Personal Defense Options Against Opportunistic Cyber Attackers

A White Paper by Adam Merrill

Abstract

With a wide variety of hostile actors having different motivations and capabilities there's no one-size-fits-all method for keeping yourself (or more specifically, your data) perfectly secure from cyber attackers. Rather, an effective personal security plan must be developed in relation to a personal threat model- a breakdown of what you need to protect, and from whom. This paper will analyze the efficacy of a variety of common security suggestions in relation to a threat model of personal data being targeted primarily by opportunistic attackers.

Context

In the Information Age nearly every person and entity with access to the internet has some kind of personal data that they want to keep secure or private from most of the rest of the world. From proprietary business secrets to classified military projects to personally identifiable information, there is a lot of information to be secured with widely varying consequences for failure to do so. Unfortunately, there isn't any silver bullet for securing all information, or even for securing any one type of information perfectly. While it's theoretically possible to secure a piece of information from all *known* attack methods, it's inherently impossible to intentionally secure it from *unknown* (ie yet to be discovered or disclosed) attack methods.

Since no information can be 100% secure from all attempts to access it, a better approach is to define a "threat model." As defined by the EFF, a threat model is an analysis of "which people might want your data, what they might want from it, and how they might get it" [1]. Once a threat model has been defined, decisions can be made about how to minimize the risks associated with those anticipated attacks. If the model is reasonably accurate then this approach will still leave the data open to other threats that are not included in the model, but does so under the assumption that the data is extremely unlikely to be targeted by those threats, and it therefore isn't worth the resources required to protect against those threats.

"The Motherboard Guide to Not Getting Hacked" [2] provides a fairly comprehensive guide to threat modeling for the average citizen. This paper will be an analysis of their suggestions against the personalized threat model of the author.

My Threat Model

My threat model mostly consists of opportunistic hackers who would like to take control of anyone's online accounts in order to either sell them (mostly for gaming accounts), use them to send spam (often via email or social media), or access the information contained in the accounts to make money through credit card or identity fraud. These attacks are generally limited to broad phishing attempts [3], trying to use username/password combinations from data breaches to access different accounts [4], or just guessing weak account passwords. In my case I have no reason to suspect that I would specifically targeted by law enforcement, nation-state hackers, or any other advanced persistent threat, so this threat model assumes there isn't any specific need to protect against those.

What do I want to protect?

- Access to various online accounts (login details)
- Personal documents stored in the cloud
- Files stored on my personal computers and other devices
- Personal website
- Physical electronic devices
- My identity and non-public personal information

Who do I want to protect them from?

- Opportunistic hackers
- Data mining companies (like Facebook)
- Employees of the companies that I trust to store my information
- Opportunistic burglars

How likely is it that I will need to protect it?

More specifically, I will address how likely I think it is that someone will seriously consider attempting to steal or destroy these assets.

Online accounts: High probability.

Personal cloud documents: Very low probability.

Local files: Low probability.

Personal Website: Very high probability. Opportunistic hackers regularly target websites in wide sweeps to compromise them and use them to make money through spam or botnets [5]. In the past I've noticed that there have been lots of random attempts to gain access to my site's database, and I expect those attempts will continue.

Physical electronic devices: Moderate probability:

My identity and non-public personal info: High probability. Data mining is a huge (and growing) market [6], and virtually every website I visit is going to try to track me in one way or another [7]. Although I wouldn't consider my browsing habits to be particularly sensitive, I still classify that information as non-public and personal.

How bad are the consequences of failing to secure it?

[This section has been removed for reasons that are hopefully obvious]

How much trouble are you willing to go through in order to try to prevent those consequences?

[This section has been removed for reasons that are hopefully obvious]

Analysis

Updates, Passwords, and 2 Factor Authentication (2FA)

The three overarching recommendations by Motherboard are to keep software up to date, use strong and unique passwords, and enable 2FA wherever possible.

While I'm personally not always a fan of updates (they sometimes break things) I agree that they're critical for security. While there's always a possibility that an update will have a new bug that adds security vulnerabilities, I would argue that it's usually less of a risk to be vulnerable to a new bug than an old one because attackers have had more time to perfect attacks based on old bugs. And since my threat model doesn't include any advanced attackers who are going to jump at the chance to exploit a new bug, frequent updates are a good recommendation.

Having strong, unique passwords has always been one of the most important security recommendations [8], and I absolutely agree with it. You can't control how a company handles your login credentials, or ensure your credentials aren't leaked in a data breach, but you CAN make sure that any given set of credentials can't be used anywhere else or easily brute-forced. This is a relatively simple way to drastically minimize the consequences of a data breach, made feasible by a wide selection of free password managers. I wholeheartedly endorse it.

