for less than $60. Either way, it was not a powerful device. Instead, consider a used phone.

Searching your local craigslist.org community will identify hundreds of used devices for sale. You will need to be very careful. Many of these are stolen, some are broken, and others are counterfeit. I recommend filtering these results until you are only left with the following

- Devices that include the original box, cables, and manuals: This is an indication of a one owner phone that is not likely stolen property. A person that keeps those items probably takes good care of their property.
- Sellers that have recently upgraded: Many people must have the latest and greatest devices and upgrade the moment a new version is available. While you can never believe everything that you read on Craigslist, this is an indicator of a decent phone.
- High prices and old posts: Many people believe the value of their used equipment is higher than what others are willing to pay. Seeking phones that were posted over three weeks' prior at a high price will usually reveal people

desperate to sell. Make a reasonable offer and you will be surprised how many people accept.

You may already have an unused device collecting dust. Usually, when you upgrade a phone, you are allowed to keep the old unit. You could use a device that was previously attached to your name and account, but I urge caution in this. Financially, it makes sense to use a device that you already have. Unfortunately, providers never truly forget what you have used. If you decide to use a phone that was previously attached to an account in your name, please know that the history will continue to be available.

Your device possesses an IMEI (International Mobile Station Equipment Identity) number that is transmitted to the carrier. When you activate an old phone, even as a pre-paid, that number could still jeopardize your privacy. This may seem extreme, and it may not be important to most readers. If you want to completely start over and not contaminate your new communications device, you should obtain a unit that has no association to you.

If you are not concerned with the trail left to the cellular provider, then you can re-activate an old device. Only you can decide which is appropriate. I ask that you consider the following question. Will anyone ever ask your cellular carrier for a list of every phone that you have owned or used? By “everyone” we include hackers, enemy government agencies, the media, and general public after the next big data leak. In the most basic terms, your cellular telephone that was used in your real name is permanently attached to you. There is no way to break this connection. This device tracks your location at all time and reports to your provider. That data is stored forever. Therefore, I believe that now is the time to activate a new device with a new account.

I encourage you all to start fresh with different new or previously-owned devices from strangers. You could organize a swap with someone else that you have no official connection with. New non-subsidized phones are becoming more affordable while offering a level of privacy unavailable through a traditional

contract. This might be a good time to try a different operating system. Android versus iPhone is a matter of personal preference.

If you are looking for an extremely affordable solution, you might consider the various “Mini Card Cell Phones” available at online retailers such as Amazon. These miniature telephones usually cost $20 or less and are the size of a credit card. They do not contain touch screens, cannot use data plans, and do not work with apps. They can only make and receive calls and texts. I have these many times as “burner” phones. The lack of data usage and internet access creates a fairly secure phone for minimal communication. These are almost always based on GSM networks and nano SIM cards, and the carrier plans for these phones are minute compared to those of modern smartphones.

FACTORY RESTORE

Regardless of the operating system, previous owner, or current state of the device, you should conduct a factory restore. This eliminates all personal data from any previous user and replaces the phone’s operating system in the identical state as the day it was first purchased. This will ensure that there are no unique configurations that could jeopardize your privacy. The process for this will vary slightly by device.

CELLULAR SERVICE

After you have performed a factory reset, you are ready to activate it on a cellular network. For complete privacy, I only recommend prepaid plans. Subsidized contract plans require a real name or credit check but prepaid plans generally do not. Every major U.S. provider offer these types of plans. The following list compares the most affordable advertised services offered at the time of this writing. After, we will discuss an even better option.

SERVICE	PRICE	MINUTES	TEXT	DATA
AT&T	$45	Unlimited	Unlimited	1.5GB
Sprint	$35	Unlimited	Unlimited	1GB
T-Mobile	$40	Unlimited	Unlimited	Unlimited
Verizon	$45	Unlimited	Unlimited	1GB

T-Mobile "Hidden" Plan

Privacy advocates have known about a hidden pre-paid plan at T-Mobile for a while. This plan, sometimes called the "Wal-Mart Plan", is not available at T-Mobile stores or kiosks. You will not find it advertised on billboards. In fact, it takes effort to locate the plan online. The plan gives you unlimited text and data, and 100 minutes of talk time, per month, for only $30. The talk time may seem low, but that will not matter once you have your device properly configured for free unlimited calls. The following instructions will guide you through the process of obtaining a great anonymous phone plan at an unbelievably low cost.

- Ensure that you have a cellular telephone that is T-Mobile friendly. This device needs to support the GSM network. Most iPhone and Samsung Galaxy models will work as will phones that have previously been registered with AT&T. You should check the T-Mobile website before you commit to this plan.
- Obtain a T-Mobile SIM card. Stores and kiosks will not offer you a card without committing to a plan. The T-Mobile website will send you a free card but will require you to buy a more expensive plan. A third party online order is your best option. At the time of this writing, several vendors on Amazon were offering a T-Mobile SIM card start pack, including a $30 credit, for $24.99-$30.95. This is the best deal that I have found. Use the method explained in the previous chapter to create an anonymous Amazon account before ordering.
- Insert the SIM card in your device and turn on power. Have the SIM card serial number and the phone's IMEI ready. On a computer, navigate to the T-Mobile prepaid activation site and enter these details. On the next page

enter your anonymous information. You can provide any name and address that you choose. This will not be verified. I recommend a common name and address that does not exist. Finally, it's time to choose the plan. Choose the $30 plan with unlimited text, data, and 100 minutes of talk time. Follow the activation prompts and you should possess an active phone.

- If you can make calls, but cannot use data, manually enter the T-Mobile APN settings. Navigate to https://support.t-mobile.com/docs/DOC-2090 for specific instructions for your device.

You should now have a fully functioning, and fairly anonymous, cellular telephone. You should have fast 4G data, and the ability to install or uninstall any apps. However, this device is not ready for completely anonymous use. As mentioned previously, your phone is always tracking you, your calls and texts are being logged, and the data that you send is being monitored. You will need to make some modifications to the way that you use a cell phone. The following is an actual plan, from start to finish, that I executed for myself.

AN ACTUAL SAMPLE STRATEGY

First, I purchased a used Samsung Galaxy S4 on Craigslist. It was listed at $125, and the ad had been posted over 30 days prior. I offered $75 and obtained the device at that price. I conducted a factory reset and rooted the phone. I removed all Samsung and Verizon bloatware. I purchased a T-Mobile SIM card and activated the hidden plan as discussed.

Next, I secured the data traffic by installing a Virtual Private Network (VPN). These will be explained in much greater detail in further chapters. Basically, it encrypts the network traffic, whether through cellular or Wi-Fi, for all data transmitted to or from the device. For this specific installation, I chose NordVPN as the provider. This will prevent the cellular provider from having the ability to intercept the data or implant data packets with tracking codes.

The hidden T-Mobile plan includes only 100 minutes of talk time. For many, that is plenty. Most use the unlimited text and data for communication.

However, it is important to have options for placing outgoing calls and accepting incoming calls that do not count toward this limit. In order to subsidize voice calling features, and add another layer of anonymity, I added two additional free telephone lines to the phone.

GOOGLE VOICE

First, I installed the Google Voice app. Yes, I know that Google analyzes all of our data and uses it to generate targeted ads. I also suspect that Google stores every bit of data possible from its users. However, they offer a free product that will work well for our needs.

I created a new account while connected to a public Wi-Fi at a library, used the name of an alias, and selected a number from a different area code. Will Google still collect data on this account? Yes. Will they know it is you? No. Not if you are careful. If you use a VPN at all times on the device, Google will only know the IP address of the VPN provider and not your cellular provider's IP address. You can use the Google Voice app to send and receive unlimited text messages. Please note that while you can delete messages within the app, it does not delete them from the "Trash". You will need to access this account from a web browser in order to properly delete messages from the account.

HANGOUTS DIALER

Next, I downloaded the Google Hangouts Dialer app. This will allow you to make free calls from your device, using your data connection, without sacrificing any talk minutes. The calls will appear to come from your Google Voice number. The VPN will prevent Google from knowing where you are or which internet connection you are using. This solves the problem of free outgoing telephone calls, but not the issue of incoming calls. If someone calls your Google Voice number, they will either be forwarded to your real number (not recommended), or voicemail (recommended). This will vary based on your user settings. Instead, we will use another service to fill this void.

BURNER

Burner allows you to create semi-anonymous, disposable phone numbers. These numbers can send and receive calls without requiring you to give out your real phone number. If you need to make a call or give out a number, you set up a new burner. You can choose your area code and “size” of the burner you need. The size is determined by how many days it lasts before self-destructing, how many texts and voice minutes are allowed, and whether or not it can send and receive photos. The burner will be created and you can then send and receive calls at this number.

It is important to note that the makers of Burner, Ad Hoc Labs, explicitly acknowledge in their privacy policy and terms of service that they will comply with law enforcement requests for information about the use of their product. They also acknowledge that they maintain only limited information. What it does offer is a thin layer of privacy for everyday situations when you don’t want to give out your real number or one of the other, more durable options you have set up on your device.

BLUR

Blur was mentioned earlier when explaining masked credit card numbers. Another privacy related service they offer is masked telephone numbers. This feature allows you to create a phone number with which you can send and receive calls. When you create a masked phone number, it forwards calls to your real phone number (or Google Voice number), protecting the “real” number. I mostly use this for things like verification and two-factor authentication text messages. You can sign up for the service using your BTC/XMR anonymous debit card, and it is extremely recommended you do so, instead of linking your real identity to these services.

WI-FI ONLY

You may have noticed that the majority of the services that I recommended do not necessarily require a cellular service provider. They only require internet access through cellular data or Wi-Fi data. If desired, you could eliminate the activation of cellular service and rely on wireless internet alone. The pitfall in this plan is that your device will be useless for communication when you cannot find open access.

I always keep two devices operational at all times. My primary device possesses cellular connectivity and the secondary device only contains a Wi-Fi connection. While the setup for the secondary device is very similar to the primary unit, there are a few differences.

- My secondary phones never attach to a wireless internet connection that I use with my primary device or laptop. This prevents me from creating an association between the two devices. If I logged into two Google Voice accounts, on two unique devices, from the same network, Google would now know that I am the same person on both accounts.
- The secondary device possesses a Google account that was not created on a network connection that my primary devices access. Again, this creates a trail to the primary unit. I use public Wi-Fi to create, activate, and connect these accounts directly from my secondary device. While this seems careless in regards to security, it is optimal for secondary devices that you do not want associated with your real identity.
- The secondary phone remains turned completely off until needed. It is always in airplane mode with the Wi-Fi enabled. All location services are disabled. These actions prevent your movements from being collected and stored.
- Finally, for the truly paranoid, I always turn my primary devices off before turning my secondary device on. I also confess that I do this while in motion so that the secondary device is not turned on at the same location the primary was powered down. Again, this prevents Google and other interested parties from knowing that I may be the same person using these devices.

Is this all overkill? Some may think so. However, my experience supports my paranoia. I have witnessed investigations involving Google and other similar companies. They know more than you think. They know that you have multiple Gmail accounts under various names. They record this activity and will disclose all of your related accounts if given an appropriate court order. More concerning is when their data is compromised during a breach and all collected information is exposed.

SMARTPHONE SECURITY

To call a smartphone a “phone” is a bit of a misnomer. With the increased technology being poured into these devices a phone is no longer “just a phone”. In fact, the telephonic functionality of such a device is usually a third or fourth consideration and is not the most frequent or most common way in which such devices are used.

Today’s smartphone is an incredibly compact, marvelously powerful computer that is carried on a daily basis, and also happens to be able to place and receive calls. For most of us the collective time spent snapping and reviewing photographs, texting, streaming music, reading e-books, playing games, and browsing the internet far eclipses time spent actually talking on the phone. I believe it is important to realize this distinction and to think about smartphones differently than “just a phone”, and to understand that this conceptualization has serious security implications.

Why is this distinction important, and how does it impact security? Many still view their phone through the “just a phone” lens and put very little effort into securing it. But with all of their uses, smartphones are now a part of our everyday lives and reflect this daily inclusion more each year. With the Internet of Things becoming a reality, smartphones are now linked to our real, physical worlds in ways that were unimaginable just a few decades ago.

The threats arrayed against smartphones are also increasing. Because they are used everywhere and contain increasingly large chunks of personal information, smartphones are more dangerous than ever. Fortunately securing them is getting somewhat easier. Both Apple and Google have taken steps to make privacy and security easier, but there are still many ways this can be compromised. There are many improvements that can be made. Ultimately it is up to the individual user to take control of his or her own security and privacy to the extent possible.

In this chapter, I will examine the threats against smartphones, of which there are many. I will also discuss how to take your anonymously purchased and registered phone and secure it against these threats.

SMARTPHONE THREATS

There is no perfect secure solution to any security problem, and making your phone completely secure against the threats they face is an impossible goal. The only way to be completely secure is to forego having a phone at all, an idea that becomes more attractive to me with each passing day, even as it becomes less and less realistic. With the knowledge that a mobile phone can never be completely secure should come the realization that a smartphone is a security and privacy compromise regardless of the measures you take.

Before you begin the process of securing your device, it is important to understand the threats arrayed against it. With this knowledge you can assess your own threat profile and the treats from which you wish to defend yourself. The primary threats facing smartphones can be broken down into three broad categories: metadata collection, traffic interception, and hardware exploitation.

The widespread collection of millions of Americans' metadata was the first of the Edward Snowden revelations that was published by the Guardian during the early summer of 2013. The fact that this information was collected was extremely alarming to those within the security community. But what is metadata exactly and why is this so alarming?

METADATA: Metadata is data about data. In the context of a telephone conversation, metadata would not include the content of the call, the actual conversation. Metadata would include such information as who placed the call, to whom it was placed, and how long the conversation lasted. Where text and SMS messages are concerned, metadata would include who placed the text and to whom, how often the two text each other, and how many texts are generated during a conversation. Metadata about text messages and telephone calls can be used to link you with others and to draw conclusions about your level of association.

Historical location data is also a form of metadata that can be collected from smartphones. Combined with call and SMS data, this information amounts to an alarming body of information. Anyone with this data can see where you went, how long you stayed there, who you talked and texted with, when you left, and where you went after that (as well as all of this data for everyone with whom you interacted). If every individual were legally compelled to carry a personal tracking device at all times, revolt would ensue. In spite of that we still pay hardware manufacturers and service providers hundreds or thousands of dollars per year for the privilege of carrying a tracking device in our pockets.

This is because a phone (whether smart or dumb) is, first and foremost, a tracking device. In order for the phone to function correctly it must be able to connect to nearby service towers. These tower connections or “check-ins” are the most common way mobile phones are tracked and can be used for both near-real-time (NRT) and historical data. Cell providers can access your location data now and forever through your use of their towers. Law enforcement may do so through warrants to obtain the tower data, or through cellular site simulators. Smartphones may also be tracked through a number of other means as well. Most smartphones utilize an internal global positioning system (GPS) to provide mapping and other location-specific services. The GPS data may be shared by a number of applications and transmitted back to numerous third-parties. Other technologies such as Wi-Fi and Bluetooth may also allow their location (and that of their owners) to be tracked, often with extremely high levels of precision.

Location tracking may not seem like a big deal or it may seem so beyond the pale that few will worry about it. However, location tracking can reveal a great deal of very sensitive personal information about you. It can reveal with whom you meet, where you meet, and for how long. Location tracking can reveal what church you go to, how often you go, or whether you go at all. It can reveal your interests and hobbies as well. Do you visit gun stores, marijuana dispensaries, adult-themed shops or club, or other niche locations? Do you attend politically-oriented conventions, speeches, or protests? Do you attend alcohol or drug-addiction recovery meetings or clinics? Have you had a one-night stand lately?

If you took your phone with you (and it is a near certainty that you did), your cell service provider knows all of this about you. The stores and shops are mapped, and the trysts can be extrapolated from the confluence of two phones in the same location overnight. Some of the apps on your device know where you've been, too. In all likelihood, so does your device's hardware manufacturer. Though none of these things may seem especially provocative or embarrassing to you now, how would you feel if this data was breached or accessed through a court order by law enforcement? How will you feel about those actions in 10 years? Data storage is cheap and it is unlikely that any of this information will ever be forgotten.

TRAFFIC INTERCEPTION: Traffic interception is the practice of capturing the actual content of your phone calls, texts, and emails. While traffic interception is a major concern for individuals traveling overseas or those who work on exceptionally sensitive projects, it is also still a concern for the average individual. Cell site simulators have placed the ability to intercept voice and data traffic in the hands of even small local police departments. And as security guru Bruce Schneier reminds us, "Today's NSA secrets become tomorrow's PhD thesis and the next day's hacker tools".

CELL SITE SIMULATORS

Cell site simulators are devices that, as the name suggests, masquerade as legitimate cell phone towers. These devices are useful only in a relatively small area, but they emit a very powerful signal that forces all the phones in that area to connect to the simulator rather than legitimate towers. Once connected these devices collect metadata about every device in the area, not just the target's. They can capture the content of phone calls, texts, emails, etc...

HARDWARE EXPLOITATION: Hardware exploitation is taking data directly from the device through physical access. It is hardly news that smartphones store impressive quantities of data (up to 256GB in the case of the iPhone). A smartphone may contain or be able to access tens of thousands of emails, thousands of photos, personal and intimate text messages, logins, web browsing history, call histories, and more. The loss of a device can potentially give all of this information away to anyone who bothers to look, which will almost certainly be someone. Like so many problems in the security world, the best solution to hardware exploitation is encryption. Well-implemented encryption and a strong passcode are the surest defense against this type of exploitation.

Another potential avenue through which your hardware may work against you is camera and microphone hijacking. Sometimes this is a feature, not a bug. In the case of some smartphones with voice-recognition capabilities, the phone may "listen" constantly, even when you are not using the voice recognition feature. This information is recorded, saved, and analyzed. Your camera and/or microphone can also be compromised by malware that allows the attacker to turn one or both on at will. Microphones may be hijacked by government agencies by calling into the phone in a way that does not make the phone show any signs of being on or operating but leaves the line open so an eavesdropper can hear everything within earshot of the device.

OS AND APP UPDATES

Keeping the operating system and applications on your mobile device up to date is just as important as it is on your home computer. OS and application updates are patched to add more function. In nearly all cases they also patch known security vulnerabilities.

iOS DEVICES: A badge will typically be displayed on the settings icon when an update is available. If you suspect an update is available but do not have a badge on the Settings icon, you can search for and update manually. If an update is available, follow the instructions and allow it to download and install.

Application updates are made available for iOS devices through the App Store. You have the option to have app updates download and install automatically or on demand.

ENCRYPTION AND PASSCODES

This section is one of the most important to the physical security of a mobile device. Apple has used very strong full-disk encryption (AES) on iOS devices since iOS 3 and the iPhone 3GS. To take advantage of this encryption, you must passcode-protect the device. On most Android devices you will still have to choose to encrypt the device. I recommend you use a very strong password for your iPhone, to make it very hard for anyone to crack.

WI-FI

Wi-Fi should be turned off when you are not connected to a network that you trust. When your device is not connected to a network and Wi-Fi is on, it constantly sends out probes searching for all networks that it “knows”. Knowing a network means that you have previously connected to that network and have not manually removed it. These probes can be identified and can set you up for an evil twin attack.

An evil twin attack occurs when an attacker sets up a rogue Wi-Fi access point that masquerades as a legitimate access point. Unsuspecting users will connect to it, not realizing that all traffic transmitted over it is being intercepted. If the attacker conducts this attack in real time, he or she can make it more effective by making a network with the same name as a network your phone knows. By capturing your phone's probes, he or she can see these networks and quickly set up a malicious network of the same name. Your phone will automatically connect to that network when it recognizes the name, and all your traffic will be routed through that network.

Leaving Wi-Fi on can also allow an attacker to discover a great deal about your pattern of life in the real world. He or she can see which Wi-Fi access points you have connected to and map these networks using websites like wigle.net. If you connect to a typical number of wi-Fi networks and these probes are captured, a quick analysis will likely reveal where you live, work, and the coffee shops, stores, and bars that you frequent. Several national retail stores have been caught using unique sets of Wi-Fi probes to track customers around stores to identify their shopping behavior.

To avoid this, I recommend keeping Wi-Fi off when you are not actively using it. At home, for instance, I will enable Wi-Fi long enough to download podcasts, application updates, and other bandwidth intensive data. I then immediately turn it off. It is very easy to forget to turn it off when you leave your home or office. Not only does leaving Wi-Fi on have security ramifications, your phone's constant searching for a signal can drain your battery rapidly.

In addition, when you are finished using a wireless network that you will never use again, you should remove the network from the list of networks in your phone. One complaint that I have about iOS is that it never forgets a wireless network and doesn't let you remove that network manually if you don't remove while connected to it. This means that every Wi-Fi network that you have ever connected to is still remembered and searched for by your phone. If you have had your phone for a couple of years, or have rebuilt new phones from previous iTunes backups, there may be scores of Wi-Fi networks on your phone that make your

device unique and reveal quite a lot about your pattern of life. If you wish to remove them (and I strongly recommend you do), you can reset all network connections. Be aware that this will remove all of your Wi-Fi networks as well as any credential-authenticated VPNs that you have set on your device. If you have been careless with Wi-Fi up to this point, it is not a bad idea to start fresh. To do this, go to Settings > General > Reset > Reset Network Settings.

BLUETOOTH

Bluetooth presents challenges similar to those presented by Wi-Fi. Bluetooth can be used to track your location to a very high degree of accuracy (though only over short distances from a receiver. Bluetooth traffic can also be intercepted and though the security protocols for Bluetooth have gotten better, it can still be broken by a sufficiently skilled attacker. Because of its susceptibility to attacks like Bluebugging, Bluejacking, and Bluesnarfing, Bluetooth should be turned off when not actively in use. Bluetooth can be toggled on and off by accessing the control center in both Android and iOS devices.

CELLULAR

Cellular data is the primary communications pathway for mobile phones and tablets that have a cellular data plan. By default, many applications and services on your device will want to access or use your cellular data. Allowing all applications and services to use this data has two potential consequences. Most prosaically, this uses the expensive data that you pay for each month. From a security standpoint, access to a communication pathway allows the application a way to transmit and share data in the background without your knowledge or explicit consent. Though it may do more good on some apps than others, I prefer to restrict the ability to use cellular data to only those applications and services that truly need it.

AIRPLANE MODE

Airplane mode is designed to allow you to turn off all transmit and receive capabilities (interfaces) inherent to the phone with the touch of a single button. This allows the device to be used on aircraft without risk of interfering with the aircraft's navigation and communication systems. Placing the device in airplane mode eliminates all communication, including your ability to send and receive texts, phone calls, emails, or anything else requiring a cellular or data connection.

Airplane mode may be useful for privacy and security in certain instances: if you want to disable all transmission from the phone (when having a sensitive conversation, for instance) you can do so easily with the push of a single button. It can be used to defeat location tracking by Apple, Google, or any of the apps that are installed on your phone. I am a big proponent of using airplane mode frequently. As a word of warning, this is not a one-hundred percent solution. As long as the phone has power applied (even if it is turned off), it may be accessed by entities with the requisite technology (US Government for example) and should not be relied upon to fully protect you.

LOCATION SERVICES

The absolute best practice would be to disable Location Services entirely but there are negative security consequences to that. With Location Services completely disabled, the phone cannot be tracked if it is lost or stolen. iOS offers very granular control over what applications request access to your location data. I recommend leaving Location Services on and individually selecting apps and services that can access this data. You should limit these applications to the smallest number of apps possible.

EXIF DATA

We discussed in previous chapters how metadata within photos, often called Exif data, could potentially identify sensitive data within the image files. This has become fairly common knowledge. However, many people become careless when distributing video files created on mobile devices. The following details were extracted from the hex data of a video file that I created on an iOS device.

FORMAT: MPEG-4
FORMAT PROFILE: QuickTime
FILE SIZE: 1.00 MB
DURATION: 10s 712ms
RECORDED DATE: 2018-02-15T17:46:36-0500
MAKE: Apple
XYZ: +19.369528-81.40232038.8890+161.000/
MODEL: iPhone 8
com.apple.quicktime.software: 6.1.3

As you can see, anyone that possesses this video file would know my phone make and model, the operating system installed, and the GPS location of the image capture. Free programs such as MediaInfo make this collection process automated.

CONSIDER APPS CAREFULLY

The biggest thing you can do from a privacy standpoint is limit the number of applications that you install on your phone to the absolute minimum. Each additional application you install on your device introduces new potential vulnerabilities. Before installing a new app, ask yourself if you really need it. If you decide that you do need a particular application, do your due diligence. See what it does in the background and read its privacy policy carefully.

REVIEW APP PERMISSIONS

You should verify the permissions that each app on your device is allowed access to is actually needed for the function of that app. Though changing global settings should enforce these settings for each application, it is not a bad idea to view the settings for each app individually. The most dangerous of these settings are Location Services, Contacts, Photos, Microphone, and Camera. Some applications may have a legitimate need for access to these functions that may not be readily apparent. For example, two-factor authentication apps often request access to the camera. Though this may not seem necessary the app does need the ability to scan QR codes when setting up two-factor authentication on a new account. Regardless, when in doubt deny the permission and if it interferes with the function of the app, you can temporarily or permanently allow it in the future.