2FA is the last major recommendation made by Motherboard. I also recommend it, but with some caveats. I would agree with the statement that "any 2FA is better than none at all," [9] but only in the sense that even an easily bypassed additional layer of security still represents one more hoop for attackers to jump through before they can get to your data. However, I think it's important for users to realize that not all forms of 2FA are created equal, and you might be in for a nasty surprise if you assume that the 2FA method you choose can't be circumvented. SMS

2FA is vulnerable to SIM swapping attacks [10], email verification is vulnerable to personal device theft (where your accounts are already logged in), and even authenticator-app-based 2FA is susceptible to phishing attacks with surprisingly little effort [11]. All of these attacks can be carried out against random targets “at scale” to a certain degree, which puts them well within the realm of possibility for this threat model. So while I do recommend using 2FA (particularly for email, banking, and social media accounts), I would put a much greater emphasis on the importance of having strong, unique passwords since that drastically minimizes the potential damage from a successful attack that bypasses 2FA.

Don’ts: Flash, plugins, attachments, and public information

Uninstalling Flash is practically a no-brainer thanks to HTML5, which accomplishes pretty much everything Flash could do without the side effect of having tons of vulnerabilities.

Avoiding sketchy plugins is great advice that should be extended to avoiding any sketchy software from the internet. Specifically, I recommend trying to find a review from a reputable source for any specialized or less-common software you consider installing- if you can’t find one, stay away from it. In my experience sites like Lifehacker, CNET, or HowToGeek have reviewed nearly every piece of obscure software worth considering, and are good sources for finding legitimate software alternatives to provide the same services that an obscure piece of software promises to provide. Email attachments fall under this same mindset- if you aren’t expecting it or don’t know what it is, don’t open it!

Sharing personal information publicly can quickly lead to identity theft. I agree with the recommendation to avoid posting (or sending) ANYTHING via the Internet that you wouldn’t want the entire world to potentially see or know. But for my threat model I wouldn’t worry very much about stickers on my laptop since I’m not involved with any group or organization that I think would make me a target for surveillance. On this topic I would also add that using a free service to keep an eye on your credit score [12] (and maybe even getting notifications about changes to it) is a smart, easy way to minimize damage in the event that your identity or credit card information is stolen, and has the added benefit of helping you to be more aware of your ongoing financial health.

Do’s: antivirus, adblocker, VPN, backups, and data broker opt-out

Having an antivirus is definitely a must for any computer, but shouldn’t be considered a magic catch-all for all malware. Even more important, in my opinion, is good browsing habits [13]. Opening sketchy email attachments or downloading software from questionable websites or opening unknown web links are the primary avenues for getting malware on your device for this threat model. An antivirus software should be your last line of defense, not your first. Using a good adblocker will have the additional benefit of blocking a lot of links to unscrupulous sites from your everyday browsing, so I highly recommend that as well.

VPNs are another recommendation that I’m not fully on board with for my threat model. From a personal data security standpoint, the main benefit of a VPN is that it prevents other devices on the same network from being able to potentially see your unencrypted web traffic [14] (which they can do even if the network itself is password-protected). But if you almost

always connect to the internet from your encrypted home network (or other trusted, encrypted networks) then using a VPN isn't going to really add any meaningful additional security for this threat model- you'll mostly be wasting your money on a service you don't need. However, I do recommend using one if you travel a lot or if you regularly connect to open wifi networks. In these cases a VPN would be a good investment to prevent you from accidentally sending or receiving sensitive data over an otherwise unencrypted connection (which is independent of network encryption).

Offsite backups of irreplaceable data are critical, and full-system backups (onsite or offsite) are also a good idea to prevent time-consuming manual system reinstalls. For this threat model I recommend using a backup service that encrypts your data on their end, and then additionally encrypt any especially sensitive information manually on your end. This way any data breach on the company's end will either yield useless encrypted data or, in the rare event that the data breach is decrypted, your very sensitive files will still not be public.

For my threat model you'd only need to opt-out of data brokers if you've already put out a lot of personal information publicly for them to find- which, in my case, I apparently haven't. I would recommend checking them out to see what kind of information they have collected, and then follow the opt-out process only if they have more information than you would include on a general resume. In fact, if they all they have on you is accurate, resume-appropriate data then it may be advantageous to leave it up and just think of it as an easy way for potential employers to find or verify your contact information!

iPhone vs Android

Motherboard highly recommends getting an iPhone if mobile security is a big concern. For my threat model I don't expect anyone to be interested enough in me personally to steal (or confiscate) my phone for the purpose of getting data off it, and I don't care for iOS, so sticking with an Android is acceptable. I additionally don't think that doing a full-device encryption is necessary with my threat model since I'm already vigilant about keeping tabs on my phone, and can remotely track and/or wipe it if it gets stolen. Since I don't consider my phone to be a very big target, and because I rely on a lot of the conveniences of lower security (with some basic worst-case-scenario countermeasures) I don't think it's necessary to put a lot of extra effort into mobile phone security. Mobile antivirus seems particularly overkill with my safe browsing and downloading habits.