A FINAL STRATEGY FOR SMARTPHONE SECURITY

Sometimes, the best solutions are the simplest. I believe that one extremely powerful, yet simple idea, is to turn your device off when not in use. Compare your smartphone to your computer. Do you shut down your computer when not in use? Do you leave it on all night every night? We need to view smartphones as computer, which they are. While you sleep or work away from your device, it is constantly communicating with several servers. It is exchanging information about your contacts, messages, and activities with numerous data collection sources. On many devices, the audio noise occurring near the unit is being recorded as a "feature" for use within apps. You may have followed my methods of having an anonymous phone. This will provide an amazing layer of security, but it will not stop the data transmissions about your alias.

If you shut your device completely down, or at least place it in airplane mode without any active connections, you prevent this data from escaping. You may choose to simply turn your phone off at night. If you use it as an alarm, disable the cellular, Wi-Fi, GPS, and Bluetooth connections. You may choose to take this to another level and shut down your device while traveling. I like both of the following strategies.

- When traveling toward your residence or workplace, turn the device off within five miles. This will prevent your cellular records from profiling these important locations. When leaving your residence or workplace, turn the device back on after passing the five-mile radius.
- If you travel extensively, turn your device off before arriving at an airport and back on when needed away from the airport in the new city. This will create a wild pattern and chaos will appear normal in your profile. If your records are ever compromised or monitored, and your device is turned off routinely, this will appear normal to the viewer.

Remember that even with a VPN on your device, it is still connected to a cellular provider. You cannot prevent them from knowing the location of the device if the cellular connection is established. Possessing a device completely in an alias name cannot stop the companies from tracking the device, but they will have no idea that you are the owner. Below, I will detail my individual configuration which may inspire you to create your own strategy.

Primary Device

Hardware: iPhone 8
Carrier: Various
Primary Alias Incoming/Outgoing Calls: Google Voice (non-personal use only)
Secondary Alias Outgoing Calls: Silent Circle
Secure Personal Incoming/Outgoing Calls: Signal
Primary Alias Text Messaging: Google Voice
Secure Personal Text Messaging: Signal/Wickr
Secure Personal Email: ProtonMail
VPN: NordVPN

NOTES: Because the iPhone is capable of operating on both CDMA and GSM networks I alternate between a variety of providers. Because I nearly always have a Wi-Fi connection, I only need a limited phone plan and go with the smallest and most economical prepaid plans available. I have no need to maintain the same telephone number for any extended period of time.

Secondary Device

Hardware: iPod Touch
Carrier: None
Primary Alias Incoming/Outgoing Calls: Google Voice
Primary Alias Text Messaging: Google Voice
Primary Secure Voice: Signal
Secure Text Messaging: Wickr
Secure Email: ProtonMail
VPN: NordVPN (different account)

NOTES: I purchased this lightly used, latest-generation iPod Touch from Craigslist. I paid more for it than most used devices of similar age and condition but am confident it is not a stolen device. I keep it turned off at all times when not in use, it is never connected to my home Wi-Fi network, none of the accounts on it are associated with true name personal accounts, and it is on a completely separate iTunes/iCloud account. This means I had to pay for some apps twice but I am OK with that.

I like that this is an iPod rather than a phone; that means a SIM has never been associated with it and it does not even have an IMEI, making me that much more anonymous. Without GSM or CDMA architecture to work with it is that much more difficult to track my location. The phone company doesn't get any of my data, either, which I really dig.

COMPUTER SECURITY: DATA-AT-REST

In this chapter, I will talk about data-at-rest. Data-at rest is the information that is stored on your computer's hard drive or on removable media when it is not being used or transmitted, which is most of the time. In the event your computer is lost or stolen, accessed by an unauthorized person, or malware is scraping your personal files, encryption will prevent any information from being compromised. This chapter will cover some basics of encryption, encryption programs, and best practices for effective employment of encryption. Let's go.

ENCRYPTION BASICS

Encrypting sensitive data is one of the single most important steps users can take in the interest of securing sensitive personal information. Unfortunately, it is also something that many users seem very hesitant to do. To the uninitiated it seems like a lot of work and may even seem to be a sign of paranoia. Though encryption does require a very minor shift in how users think about their data, it isn't a great deal of work to set up initially. After it is installed and running it is almost completely transparent to the user.

Before we move into the specifics of encryption programs it is important to discuss the two broad categories of encryption that are used to protect data stored on a computer. They are file-level and full-disk encryption. I believe that it is important to understand the benefits and limitations of each, and to use each where appropriate.

FILE-LEVEL ENCRYPTION: File-level encryption allows you to create a file "container" that encrypts all the files within it. When you "close" the container, all the files within it are encrypted, restricting access to anyone who does not possess the correct password. This is perhaps the most commonly implemented type of encryption employed by the average user. I use file-level encryption for some applications but consider it generally inferior to full-disk encryption.

FULL-DISK ENCRYPTION: Full-disk encryption (FDE) offers the ultimate security for the data on a computer's hard drive. Full-disk encryption means that the entire hard drive, including all files, the operating system, applications and programs, and anything else on there is encrypted when the computer is turned off. The only portion of the hard drive that is left unencrypted is the boot loader, a very small portion that allows the computer to accept the entered password and begin the boot process upon startup.

Most users assume that file-level encryption is sufficient as long as all versions of sensitive files are encrypted. Unfortunately, this is fairly inaccurate. While using your computer, it stores various versions of files such as saved "recovery" versions, records of filenames that you have accessed, internet browsing history, and a great deal of other sensitive information, the majority of it without your permission or knowledge. If your computer is unencrypted, this information can be exploited to reveal sensitive information about you. This information may reveal the names, sizes, and even the contents of your most sensitive encrypted files. For example, if you edit a Microsoft Word document, it will automatically create an AutoSave version that can be recovered in the event your computer crashes or you accidentally close without saving. Unless you specifically change the location to which this file saves, it is written unencrypted to your hard drive in a nebulous location that is not always easy for the average user to locate. Full-disk encryption prevents this kind of leakage from being accessed and exploited.

Encryption of the entire hard drive is beneficial for several other reasons. Full-disk encryption is the most transparent form of encryption. After the user initially enters a password and the computer boots, it functions as it normally would. And if your computer is lost or stolen, no information can be recovered from it. When a thief or attacker turns the device on a password prompt will appear, and the computer will not boot up until the correct password is entered. If the hard drive is removed and plugged into another device as an external hard drive, or if the computer is booted with another operating system like a bootable DVD (two common techniques to get around operating system passwords), all of the data on the computer will still be encrypted and inaccessible to the attacker.

Though some users possessing some familiarity with encryption consider full-disk encryption overkill, I firmly believe it should be the standard. Full-disk encryption is the simplest form of encryption to use. Though setup may be a bit more daunting, the simplicity of its day-to-day use (especially in comparison to file-level encryption) far outweighs the hassle of encrypting it in the first place. Once installed and running, FDE only required a single password (when booting). It is totally transparent from then on, and offers total protection whenever the device is powered down.

Users should also recognize there are downsides to everything, and FDE is no exception. There is a degradation in system performance when using any form of encryption because the computer must decrypt everything on-the-fly as it is used. I have found this reduction in processor power to be minimal, though your circumstances may vary depending on your processor speed, the encryption algorithm you use, and some other factors. Power users who depend on their devices for processor-heavy functions like video editing or graphic design may find this slow-down noticeable but the overwhelming majority of users will not.

FULL-DISK ENCRYPTION ON REMOVABLE STORAGE

Full-disk encryption can apply to system and non-system drives alike. System drives are the hard drives upon which the computer's operating system resides and from which it runs; non-system drives are other disks that are connected to the computer such as auxiliary internal or external hard drives, SD cards, and USB flash drives. If you do not enable full-disk encryption for your system drive we highly recommend enabling it for your non-system drives and devices, especially those with which you travel. USB flash drives are notoriously easy to lose, and the loss of one containing sensitive data can be extremely damaging.

ENCRYPTION ALGORITHMS: There are three encryption algorithms that are used with the programs that will be discussed in this chapter. They are AES (Advanced Encryption Standard), Serpent, and Twofish. AES is currently the United States Government's only approved algorithm for protection of classified information.

The algorithm that underlies AES was selected by the National Institute of Standards and Technology (NIST), in a contest to transition the US Government to a new, improved algorithm from the elderly and inferior 3DES. After selection by NIST the AES algorithm was further vetted by the National Security Agency (NSA) before being certified for the protection of classified information in 2003. Currently there are no known workable defeats for AES.

Serpent and Twofish were both finalists in the AES competition, and both are very strong algorithms. While some of the programs discussed below will allow you to use cascaded algorithms (i.e. AES encrypted by Serpent, which is then encrypted by Twofish), AES is currently susceptible to no known defeats, as is widely believed to be more than sufficient. While I leave it in the hands of the user to decide which algorithm he or she trusts, I add a morsel of food for thought. Cryptanalysts are probably much busier working on defeats for AES than they are for Serpent or Twofish because of the ubiquity and popularity of AES. For this reason, we consider using all of the algorithms for different things.

VERIFYING FILE INTEGRITY

Verifying the integrity of a computer program before installing and using it is incredibly important, especially for security software. Verifying the program ensures that it has not been modified. While a modified or look-alike version of more conventional software is almost certainly an attack vector for malware, modified versions of security applications are typically more insidious. A security application that has been modified will probably have no immediately obvious indicators that it has been tampered with. The program will function normally and appear to do all of the things it was designed to do. The changes made to it will be visible only to someone closely examining the source code. The purpose for such a modification would be to weaken the security it offers or insert a backdoor. This is unacceptable if you are truly relying on a security program to keep your data safe.

The simplest way to ensure you are getting the original, unmodified version of the application is to verify its checksum. Every file created in Linux (or any other operating system) has a checksum.

A checksum is simply the product of all the 1s and 0s of a program when hashed through a cryptographic algorithm. Hashing produces a reliable output code that will be of a consistent length, and will not change, no matter how many times the program is copied, moved, or renamed, as long as its underlying source code remains the same. If even the slightest modification has been made to the code, the checksum will also change drastically. The example below shows the difference even very subtle changes to the word “hello” can make when this text is hashed using the MD5 hashing algorithm. Even though only one letter has been changed in each example of the word, you will notice that the output product for each is drastically different.

hello: 5d41402abc4b2a76b9719d9111017c592
Hello: 8b1a9953c4611296a827abf8c47804d7
hellO: 06612c0d9c73d47a7042afd7024d7c82

If you download a program and the checksum is not what it should be, you should not rely on that software. To verify a checksum, you must have access to a known good checksum to compare it with. This checksum should not come from the same website from which you downloaded the program. If you have been redirected to a look-alike site from which you are tricked into downloading a modified version of the program, it is reasonable to assume that the checksum on that site reflects their modified version of the software. A better option would be to get the checksum from a trusted, unaffiliated, third-party site. It is also important to use a checksum that has been calculated using a hashing algorithm that is secure.

VERACRYPT

Until May of 2014, TrueCrypt was the de facto encryption du jour for individual and home users. TrueCrypt offered very robust encryption, was exceptionally feature-rich, and was fairly user-friendly. TrueCrypt could be used for both full-disk and file level encryption, and could support various two-factor authentication schemes, was available for Linux, Mac, and Windows, and was totally free. Unfortunately, the developers of TrueCrypt decided that they would no longer support the program and dropped it in a rather public and alarming manner.

The TrueCrypt homepage (www.TrueCrypt.org) was redirected to a warning page that advised, “WARNING: TrueCrypt is not secure as it may contain unfixed security issues”. The site then went on to detail the procedure to migrate data to a different encryption program. In conjuction with this warning, one final version of TrueCrypt, version 7.2 was (and still is) offered. This version is not useful for encryption purposes as it only allows users who had previously used TrueCrypt to decrypt their files if need be.

VeraCrypt is a fork of TrueCrypt and is almost identical in appearance and function. Some functions have been changed “behind the scenes” that make VeraCrypt more secure than TrueCrypt (assuming they have been implemented properly), but the biggest benefit is that bugs in the code are patched. This is not the case with TrueCrypt, which will never again be patched. VeraCrypt is free and available at https://veracrypt.codeplex.com/.

VeraCrypt can be used on Qubes, and I highly recommend you do so for any sensitive files. Especially for your KeePassX password manager database. Never leave any sensitive files unencrypted on your hard drive, as that is a serious security risk and could lead you to a lot of headache. In fact, I recommend you don’t even download files if not to an encrypted container.

VeraCrypt offers the ability to create file-level encrypted containers (called “volumes”), hidden volumes (which are built inside standard volumes and offer a layer of plausible deniability), and full-disk encryption for the system drive and non-system drives. It is also capable of encrypting a partition or entirety of a USB flash drive or hard drive. Further, with VeraCrypt you can use two-factor authentication for volumes (using keyfiles), choose any of three very strong algorithms or use them in combination, and even create a hidden operating system on your computer.

VeraCrypt is incredibly well documented, and the 161-page VeraCrypt User’s Guide that is included in the download of the program does a very thorough job of explaining how to use all the functions available in the program. For this reason, I will not duplicate this effort here.

LINUX UNIFIED KEY SETUP (LUKS)

The Linux Unified Key Setup comes standard with Qubes OS and most Linux operating systems. Setup is prompted upon initially installing the operating system.

BACKUPS

Anyone reading this tutorial should already understand that backups are a CRITICAL component of a thorough information security posture. In the event a hard drive fails (as has happened to me before), your computer is lost, stolen, or irreparably damaged, or you mistakenly overwrite data, you have a copy. It goes without saying that backups should be encrypted at least to the level of the original data being backed up. In my opinion, if it's worth backing up, it's worth backing up twice. I don't use traditional full-image backups that record all the settings and applications on my computers. Though it would take some time and effort, if one of my computers crashes I can easily restore all of the programs on it.

COMPUTER SECURITY: DATA- IN-MOTION

Data-in-motion is information that is in transit from one device to another. This data is vulnerable to a number of potential exploits. Your traffic may be intercepted by "legitimate" entities to serve you advertising information, ensure you are complying with the Digital Millennium Copyright Act, insert tracking codes into your data packets, or for other reasons. On the other end of the spectrum, data may be intercepted by an attacker. A malicious actor may sniff (intercept) your packets, set up a man-in-the-middle attack, or launch an evil-twin attack, depending on what you are most vulnerable to. One of the most important steps you can take to protect yourself is to encrypt all of your data-in-motion to the extent possible. This is possible through a number of methods including Secure Sockets Layer (SSL), and Transport Layer Security (TLS), high quality modern Wi-Fi encryption protocols, and the use of Virtual Private Networks and the Tor network. These factors working together can protect that data while it is in motion from one place to another.

SSL AND TLS

Two protocols, Secure Sockets Layer (SSL) and Transport Layer Security (TLS), are the first line of defense in securing your data-in-motion. These two encryption protocols rely on asymmetric encryption. This is a form of encryption where the site to which you are connecting and your computer negotiate an encryption key for the information they will exchange. Websites encrypted with SSL or TLS are "HTTPS" sites and are considered secure. In addition to websites, connections to mail clients, online calendars, data transferred between devices, and other services like Voice Over Internet Protocol (VOIP) and instant messaging applications are frequently encrypted with one of these protocols.

Transport Layer Security is an upgraded version of the aging SSL protocol and provides very robust encryption for data-in-motion. Most reputable sites should employ TLS, though some still rely on SSL 3.0. Despite the differences in the two protocols, many still refer to both generically as “SSL”, making things somewhat confusing. (In order to simplify here, we will refer to all such connections as SSL/TLS). Until early 2014, security experts considered SSL/TLS to be fairly secure if implemented properly, but a litany of vulnerabilities was revealed in these protocols in recent years.

When using a site that is encrypted with SSL/TLS, it is a good idea to check the certificate of the site if you have any question whatsoever about its authenticity, or maybe even if you don’t. Clicking on the padlock icon (shown during encrypted connections) just to the left of the address bar of Chrome, Epic, Firefox, or Safari will display a small amount of information about the site you are visiting.

VIRTUAL PRIVATE NETWORKS

A Virtual Private Network (VPN) provides a good mix of both security and privacy by routing your internet traffic through a secure tunnel. The secure tunnel goes to the VPN’s server and encrypts all the data between your device and that server. This ensures that anyone monitoring your traffic before it reaches the distant server will not find usable, unencrypted data. Privacy is also afforded through the use of a distant server. Your traffic that exits the VPN’s server does so in plain text (or ideally, still encrypted with HTTPS if you are visiting an SSL/TLS capable site) en route to the destination site, but it is mixed in with the traffic of scores or hundreds of other users. This makes it much more difficult to distinguish your traffic from all the rest. Also, because your traffic appears to be originating from the VPN’s server, websites will have a more difficult time tracking you, aggregating data on you, and pinpointing your geographic location.

Virtual Private Networks are not a perfect anonymity solution. It is important to note that VPNs offer you privacy, NOT anonymity. The best VPNs for privacy purposes are paid subscriptions with reputable providers. Though some providers take anonymous payment in the form of Bitcoin/Monero or prepaid gift cards, it is

difficult (though not impossible) to create an account with one of these providers without associating yourself in some manner. This will be discussed in detail later. If you log into an account that is associated with your true identity this login can be associated with your VPN account. Additionally, if you use the VPN from your home's internet connection, the VPN provider will be able to capture your IP which can be used to identify you.

There are several excellent paid VPN providers out there and I strongly recommend them over free providers. Free providers often monetize through very questionable means, such as data aggregation. This compromises one crucial benefit of a VPN: privacy. Paid VPN providers monetize directly by selling you a service. Reputable providers do not collect or monetize data. Paid providers also offer a number of options that will increase your privacy and security. The first option you should pay attention to is the number of servers they have.

EXIT SERVERS: Most reputable VPN service providers will have a number of geographically remote servers from which your traffic will exit. When you visit a website, your traffic will appear as originating from the VPN's server IP. VPN services with a number of servers to choose from give you the ability to switch servers if one is exceptionally slow, as may be the case depending on the number of users on that server and your distance from it. Further, if you are traveling to a country that has internet restrictions and you cannot access certain websites, connecting to a VPN server in another country can allow you to bypass these geographic restrictions. When using a VPN, ensure that you patch the WebRTC vulnerability in your browser (See the chapter on Web Browser Security in the beginning of this tutorial). This vulnerability allows websites that you visit to capture your true IP address despite the use of a VPN.

ENCRYPTION: Another set of options a good VPN provider will offer is the ability to choose between a variety of encryption and tunneling options. These will typically include OpenVPN, IPSEC, L2TP, and PPTP. This versatility is desirable because although most VPN services will work well cross-platform, some devices may not work with certain protocols. Further, some VPN providers even sell routers or allow you to set up your own with their VPN software built-in.

This allows all of your home's traffic to be protected with a VPN connection. This is helpful, as not all devices (such as smart TVs and gaming systems) have the ability to have VPN software installed. Though most VPN providers offer several options for encryption I recommend you use the OpenVPN protocol where available. Though I have previously used and recommended IPSec, recent months have demonstrated some successful pre-computation attacks against IPSec protocol. I now believe OpenVPN to be the most secure protocol currently available for virtual private networks.

A good VPN service provider will offer a totally transparent privacy policy about the information they collect on your usage. The best ones will retain only minimal records, and although bound by law to cooperate with warrants and other legal instruments, if they do not store your information, the cannot turn it over. Minimal logging is actually used by most VPN providers to improve connection speed, performance, reliability, troubleshoot customer problems, and protect the service from abuse such as spammers, port scanners, and the execution of DDoS attacks across the service. It is important to realize that paid providers are also vulnerable to financial and legal pressure from their host-nation governments to cooperate with measures that may compromise security for all users. With that said, you should aim for VPNs hosted OUTSIDE the United States.

I also fully recommend that you, as the user, conduct your own research and find the provider that works best for your situation. There are also times when it may be appropriate to have several different VPN services simultaneously. You may wish to have one on which you do personal tasks like banking and email, and another across which you do internet browsing that you would not wish to be associated with your true name or identity. You may also wish to use different VPN service providers from time to time to limit the amount of information that could possibly be collected by a single provider, rogue employee working at that provider, or government agency with a backdoor into their servers. For this reason, I have listed several VPN providers that meet all of the criteria list above and that I personally recommend are:

1. NordVPN: https://nordvpn.com/
2. TorGuard: https://torguard.net/
3. PureVPN: https://www.purevpn.com/
4. Mullvad: https://www.mullvad.net/en/

Two other factors that are definitely worth considering when choosing a VPN are bandwidth restrictions and speed limitations, both of which can be annoying. It is also possible to build your own VPN, but I do not recommend that. It does not protect anything leaving your home, which would leave you vulnerable to Wi-Fi sniffing, packet inspection by your ISP or government agency, tracking, and other forms of interception and monitoring.

ENHANCED VPN PRIVACY: If you do desire a stronger level of privacy than a "standard" VPN setup affords there are some steps you can take to make your VPN more private. You will notice I did not say it will make you "anonymous". If you access a true name account with it, you should assume that it is now tied to your true name. You can still be browser-fingerprinted. You can be exploited through Java and Flash. Cookies on your machine can still leak data from one browsing session to the next. A pseudo-anonymous VPN can create an excellent privacy layer but it does not create true anonymity.

Each of these steps will require additional expense and effort, and a tremendous effort will be required to maintain this privacy. To have a pseudo-anonymous VPN you must first register for it anonymously. This is a difficult part; the internet connection from which you register it can compromise your privacy. I personally recommend you go to a public Wi-Fi and register with your VPN provider through that public Wi-Fi. Paying for a VPN may be somewhat easier. You can pay for all the VPNs listed above with Bitcoin, but make sure you're paying with CLEAN bitcoins that are already mixed and properly cleaned. That way it would be impossible to ever correlate that VPN with your real identity. NordVPN will also accept Monero, which would be an even further security layer. After you have registered with the VPN provider, you must exercise extreme caution to maintain your privacy.

QUBES OS: VPN SETUP

For Qubes, I personally recommend you go to the website below and follow the steps to install a custom-made VPN VM, that will block all traffic leaking from your VPN. That way, we can be sure that our true location is not being leaked accidentally. I also recommend you create 2 of those VPN VMs or 3 depending on your threat model, and chain them together for maximum anonymity. If you're having any problems setting this up, again, feel free to contact me and I will help you.

https://github.com/tasket/Qubes-vpn-support

Once you have installed your VPN on Qubes, make sure it is not leaking any of your traffic, by going to the websites below and running tests on your connection.

https://www.dnsleaktest.com/
https://ipleak.net/
https://whoer.net/
http://check2ip.com/

If your real location doesn't appear in any of these websites, then your setup is perfect.

WI-FI SECURITY

As was pointed out in the introduction to this tutorial, security and convenience are inversely related. Wi-Fi is an undeniable convenience. Negating the need for a physical cable, Wi-Fi allows us to access the internet from just about anywhere at just about any time. Intrinsic to this convenience, however is a great deal of insecurity, especially when compared with wired internet connections.

Wi-Fi is nothing more than a radio transmission that carries data packets between your computer's Wi-Fi card and the wireless router. Because of this anyone with a capable radio can "listen" in on your traffic. Simply listening in by capturing your packets as they travel to and from your computer is called sniffing. Sniffing requires some specialized (but free) software and a Wi-Fi card that can be placed in promiscuous mode (the ability to "listen" to all Wi-Fi traffic while not broadcasting). USB Wi-Fi antennas can be purchased very inexpensively and require only very little technical know-how.

While some of the techniques I will discuss below are changes made to your operating system, the majority of this chapter will deal with securing your wireless signal and best practices when using Wi-Fi. Before continuing with the security of Wi-Fi I will digress for just a moment to talk about how it is exploited.

WI-FI EXPLOITATION

Capturing packets is not terribly technically demanding and can even be beneficial. Seeing first-hand how Wi-Fi is exploited can underscore the point of how insecure Wi-Fi truly is and help you understand the importance of good encryption. Sniffing your home network is also a good way to see what vulnerabilities you have. If you are interested in learning how to do this, you will need the following:

- Software. There are various Wi-Fi sniffing programs and many of them are free. Using them often requires using a Linux operating system. Kali Linux is a penetration-testing specific Linux operating system that comes with an incredibly capable suite of Wi-Fi exploitation tools built-in.
- Hardware. The only specialized hardware you need is a promiscuous-capable Wi-Fi card. These are available online for as little as $30 on Amazon.com. As long as your computer has an optical drive or you can boot from a USB flash drive you will not need a new computer. Kali can be booted from optical or USB flash media. Or you can use it with Qubes OS itself by following the tutorial in the Qubes docs (https://www.qubes-os.org/doc/pentesting/kali/)
- Technical know-how. Though hacking Wi-Fi is relatively simple it does require some specific knowledge. The graphic user interfaces for most of the

programs consist mostly of a command prompt, so good working knowledge of Linux command line is necessary, though most of these commands can be found online.