As an additional note on the topic of mobile security I also recommend avoiding SMS-based 2FA since there are many avenues for an attacker to intercept those codes [15].

State and Law Enforcement surveillance

Since my threat model explicitly precludes the possibility of more advanced attackers targeting me directly the recommendations in this section are overkill. While I do happen to follow some of their recommendations in this section (encrypt the occasional sensitive message, minimize social media posts, cover cameras, and avoid "always listening" devices), I wouldn't consider any of these things to be "musts" for this threat model, since they're mostly not going to be used by (or exposed to) opportunistic attackers. I mainly take these measures under the assumption that, by going into the cyber security field, I might eventually become someone

worth targeting specifically, and if that happens I want to already have these basic habits in place and not have old personal information still being stored unencrypted anywhere.

Conclusion

Not every eventuality can be prepared for, but there are some pretty basic best-practices that the average online citizen can follow to keep themselves safe from opportunistic attacks. Keeping everything updated, using strong, unique passwords for every account, and enabling 2FA for critical accounts will protect you from the vast majority of attacks and drastically reduce the consequences of the few that succeed.

Developing safe browsing habits will help you avoid the vast majority of malware on the web, and having a sturdy antivirus provides a critical last line of defense for your computer. Secure offsite backups of important data on top of that will provide peace of mind against a potential worst-case data loss scenario, and free credit monitoring will allow you to react quickly if an attacker gets enough data to commit financial fraud under your name.

Other defenses can be used on top of these, but these are the core ones I would recommend for this threat model. I give it as my professional opinion that they will provide the ideal tradeoff between convenience and defense against the opportunistic attackers described in this threat model.

References

[1] Surveillance Self-Defense. (2019). *Threat model*. https://ssd.eff.org/en/glossary/threat-model

[2] Motherboard Staff. (2019). *The Motherboard Guide to Not Getting Hacked*. https://motherboard.vice.com/en_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide

[3] KnowBe4, “What Is Phishing?,” *Phishing*. http://www.phishing.org/what-is-phishing

[4] F. Y. Rashid, “What is the biggest threat from the Equifax breach? Account takeovers,” *CSO Online*, 12-Sep-2017. https://www.csoonline.com/article/3223232/what-is-the-biggest-threat-from-the-equifax-breach-account-takeovers.html

[5] D. S., “What Is SEO Spam And How Can It Hurt Your WordPress Site,” *ThreatPress Blog*, 20-Jun-2018. https://blog.threatpress.com/seo-spam-can-hurt-wordpress-site/

[6] “Big Data Market 2018 Global Analysis, Industry Demand, Trends, Size, Opportunities, Forecast 2023,” *MarketWatch*, 31-Aug-2018. https://www.marketwatch.com/press-release/big-data-market-2018-global-analysis-industry-demand-trends-size-opportunities-forecast-2023-2018-08-31

[7] J. Balke, “What's With All the Privacy Notices and Website Cookie Notifications?,” *Houston Press*, 25-May-2018. https://www.houstonpress.com/news/why-are-you-seeing-privacy-notifications-online-all-of-a-sudden-10510337

[8] “Why Strong, Unique Passwords Matter,” *CIS* https://www.cisecurity.org/newsletter/why-strong-unique-passwords-matter/

[9] “Why Is The Authy 2FA App Free For Users?,” *Authy*, 24-Sep-2018. https://authy.com/blog/why-is-the-authy-2fa-app-free-for-users/

[10] B. Barrett, “How to Protect Yourself Against a SIM Swap Attack,” *Wired*, 17-Aug-2018. https://www.wired.com/story/sim-swap-attack-defend-phone/

[11] C. Cimpanu, “New tool automates phishing attacks that bypass 2FA,” *ZDNet*, 26-Mar-2019. https://www.zdnet.com/article/new-tool-automates-phishing-attacks-that-bypass-2fa/

[12] See for example https://www.creditkarma.com/

[13] K. Rollins, “Safe Browsing Habits,” 29-Nov-2016. https://www.bluelinkit.com/safe-browsing-habits/

[14] A. O'Donnell, “What is a Personal VPN Service and Why Do I Need One?,” *Lifewire*, 14-Nov-2018. https://www.lifewire.com/what-is-a-personal-vpn-service-2487492

[15] R. Brandom, “This is why you shouldn't use texts for two-factor authentication,” *The Verge*, 18-Sep-2017. https://www.theverge.com/2017/9/18/16328172/sms-two-factor-authentication-hack-password-bitcoin