WI-FI SECURITY MEASURES

Wi-Fi should be turned off when your computer is not actively connected to a network, and the computer should not be set to connect automatically to networks. When your computer is not connected to your network (e.g. when you are traveling), it will actively search for networks it is set to automatically connect to. This searching is not passive. Other computers can detect this searching and see the name of the network(s) with free software. If your networks are all being broadcasted through probes it is trivially easy for an attacker to set up an “evil twin” or “rogue access point” attack. To execute this form of a man-in-the-middle attack, an attacker will set up a network that has the same name as one of your trusted networks. When your device recognizes this name, it will connect to the rogue network automatically (unless you have disabled automatic connections) allowing your traffic to be routed through his or her device and potentially compromising it. Even SSL/TLS-encrypted traffic is vulnerable to a technique called “SSL Stripping”. If, on the other hand, you have disabled automatic connections, the names of your stored networks will not be available to the hacker. Even if they were, your computer would not connect to them automatically.

WI-FI SETTINGS IN QUBES OS

On Qubes, disabling automatic connections is fairly simple. You navigate to the network-manager icon, on the bottom right corner of your Qubes toolbar, it should be a little red icon. Then you go to your connection, and make sure “Connect to this network automatically when available” is disabled. It’s as simple as that. So, from that point on, you will always connect to a network manually yourself, which increases your security considerably and leaves you safe against these kinds of attacks.

BASIC ROUTER SETUP

When setting up your home's network there are some basic steps you can take to make your account much more secure than the average account. Some of these settings will require that you be physically connected to the router via an Ethernet cable.

CHANGE MANAGEMENT ACCOUNT CREDENTIALS: The first step you should take when setting up your home's network is to change the management account credentials. This account is the account you log into to change the router's settings. Anyone having access to it can turn off your encryption, view your usage logs, or take other malicious actions. The default credentials that are preset on the router are openly available information and could allow anyone connecting to your network to make changes to your router. To change these settings, log into your router by typing the router's internal Internet Protocol (IP) address into the address bar while connected via a wired or wireless connection to the router. The internal IP address for most Linksys routers is 192.168.1.1, while most D-Link and NetGear routers use an IP of 192.168.0.1. This will bring you to the administrator login page. If you have never changed your router's login credentials they are probably set to the default. Conduct an internet search for the default username and password, then change these credentials immediately using a randomly generated username and a good, strong password. By the way, sometimes the router's login instructions are written on the router itself.

You can also make it more difficult to change the settings on your router by changing the IP address used to log into it. Login credentials can be defeated, so this step makes it more difficult for an attacker to connect to the router. The IP address can be changed to anything between 192.168.0.0 and 192.168.255.255 but ensure you remember what you change it to. As soon as this change is saved and takes effect, you will need the new IP to log back into the router to make additional changes.

DISABLE REMOTE MANAGEMENT: Remote management give you the ability to log into and change the router's management system without physically accessing the

router or being connected to the router's network. When this function is disabled you may be required to physically connect to the router with an Ethernet cable to log into the management account. Though slightly inconvenient, you shouldn't have to make changes to the router very often and the security upgrade is well worth it.

ENCRYPT THE SIGNAL: Next, encrypt the wireless signal using WPA2-PSK encryption. There are several options on many routers for encryption, including WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), and WPA2 but the only one you should consider using is WPA2-PSK. WEP has been broken for years and is extremely easily defeated through an attack known as a "statistical attack". WPA has serious vulnerabilities, especially with its Temporary Key Integrity Protocol (TKIP). WPA2 is a re-engineered version of WPA offering AES encryption and the greatest security for wireless networks currently available. If your router does not offer WPA2-PSK (Pre-Shared Key) (802.11n) upgrade your router as soon as possible. Do not neglect to assign a good password to your network. Though it may take some time and effort to enter the password on your devices, it only has to be done once.

CHANGE YOUR SSID: You should also change the SSID, the name of your network that is broadcast to your devices. Though it is possible to (and some recommend this) hide the SSID, this is a fairly ineffective technique. Wi-Fi sniffers (programs designed to detect and exploit Wi-Fi networks) can easily find hidden networks. Instead, rename the network with a name that does not leak information about you.

Renaming your network is an excellent opportunity to provide some disinformation about your home. There are websites that map every known wireless network (https://wigle.net). Anyone seeing your true name attached to a network can make a reasonable assumption about the location of your residence, while false name on these websites could obscure your home address. Instead of naming your network something personally relatable to you like "NicoSellNet" or "NSell_Wi-Fi", use one of the most common names from the website above like

“NETGEAR5”, or “xfinity-wifi”. If anyone is looking for your house based on Wi-Fi networks, this will make it much more difficult to locate.

OPT-OUT OF WI-FI MAPPING: Wi-Fi networks are now mapped in tandem with other street mapping efforts such as Google Street View. This means that if your network name is collected, it can be looked up as an overlay on a map. This allows anyone to map your location, based on your Wi-Fi networks, by capturing the SSID that your computer broadcasts when searching for a network to connect to. To prevent your home network from being mapped (at least by Google), an option you can take is to terminate your router’s SSID with the suffix “_nomap” (for example: Luna_wifi_nomap). This is the opt-out for Google’s Wi-Fi network mapping. Any router SSID containing this suffix will not be included on Google map overlays that display Wi-Fi networks. Alternatively, assign your Wi-Fi network an SSID that creates disinformation as described in the previous paragraph.

DISABLE WI-FI PROTECTED SETUP (WPS): Wi-Fi Protected Setup is a convenience feature that is intended to make it easier to connect to a wireless device. Rather than entering the password when connecting to an encrypted network the use can physically push the WPS button on the router or enter a six-digit WPS code when connecting for the first time. Unfortunately, the WPS protocol is broken. No matter how strong the password on your network is, cracking the simple six-digit WPS code can grant access to the network. Disable WPS completely, even though it makes logging into your network more time consuming (though again, you only have to do this on your home network on initial setup and when you change the password).

TURN OFF THE SIGNAL WHEN NOT IN USE: In the setup menu for most routers, you can elect to turn the router’s signal off between certain hours and on certain days, at times when everyone in your home is typically asleep or everyone is gone, for example. Unless you rely on wireless IP cameras or other Wi-Fi devices as part of your physical security system, there is no need to leave your router on when you are going out of town; simply unplug it. Powering the router off lowers it profile; the less time it is on and broadcasting, the smaller its attack surface.

SCAN YOUR HOME NETWORK: Though this does not pertain to router setup specifically, it is a good step to take after setting up your home router. My antivirus application of choice (Avast) can conduct a home network scan. It will test to see if your devices are visible from the internet, check router security configurations, and ensure that your wireless signal is encrypted. You can run this scan on any network to which you are connected to give you an idea of the security of the network before you use it to transmit sensitive information.

MAC FILTERING: One security measure that is sometimes touted but is largely ineffective is MAC filtering. A MAC address (Media Access Control) is a number unique to your device, analogous to its electronic ID. Filtering MAC addresses allows connections only from devices on a "whitelist" (a preapproved list of trusted devices). While MAC filtering is good in theory, it is very easily defeated through MAC spoofing, a technique used by attackers to capture your MAC and assign it temporarily to their device. This technique is not especially difficult to do, especially by anyone with the ability to crack your (WPA2) encryption. Additionally, MAC filtering requires you to log into the router and update the whitelist each time you need to connect a new device.

A technique that is allowed on many routers similar to MAC filtering, though slightly less onerous, is to limit the number of devices that may connect at a given time. This is intended to keep networks uncrowded to manage bandwidth, though you will occasionally hear it listed as a security measure.

BEST PRACTICES FOR UNTRUSTED/UNENCRYPTED NETWORKS

There are times when it may be necessary to use an untrusted, unencrypted wireless network. While ideally you would never use such a network, the convenience of such networks makes them hard to resist and there may be situations in which you have no choice but to work from one. Some basic best practices when using these networks (if you must use them) can make your browsing much more secure.

ABSOLUTE BEST PRACTICE DON'T USE THEM: Again, Wi-Fi is terribly convenient and it can be hard to resist the urge to connect and watch YouTube, download your podcasts, or log in and get some work done while you wait to board your flight. The risks of using untrusted networks are very high though. If at all possible avoid using them and instead tether your phone or better yet, wait until you can use a trusted connection. If you can wait to use the internet until you get home or at least to your hotel, where you can likely use a wired connection, do so. If not, do not enter any sensitive information (like login credentials) on that network, and follow the steps listed below.

CONNECT TO THE RIGHT NETWORK: Every day criminals and hackers set up fake wireless access points to lure the unsuspecting into connecting to them. This is often done in public spaces where dozens of Wi-Fi networks exist and a free hotspot does not raise much suspicion. With names like "Free Wi-Fi" or "Public Hotspot", these insecure connections are used naively by many who treat them no differently than their home network. Unfortunately, many of these are merely traps to capture login, bank/credit card, and other sensitive information. When you check into a hotel, visit a coffee shop or bookstore, or use Wi-Fi at a public library, ask someone who works there which network you should use. If two or more networks have very similar names, take a closer look at the names. If you have any doubt whatsoever, do not connect. It is worth the hassle to ensure you are on a legitimate network.

USE A WIRED CONNECTION IF AVAILABLE: Many hotels offer in-room, hard-wired connections. Some coffee shops offer wired connections, too. Using a wired connection will not make you invincible, but because of the switching involved in transmitting and receiving packets it does make intercepting and exploiting your traffic much more difficult. It also reduces the likelihood of you connecting to a phony network to almost nil. Capturing Wi-Fi packets is notoriously easy and can be pulled off by even unskilled attackers, but attacking a wired network is much more difficult. There are still many exploits against wired connections, but they are far fewer in number and require far more technical know-how. Also, be aware that even if traffic over a wired network is not being maliciously attacked, your packets are still vulnerable to inspection on the router to which you are connection, and by

the internet service provider. This is a major consideration if you are working in a country where your threat model adversary is a nation-state actor who monitors the country's internet, such as Egypt, Iran, North Korea, or the United States.

USE A VPN OR TOR: Using a virtual private network or Tor is one of the best security measures you can take if you must connect to any untrusted network, wireless or wired. While it does not prevent your packets from being captured, it will ensure your traffic is encrypted from your device to the exit server. Any packets that are captured on the local wireless network will be encrypted and therefore unusable. Using one of these measures will protect you against inspection by both the owner of the router (i.e. the coffee shop or hotel) and the internet service provider. If you have a VPN for work that you must log into to access your office's server, you can probably connect to it before accessing the internet from an unsecured Wi-Fi. Even though it will not protect your traffic from your office's IT department, it will secure your connection and prevent the packets from being captured in plaintext locally.

DO NOT OPEN FILES: Running more applications means presenting more attack surface. When using an untrusted network, you should be exceedingly cautious about opening any attachments you download or running any applications other than the web browser you are using on the network. This will lessen the chances of information being automatically sent by these applications over an unsecure connection.

If you will be using a certain network frequently in the future and would like to leave it as a known network, change the settings so that you must manually connect to it. This will eliminate your attack surface for evil twin attacks, and reduce information leaked about your Wi-Fi networks.

MAC ADDRESS SPOOFING

Every internet connection possesses a MAC address. It is assigned to the hardware element of the connection such as the Ethernet port or the Wi-Fi chip. This is hard-coded into the boards and broadcasted to the first router connection. It is unlikely for online services, such as websites, to ever see this information. However, internet service providers, wireless hotspots, and public tracking systems collect these details at all times. There are numerous ways to spoof a MAC address. Some prefer a terminal solution with system commands. Many prefer applications that automate the process. Below is the tutorial for anonymizing your MAC address on Qubes.

https://www.qubes-os.org/doc/anonymizing-your-mac-address/

COMMUNICATIONS SECURITY: EMAIL

Ladar Levinson, founder of the now-defunct Lavabit encrypted email service once stated “If you knew what I do about email, you probably wouldn’t use it”. Email is not as private as many of us have long assumed it to be. For decades, the assumption around email is that it is essentially a private communication between two parties. The analogy that is commonly drawn is that email should be like a letter mailed between two parties: the email is sealed by the sender and opened by the recipient with the understanding that any given email could be selectively opened by a third party. This myth has largely been dispelled by the Snowden leaks, and many average individuals are now much more aware of the lack of privacy inherent in email communication. In reality, email less like a letter sealed in an envelope and more like a postcard that anyone along the way can read.

Email is accessible to many parties between the recipient and the send, including law enforcement and intelligence agencies, the email service provider, and malicious third-parties. For all intents and purposes, email should be treated by the sender as a matter of public record. I assume as a matter of course that every

email sent through a mainstream provider is read by someone other than the intended recipient (or at least scanned by several computers). As a result, I am very hesitant to send anything via these channels that I would not wish to read alongside my name in the news.

There are two basic categories of “secure” email. The first is what most people typically think of when they imagine email encryption: emails that are encrypted end-to-end between the sender and the recipient and are not accessible by the mail provider. This is what I consider to be the safest and most secure form of encrypted email, even though this form of email is typically more complicated to use. I call this category “End-to-End Encrypted Email”. The second category of email encryption is less secure; the emails themselves are not necessarily encrypted end-to-end. All emails stored with such a service, including those in the box, sent, draft, and trash folders, are stored encrypted on the provider’s servers. They are not “scraped” for marketable data and their contents are safer from prying eyes. I refer to this category of email as “Securely Stored Email”.

END-TO-END ENCRYPTED EMAIL OPTIONS

One of the huge problems with encryption for email is the problem of key exchange. It would be simple to encrypt a file with VeraCrypt and email it to another party, but it would be difficult to exchange the password for that file without sending it unencrypted in some form or fashion. Sending the password in plaintext (whether through email, text message, voice phone call, snail mail, etc.) would leave it vulnerable to interception and compromise the integrity of the entire system. At best, it leaves all participants with some level of doubt about the security of the system. Meeting in person to exchange the key would perhaps be the safest method of symmetric key exchange. This may not be possible and is rarely feasible. Because of the problem of key exchange, email encryption typically relies on a wholly different encryption model than that used to protect data-at-rest. This encryption model is known as asymmetric or public-key encryption.

Asymmetric encryption solves this problem rather elegantly by using a pair of keys. Instead of a single key that is used to both encrypt and decrypt, such as the symmetric keys used by VeraCrypt, an asymmetric keypair consists of a public key and a private key. Each has a separate and distinct purpose. The public key is used to encrypt messages to the recipient, and the private key is used to decrypt the same message. For example, if Michael wanted to send an encrypted email to Justin he would download Justin's public key. Michael would then use Justin's public key to encrypt the message to Justin. When Justin receives the email, he must have his own private key and password to decrypt the message. When Justin responds to Michael, he will encrypt his response using Michael's public key. The response can only be decrypted using Michael's private key.

Because the public key can only be used for encryption, it is not secret. Public keys can be posted on websites and blog, hosted on purpose-built key servers, or emailed freely. The interception of the public key makes no difference as it cannot be used to decrypt anything. The private key, on the other hand, is secret and should be very closely guarded. The private key can be used to decrypt anything encrypted with the public key. The compromise of a private key means the compromise of all your incoming messages that were encrypted with your public key, including all historical communications until you revoke it with a revocation certificate.

This system of asymmetric encryption has been around for many years. Unfortunately, it has traditionally been unwieldy and difficult to implement. Until recently, email encryption has required a complicated process to set up and use. While this was not necessarily a problem for the security conscious and technically literate, it was difficult to convince anyone else to implement encryption. Email encryption requires participation on the part of both sender and recipient. For years, email encryption was implemented only by very few security-conscious users. Fortunately, a new breed of encrypted email providers has proliferated. These new providers automate much of the encryption process.

I believe that the automation of encryption is very important. One of the most commonly used forms of encryption for internet traffic is the HTTPS protocol. It is so commonly used because it is transparent to the user and requires no technical skill or effort on the part of the user. It just happens in the background and the overwhelming majority of internet users don't even notice it. The easier encryption is to use, the greater the number of people that will actually use it. My favorite among all these new providers that are leading the way in automating email encryption is ProtonMail.

PROTONMAIL: ProtonMail is a service that automates much of the process of asymmetric key encryption and places strongly encrypted email within the reach of even average users and has a number of exciting features. The best of these is the one that is not even seen: strong PGP encryption between ProtonMail users for the body of the message and any attachments. Because all emails sent within the ProtonMail ecosystem are encrypted, ProtonMail cannot scrape emails for advertising or any other purpose.

When a user sets up a ProtonMail account, a keypair is generated for him or her and stored wihin ProtonMail. From that point, any email that is exchanged with another ProtonMail user is encrypted using these keypairs. ProtonMail still provides security against these keypairs being stolen by requiring the user keep two passwords. One of these passwords is the login password to the account and the other is required to use the private key and decrypt messages. When you register for an account on ProtonMail, you will have to later go to options and activate the 2 passwords login to make sure you are using this private key. The second password is used only once per login and the extra step is worth the added security. All messages that are stored on ProtonMail's servers are encrypted and accessible only with the decryption password.

The two-password system offers some advantages over competing providers. If a user loses both the login and decryption passwords, the account can be reset. All mail in the mailbox will be lost because it can no longer be decrypted. However, the user will still retain his or her email address. Tutanota, which is discussed later in this chapter, uses only a single password but has no access to it.

ProtonMail also provides the ability to set destruction time for messages from one hour up to six days, after which the message will be deleted from the inbox of both recipients and ProtonMail's servers. However, there is one slight issue with this. If the email is replied to, a copy of the message is saved in the "sent" folder of the original recipient. Like other ephemeral (i.e. temporary) messaging systems, ProtonMail and similar services are designed to be used with PEOPLE YOU TRUST.

ProtonMail also allows you to encrypt emails to "outside" users, or users who do not possess a ProtonMail account. The recipient of such an email will receive a link that will allow him or her to decrypt the email with a pre-arranged password. However, this creates the problem of key exchange. ProtonMail offers some other security and privacy-related features including the ability to record login time and date information, and the IP address from which the event occurred. This allows users to verify that their account has not been accessed from an unknown IP address. These logs are stored within users' mailboxes and are not accessible without the decryption password.

At the time of this writing, 1-GB ProtonMail accounts are completely free. Paid options offering additional features such as mobile applications, 2FA, aliases, the ability to use custom domains, and additional storage are also available. ProtonMail is available at https://protonmail.ch.

TUTANOTA: Tutanota is very similar to ProtonMail. It automates the PGP encryption process for both body and attachments of emails. It also offers many of the features found in ProtonMail, including the ability to encrypt attachments to outside users and set a self-destruct time on messages. Tutanota's cryptographic implementation is free and open source and open to independent audit. It also offers paid tiers that support aliases (numerous organic email addresses that forward to a single account), custom domains, and expanded storage options.

I admit to a bias toward ProtonMail, though this is subject to change at a moment's notice as systems are upgraded or security vulnerabilities are discovered. This bias is for two primary reasons. First is the password issue. Tutanota does not have dual passwords. If you lose your password, you have also

lost your account and your email address. The second is the lack of a search and the ability to store drafts in Tutanota. The absence of these features makes it unsuitable as a primary email provider.

Tutanota is still a far superior option for privacy and security over mainstream email providers and I do not discourage anyone from using it. Redundancy is good, and I have many Tutanota accounts created and ready should a vulnerability be discovered in other systems and an immediate switch becomes necessary. For more information on Tutanota and to setup an account, visit https://tutanota.com.

DISROOT: Disroot is also very similar to Tutanota and ProtonMail. The service is completely open source, 100% free, and the graphical user interface (GUI) is absolutely amazing. It uses Rainloop, a modern mobile friendly UI for email management with GPG support for easy email encryption. It also has XMPP support, which is a huge plus. It is secure, encrypted, and they promise to never track your activity, display ads, profile you, or mine your data. Which means all your emails are private. It is worth noting however, that this encryption is server-side encryption and you have no control of your secret key, which is definitely a security issue. It is still much more private than any mainstream email provider though.

Disroot is available at https://disroot.org/en/services/email.

MAILFENCE: When talking about secure and private emails, Mailfence is one of the top names that comes to mind. They are based in Belgium and have become one of the most popular email services among the security and privacy community. The service came into existence following the Snowden revelations under a belief that users have an absolute and irrevocable right to internet privacy. During the 15 years of ContactOffice's (Mailfence Devs) operation, the company's policy has always been that tracking and profiling users for the sake of government surveillance or commercialization of data is obscene and an unacceptable breach of privacy.

Mailfence is end-to-end encrypted just like ProtonMail, Tutanota and Disroot. It gives uses FULL CONTROL in managing encryption keys without any third-party plugins or addons.

It has many security features including enforcing strong password and key passphrase policy, two factor authentication, authentication log for every connection, stripping IP addresses from the email headers by default, DKIM and much more.

Definitely consider signing up with them when deciding which email provider you want to go with, as they are extremely reliable and safe. I want to make clear though, that ProtonMail is still my first choice for many reasons as I have stated above.

FULL MANUAL ENCRYPTION OPTIONS: As mentioned earlier, ProtonMail offers free email accounts that are automatically encrypted using PGP (Pretty Good Privacy) and enjoy the tremendous benefit of requiring no working knowledge of public key encryption. However, because all these providers are in-browser crypto, they are still vulnerable to Java exploits and other remote attacks against the browser. Further, neither of these options currently allow you to generate a revocation certificate. A revocation certificate allows the user to revoke his or her keypair. Upon revocation any historical or future messages encrypted with that keypair will no longer be accessible. By implementing manual PGP encryption users are given the opportunity to take email encryption out of the browser and enjoy the protection of a revocation certificate.

NOT RECOMMENDED

There are a large number of email providers that claim to be secure. In large part this is true; these services are almost always certainly both more secure and private than mainstream email providers. On the other hand, most of these services have also given up their keys to the U.S. Government and/or created backdoors. Backdoors in cryptosystems that are only available to a single party are technically impossible.

It is very likely such a backdoor is being exploited by other parties as well. Further, we do not want the U.S. Government having any kind of access to our communication devices. For this reason, the possession of encryption keys by the US Government makes their security questionable. Though I am an advocate against mass surveillance, my bigger fear is that the government will be hacked or otherwise lose control of these keys and compromise the security of all users.

I also highly recommend you shy away from proprietary cryptosystems. The systems I prefer and have mentioned here tend to use widely available, vetted PGP encryption, or another open-source cryptography. The systems that I recommended above, while not perfect, come very close. On the other hand, the systems I recommend AGAINST have backdoors or violate some basic principles. Insecure providers such as these include CryptoHaven, Hushmail, Startmail, Gmail, Hotmail, and Yahoo. STAY AWAY FROM THEM!

DESIGNING YOUR SYSTEM

So, which one of these options do I use? Since there is not yet a “one-size-fits-all” email encryption solution, I use a combination of some of the above to meet my needs. First, I maintain many ProtonMail accounts and have set up accounts for most of my technically-challenged friends, family, and even a few business contacts. This ensures that almost all of their personal communications are end-to-end encrypted and stored encrypted on the provider’s servers. Is it the strongest encryption available? No, but it is much stronger than the alternative of freely giving information to mainstream providers whose business model is data collection, and it is very easily implemented by anyone. Next, I use full manual encryption all the time. This is the strongest encryption available but sets a very high technical literacy and patience bar that few are willing to take the time to learn. This setup is used with anyone with the know-how and patience, and is always used by me when extremely sensitive information must be emailed.

This system is not perfect and requires that I check multiple email accounts throughout the day, but it is not overly onerous. To communicate directly with me via email, you will need to implement one of the end-to-end encrypted solutions.

PLEASE DO NOT USE OR LET ANYONE USE GMAIL

When you send a message to an acquaintance, colleague, family member, friend, or lover who uses Gmail, even from your ultra-secure, encrypted email account, you become a Gmail user. When you place data into the Google ecosystem, your data is collected and associated with your name, even if you do not have a Gmail account. Though I am picking on Gmail, the same can be said for Hotmail, Yahoo, and other mainstream email providers. The ones who do not monetize services directly or monetize primarily through hardware sales must make their money in some other way. This way is nearly always through advertising.

Gmail is an excellent product with excellent security, and even businesses rely on its powerful features. If there are individuals with whom you share intimate personal details, trade secrets, or other sensitive information, do not do so over Gmail if at all possible. It would be an extremely hard sell to convince many people to leave Gmail.

COMMUNICATION SECURITY: VOICE AND TEXT

Protecting your personal voice and text communications is an incredibly important step in achieving true privacy. Though the thought of all of your voice and message traffic being intercepted may seem incredibly paranoid and unlikely, recent news articles have indicated that it certainly is not. Though metadata collection was the first privacy bombshell to burst, it did not end there. I advocate encrypting the maximum amount of voice and message traffic possible. Fortunately, encrypting voice and message traffic is a fairly simple affair. In most cases it requires nothing more than installing an app, modifying your own behavior, and that of the people with whom you talk and text.

Most mobile telephone calls that occur on LTE (Long Term Evolution) networks are already encrypted by default. In fact, LTE encryption is one of the most successful cryptography implementations ever in regards to user compliance. It is completely transparent and requires no user input whatsoever – it just happens. The problem with LTE encryption is that is has avowed backdoors for use by law enforcement, intelligence, and other government agencies. Unfortunately, due to the technical nature of "backdoors", this vulnerability is also available to anyone else able to discover and exploit it. I strongly recommend implementing stronger, intact encryption protocols, even if no specific threat exists against you.

I also strongly encourage each reader of this work to convince as many friends, family, colleagues, clients, and anyone else to use these apps. When more of us use these products, we create noise for each other. If only one of us uses a particular encryption product, it is easy to single that user out and massive amounts of resources can be dedicated to exploiting that user's communications. When we all encrypt as much of our communications as possible, surveillance must become targeted again, and a good deal of our privacy is restored. I also believe that we can reach a point where these apps are "mainstream" and not considered uncommon or different, even among "common" users. So please, convince others to use these apps.

Most of the applications listed here are produced by security-focused companies and do not collect data about their users beyond what is necessary to create accounts or process financial transactions. This chapter will discuss products that will replace your plaintext voice and texting apps. I will also discuss some native iOS apps that are already encrypted that you may not be aware of. Finally, I will discuss an application that can replace instant-messaging style apps.

All of the applications here utilize your device's data or Wi-Fi connection rather than your service provider's calling minutes or texting plan. This has the benefit of reducing the data your wireless service provider is able to collect about your calling and messaging habits by cutting them out of the loop completely. It also allows you to use your device even when you do not have cellular service as long as you have a Wi-Fi connection.

Depending on your service provider, coverage plan, and your personal habits, you may be able to reduce your phone's calling and texting plan and send the majority of your calls and texts from your home's Wi-Fi. With the exception of iMessage and FaceTime, all of the applications mentioned here are supported by both Android and iOS.

SIGNAL

Signal Private Messenger is a free application, and my new favorite encrypted communication solution. Signal supports both voice calls and text messaging in a single app and is incredibly easy to use and convince others to use. There is no complicated setup, no username or password to create and remember, the app is incredibly intuitive, and resembles native phone and texting applications. Signal uses your phone's Wi-Fi or data connection. Signal has replaced the legacy apps RedPhone and TextSecure for Android and merged them into a single platform. To use Signal, simply install the application. You will be prompted to enter your telephone number for verification. The app will verify the number by sending you a code that you must enter into the application. No other personal information is required or requested.

If you allow Signal to access your contacts, it will identify the ones who have Signal installed. There is one slight downside to the way Signal identifies its users. In order for others to contact you via Signal they must have the telephone number you used to register the app in their contacts. This requires that you give out this number to others with whom you wish to use Signal. For this reason, I recommend setting up a Google Voice number that is used only for Signal, and giving that number out to friends, family, and business contacts that are likely to use Signal (or be persuaded to in the future). Even though the Signal app warns that Google Voice numbers are not supported for verification, I have had multiple successes using Google Voice for this purpose. This is not a guarantee, but if you are denied I recommend that you keep trying. If you are not planning to change your number or transition to Google Voice, then you should register Signal with your existing number.

Signal does not offer anonymity. Because it uses your mobile number to register you will be associated with the account. Even if you use an anonymous number to register the account consider the contacts to whom you provide this number. If they put you in their Androids phone's contact list by your full name this information will likely be transmitted to Google and dozens of other apps on their device. Signal also does not obscure your metadata: who you talk to, when you talk to them, and for how long. It merely protects the content of the message.

Signal is one of the best privacy-enhancing applications available, and I strongly encourage its use.

SILENT PHONE

Silent Phone is probably one of the most widely publicized encrypted voice applications in existence. Its parent company, Silent Circle, is well-known in security and privacy circles for their custom BlackPhone handset. Fortunately for privacy-minded users, the Silent Phone app is also available on iOS and Android handsets. The app is free to download, but you must pay for a subscription before you can use it. The legacy app Silent Text was recently merged into Silent Phone so users now have access to encrypted phone calls and messaging within a single app. Unfortunately, I have found little use for the messaging function since it can only be used between Silent Circle subscribers. I have had very little success convincing anyone to add $10 per month or more to their phone bill.

WICKR

Wickr is a free app that, in addition to being available for both iOS and Android, can also be used as a desktop messaging application on Qubes and pretty much any other OS. After downloading the Wickr app to your device you must choose a username and create a password. Wickr asks you for no personal information whatsoever during setup. Once the username is set up users can message each other through the very intuitive interface. Wickr can also be used to securely send pictures, videos, voice messages, and attachments from Dropbox and Google

Drive. According to the company's privacy policy Wickr messages are only stored on the Wickr server in an encrypted state, and then they are only stored unil the message has been delivered, after which they are erased from the servers.

Wickr is considered an ephemeral messaging service because your messages are deleted from both the sender and recipient's devices at a set interval of your choosing. You should be aware, however, that iOS users do have the ability to take screenshots of your text messages and photos, and anyone using the app in a desktop environment can take a screenshot. Wickr has found an inventive solution to this. When someone takes a screenshot in iOS everyone in the conversation is alerted to it and receives a copy of the screenshot. It is not a perfect solution but as Wickr points out, the app is intended to be used with people you trust. Also remember that if a user is on a desktop computer no screenshot protection exists.

The security of Wickr is incredibly good. When you send a message via Wickr it is encrypted locally on your device, with a unique, randomly-generated, asymmetric key for each and every message. When the message is sent the key is destroyed. The message is encrypted in transit to the recipient and decrypted locally on his or her device only where it is then forensically destroyed upon expiration. All data-at-rest and data-in-motion are encrypted with AES-256 and as Wickr's website puts it, "your messages are encrypted and secured during their entire lifespan". Wickr is very security-and privacy-focused and offers a number of settings to allow you to customize the app to your security needs.

JABBER

Jabber/XMPP is a server-federation-based protocol designed with openness in mind. Its security depends on you making good use of OTR as you can never be sure if servers are properly encrypted between each other. Privacy with Jabber is limited, as it is visible to various kinds of attackers who your account is talking to. Tor only helps to pseudonymize your account and hide your current location, but your social graph may still expose your identity. For a good OPSEC guide on chatting anonymously see this article https://archive.is/n116i

Tor Exit Node eavesdropping can happen if no encryption to the server is enabled. Some protocols have encryption disabled by default, some do not support encryption at all.

See also Overview about Pidgin protocols and their encryption features[1]. If encryption to the server is enabled, the Tor Exit Node can no longer eavesdrop. This fixes one problem, however it also leaves another problem unresolved.

Even with encryption to the server enabled, the server could still gather interesting information. For example:

- Account names
- Buddy list (list of contacts)
- Log login dates and times
- Timestamp of messages
- Who communicates with whom
    - If the recipient knows the sender and the recipient uses a non-anonymous account or the recipient ever logged in without Tor, this can be used as a hint for determining who the sender is.
- Content of messages - Can be prevented using end-to-end encryption.

On Qubes OS, the best and most secure way to use Jabber, is to connect to a Windows 7 RDP through Whonix using the Remmina program and run PSI+ from there. That way, you remove any possible connection of that account to your actual computer. Also recommend changing that Windows 7 RDP frequently.

TOX CHAT

Tox looks like a promising solution for secure, encrypted communications. The official client implementation is based on the Toxcore protocol library, which is very feature-rich and has a variety of functions besides VOIP. By default, Tox does not attempt to cloak your IP address from authorized contacts. However, Tox connections can be tunneled through Tor, allowing communication with others

even if they are not anonymous. Desktop and mobile client versions have been developed for every major OS platform.

In the Tox design, users are assigned a public and private key, with direct connections being established in a peer-to-peer network. Users can message friends, join chat rooms with friends or strangers, and send each other files. Everything is encrypted using the NaCl crypto library, via libsodium. Tox helps to protect your privacy by:

- Removing the need to rely on central authorities to provide messenger services
- Concealing your identity (in the form of meta-data, e.g. your IP address) from people who are not your authorized friends
- Enforcing end-to-end encryption with perfect forward secrecy as the default and only mode of operation for all messages
- Making your identity impossible to forge without the possession of your personal private key, which never leaves your computer

In Qubes OS, again, Tox is better run from a Windows 7 RDP, of which you connect to using Whonix and the Remmina program. Tox is much more secure than Jabber, and I personally recommend it over any other instant messaging service. It is currently the safest way to communicate instantly online. If you have any problems installing Tox in your Windows 7 RDP, feel free to contact me.

SECURE FILE DELETION

Being able to securely delete files that are no longer wanted or needed is an important aspect of computer security. If your device is fully encrypted this is less of a concern as no files, deleted or otherwise, will be recovered from your device as long as your password remains uncompromised. You may still desire to sanitize a computer prior to reselling, donating, gifting it, or trashing it, and if you do not have full-disk encryption thorough deletion is especially important. You may just prefer to know everything is gone once it has been deleted, as I do.

First, it is important to understand that there are two types of memory in a computer. The first and most commonly referenced is non-volatile and is technically referred to as “storage”. This is computer’s hard drive and it contains data that is intended to be saved permanently. The other type of memory (which is correctly called “memory”) is Random Access Memory (RAM). RAM is considered volatile memory, or memory that dissipates and is lost when the computer is shut down.

A computer’s RAM is used to store temporary files, open programs, open files for use in on-the-fly encryption applications like VeraCrypt, run virtual machines, and a host of other things for which some short-term storage is needed. Fortunately, the data contained in RAM is typically unrecoverable within a few moments of the computer being shut down. Under certain conditions (typically very cold conditions) the information in RAM can be recovered hours later but this requires a very sophisticated (and expensive) attack. Because of this, I worry very little about what is stored temporarily in RAM. Under normal room temperatures, if you remain with your device for an hour after shut down, the chances of any data being recovered from it is vanishingly small.

I am much more concerned, however, with the security of the information that is stored on a computer’s hard drive. The storage in a hard disk drive (HDD) is persistent by design – it is where files are saved and intended to be stored for hours, weeks, or years. Unfortunately, this information can also be difficult to get

rid of when it is no longer needed or wanted. When using most operating systems the most common way of deleting a file is to select it and hit the Delete key which sends the file to the Recycle Bin or Trash. When the Recycle Bin or Trash is emptied the file is presumed to be gone forever.

Unfortunately, this does not actually remove the file from the hard drive. Deleting a file in this manner simply removes the information that the operating system uses to locate it. The operating system then allocates the space on the hard drive where the file resides as “free space”. The file is still totally intact on the hard drive until it is overwritten with new information. Though it would not seem like it, it can take an extremely long time for the entire file to actually be overwritten. In the meantime, as long as the file remain intact it is easily recovered from your hard drive, even by a novice.

HDD VS. SSD: Before we move further into this discussion it is important to note that erasure techniques do not work as well when permanently removing individual files on solid-state drives (SSDs). SSDs store data in an entirely different manner than traditional spinning-disk HDDs, and in a way that does not lend itself to easy and effective overwriting of individual files. This is not to suggest that secure file deletion applications are entirely ineffective, but merely that they are less effective and will likely leave some percentage of any given file on the disk in recoverable state. While individual files are difficult to fully delete, a full wipe of SSDs will work as well as one conducted on an HDD. If you have a device with an SSD, full-disk encryption is your primary means of data erasure. Though I do not wish to downplay the importance of FDE for all computer users, it is especially important for SSD users.

QUBES OS SECURE FILE DELETION

In Qubes, to securely delete a file, you can simply run this command on any VM, for any file.

shred -u filename.extension
Example: shred -u message.txt or shred -u folder.zip

DARIK'S BOOT AND NUKE (DBAN)

If you have reached the end of your relationship with a computer or its hard drive and wish to ensure that nothing whatsoever will be recovered from it, I recommend using Darik's Boot and Nuke (DBAN). DBAN is technically a bootable operating system that, upon startup, will wipe your entire hard drive completely. It is truly the "nuclear option", and one that should be used sparingly, as nothing will be left on your hard drive. No files, no applications, no settings or operating system – nothing. To use DBAN, download the bootable file and burn the .iso to a disk. You must burn it as a bootable disk.

When the disk has finished burning, insert it into the optical drive of the target machine and boot from the disk. DBAN is free and available at http://www.dban.org/.

STATELESS OPERATING SYSTEMS

I believe that every computer should have a selection of removable operating systems ready to boot at any time. Creating bootable USB devices is the easiest and most robust solution for this. The general premise of this method is to create a USB drive that can be used to boot an entire operating system from itself. It requires no access to the primary hard drive and cannot read or write data to it. It is completely isolated from your important data. It will not leak any usage details to your regular system. There are many scenarios that support the use of a bootable USB. Please consider the following.

You may encounter situations where you consciously, but uncomfortably, allow others to access your computer. The most common scenario could be when someone with poor security habits wants to use your device to browse the web. A friend, coworker, or relative may ask to use your laptop in order to quickly research a purchase or obtain directions to a restaurant. Telling this person that you do not want to allow this will likely cause an awkward silence. However, giving them your laptop that has been booted to a secondary USB drive has minimal risk. The password to this new operating system could be disclosed when requested. Your friend can browse the internet all day and never see one private piece of your data.

You may want an operating system that you know is always clean of any malicious software or viruses. Typical browsing behavior on a daily basis is likely to bring in some type of unwanted software onto your device. Many of you are likely using a computer that possesses an operating system that has been installed and running for several years. While your antivirus software has identified known risks, there is simply no way of knowing about the unknown variants of malicious applications. This new USB device can contain a complete operating system that has never been used for any private activity. There is no contamination from previous use. The following instructions will give you a private operating system that masks your primary operating system. It will have absolutely no negative impact on your daily computer use.

First, I encourage you to use the techniques already discussed in this tutorial to ensure that you have full-disk encryption enabled on the primary hard drive. This prevents the new alternate operating system from having access to that data. When booting to the new device, it will not have the ability to decrypt the primary device. Next, you need to choose the proper USB flash storage device. I highly recommend only using USB 3.0 devices and ports. If your computer does not have a USB 3.0 port, this method will be painfully slow, and most likely unusable. Most laptops created in the past three years have this feature. The benefit of USB 3.0 versus 2.0 is speed. The 3.0 drives can be read at over ten times the rate of the 2.0 devices.

The correct USB flash storage drive is as important as the appropriate port. While USB 3.0 is a standard, not all drives function at the same speeds. You will find very cheap devices that are technically 3.0 drives, but barely function above 2.0 speeds. You will also find extremely expensive drives that operate at nearly the same speeds as internal hard drives. Your situation and budget will determine the most appropriate drive. All of my testing for this section was completed using Sandisk Ultra Fit USB 3.0 drives. I chose these as the best option for several reasons.

PRICE: These drives are very affordable at $11 (32GB) and $20 (64GB). While I appreciate the speed of some devices at 400MB/s read and write, I do not like the $100 cost.

SIZE: I believe that a micro USB device is vital. These drives fit into the USB port and are almost flush with the computer. They can sit in the ports permanently if desired and will likely be undetected. While obviously present, it will not break during travel and does not appear suspicious.

SPEED: This drive is not the fastest available USB device. However, it possesses the best speed in its price class and physical size. I have successfully used this drive to boot multiple operating systems without any obvious lag or delay. The listed speeds are 130MB/s (read) and 40MB/s (write). My tests reveal actual speeds of 115MB/s (read) and 30MB/s (write). All are suitable for our purposes.

AVAILABILITY: These devices are very popular and readily available. My test drives were purchased from Amazon, but I have seen them at Best Buy in the past.

BAILOPAN'S USB BOOT DAILY USAGE STRATEGY

I currently view my MacBook Pro as my primary business computer. I use it for anything related to my work (not illegal). It contains all of my digital media, such as training material on the encrypted internal hard drive along with several virtual machines. I also use it to maintain my web-based business email. It is my entire business world and the contents are synchronized to an encrypted USB drive. However, I do not use it for personal issues. I have two OS X 64GB Sandisk Ultrafit drives ready to boot to the latest Mac operating system. Each of their uses are outlined below.

USB DISK ONE: This is my primary personal operating system. I use this to connect to any financial institutions. My personal documents are stored on an encrypted container within this drive that also includes FileVault's full disk encryption. My MacPass password management database is on this drive. My documents backup to a Transcend 64GB SD card that fits flush into the SD slot. It also possesses full disk encryption and the documents are within an encrypted container. I never browse to any questionable websites. I rarely browse the internet at all. This is for sensitive matters ONLY. I use this drive for my personal communication through encrypted email and messaging. Every action that is personal to me, but does not involve my illegal and legal business, happens on this drive. It is safe from malicious software.

USB DISK TWO: This is my "junk" drive. This is my environment when I want to browse to suspicious websites during research. It allows me to test unapproved applications without jeopardizing the security of my important operating systems. It is an environment where anything goes. I would never connect to anything in my real name on this drive. I also keep an encrypted clone of my business laptop on this drive.

Aside from Mac operating systems, I use three additional drives for Linux devices.

USB DISK THREE: This is a 500MB Qubes OS drive with full-disk encryption enabled. I use this for all of my illegal activity. I would never put any of my real identity accounts or information on this drive. I keep only things pertaining to my illegal businesses on this drive and have a great setup there that I will outline completely below at a different section. I keep backups of different things on this drive on another 500MB external HD with full disk encryption enabled. All of my backup files are stored inside an encrypted container.

USB DISK FOUR: This is a 16GB Linux TAILS drive without persistence. As you have previously learned, this gives me a clean system every time and helps me mask my true identity.

USB DISK FIVE: This final disk is a custom Linux Mint OS on a 16GB drive without persistence. It is the drive I use to conduct specific activities and includes a custom version of Firefox with numerous add-ons. I have an Android emulator that allows me to test mobile apps and exploit the data within them. Upon reboot, none of my activity is stored.

All of these drives are with me at ALL times. The first three are completely encrypted and offer nothing of value. The others simply have nothing of interest on them. If my laptop was stolen or broken, I can be back to normal in minutes. The drives are never left in my laptop unattended.

BAILOPAN'S QUBES OS COMPLETE SETUP

For my fraud and illegal activities/businesses setup I have first of all, a NETVM only used to connect to hacked Wi-Fi's that I have hacked myself around the region I live in, and inside this NETVM I have a custom script to fully anonymize my MAC address upon each reboot.

Then from this NETVM, my other VMs receive internet access, first to my firewall VM, then to my VPN1 VM. My VPN1 VM is a custom made one, with iptables rules

that I have written myself to ensure no traffic is escaping the VPN and revealing my true IP. With this VPN1 VM setup like this, I'd have no problem having the WebRTC vulnerability on my browsers, since the iptables rules will make sure no DNS leaks are possible anyways.

Then, from this VPN1 VM, my traffic is routed through another VPN2 VM, with a completely different VPN provider. This a huge security layer, and frankly one of the best OPSEC techniques you can have in place. The protection you will add to your setup by chaining VPNs is absolutely amazing and totally worth the cost. This second VPN VM also has custom written iptables rules that make sure my traffic is all routed through the VPN with absolutely 0 leaks. Also, I should note that both of these VPNs are used ONLY with servers hosted in countries where data protection laws are tight such as Sweden, Russia and Switzerland. I never use servers from the United States, United Kingdom or such countries.

You could optionally add another VPN VM to your setup to make it even stronger. I rather not do this because of connection speed issues, when you chain many VPNs together, your connection will significantly drop in performance, but that is totally worth it.

From the VPN2 VM, my connection is then routed to a Whonix-Gateway VM with Tor obfs4 bridges. This adds an extra layer of security to my setup and makes me feel even more safe as not even my VPN provider can see I'm using Tor as that might somewhat raise my profile.

With that Whonix-gateway VM that gives me an extremely safe internet access, I access a Windows 7 hacked RDP through a Whonix-workstation APPVM using a little program called Remmina, which is very simple to install. All you have to do is open a terminal on your Whonix-ws template and type this below.

sudo apt-get install remmina

Then, from that RDP, I install Proxifier, CCleaner, CCenhancer, and Bleachbit and do my magic. Once I'm done, I make sure I clean everything with said programs.

All of my account passwords, are stored within a “vault” VM with KeePassX. My KeePassX database is saved inside of my VeraCrypt hidden encrypted container.

If you have any questions about my setup at all, feel free to shoot me a message either on Wall Street Market itself, Dread, or my preferred option, Jabber (my Jabber address is on the bottom of every page of this guide and the cover page as well).

LAUNDERING YOUR BITCOINS

Properly laundering your Bitcoins is one of the most important aspects of your OPSEC. If you are doing any kind of illegal work, you don’t want any link to the dirty funds and your real identity. You want to appear as legit as possible, and in this chapter, I will teach you how to accomplish that to the best of my abilities. I have been doing this for many years, and so I am currently watching out for the best ways to launder my bitcoins. Currently, the best way to launder your bitcoins is outlined below.

Electrum Wallet #1 > BitBlender or SmartMix mixer > Electrum Wallet #2 > Purchase Monero with OpenBazaar 2.0 > Purchase BTC with XMR.TO > Electrum Wallet #3

Now let’s break this down and explain each component of this technique.

BITBLENDER

http://www.bitblendervrfkzr.onion/?r=29404 (ONLY WORKS ON TOR!)

BitBlender is a very popular bitcoin tumbling service. It has been around since the Silk Road days, and it’s always been a very reliable service. I have never experienced any problems with BitBlender, and I have used it more times than I can remember, with my coins tumbled through there totaling in the thousands of

dollars. I always use a new account for every tumble. And I never clean more than $10,000 dollars at a single time, to avoid having a high profile tx on the blockchain. Also, I create a new wallet every single time for these processes. The only wallet that I have that remains unchanged is my last Electrum Wallet #3 and also, every 3 months, I clean my bitcoins again, and send them to a different Electrum Wallet, safely disposing of the Electrum Wallet #3.

This is a very expensive and time-consuming setup, however, with a setup like this it'll be extremely hard for anyone to connect these coins to your real identity, unless you make a very stupid mistake.

All my coins sent to BitBlender are withdrawn from the service using their multiple addresses option, so as to break the trail of these coins even more. It is very easy to use BitBlender and you can follow the tutorial below if you need help.

https://www.deepdotweb.com/2016/10/31/use-bitcoin-mixer-bitblender/

SMARTMIX

This is an alternative service similar to BitBlender. This is a fairly new service but it looks very promising. I have used it a couple of times with great success. They have low fees, fast payouts, and also give you the option of sending your BTC through multiple addresses, just like BitBlender. All their logs are deleted after 7 days. It is available at smartmixnjmuoixj.onion.

OPENBAZAAR 2.0

OpenBazaar is an open source project developing a protocol for e-commerce transactions in a fully decentralized marketplace. It uses cryptocurrencies as medium of exchange. It was developed as a proof of concept in response to the seizure of Silk Road in October 2013. All transactions are handled through Escrow by the use of multisignatures. These moderated transactions are 2-of-3 multisig, with the buyer, seller, and a trusted third party each having a key. In June 2018,

OpenBazaar released a new feature, which is cryptocurrency trading, which now enables buyers to trade cryptocurrencies on the website, and is what allows us to purchase Monero (XMR).

XMR.TO

This is a service that allows you to pay in Monero and receive Bitcoin on the wallet address you specify.

Monero is a privacy-driven cryptocurrency that uses Ring Signatures to allow completely anonymous payments that cannot be traced on the blockchain like Bitcoin can.

XMR.TO leverages the anonymous features of Monero to provide a secure “Bitcoin mixer” that is more efficient than most, and relatively cheap as there are no fees other than the actual exchange rate. The website reads:

“As long as you follow our privacy best practices, no malicious third party can trace bitcoin payments made through XMR.TO back to you. Even if, for whatever reason, they gained full access to our database”

The XMR.TO mixer can be accessed through the Clearnet and through the Tor browser. However, it is advisable that you use the Tor Browser to ensure that your IP address cannot be tracked by anyone. This will add an additional layer of privacy to the operation.

It’s also worth noting that XMR.TO lacks some of the significant features that we usually find on regular Bitcoin mixers like time delay and multiple addresses. However, Monero’s privacy properties render these features useless. Since no one can see where the payment came from on the Bitcoin blockchain or on the Monero blockchain, there is no need to separate transactions by time and there is also no point in splitting up the amount.

CONCLUSION

To keep up with the changes in various methods of personal privacy and security, visit my my Dread profile at dreadditevelidot.onion/u/Bailopan. This is also the most appropriate way to contact me. Or you can just send me a message through Jabber.

Thank you for reading and purchasing this tutorial, I have put a lot of time, effort and dedication to creating this for all of my customers. If you have any questions regarding anything in this tutorial, don't hesitate to contact me. I will usually give you a response in under 24h. Below are all my contact details.

JABBER: bailopan@exploit.im
EMAIL: bailopan1975@protonmail.ch
DREAD: dreadditevelidot.onion/u/Bailopan