11

TIPS FOR MANAGING USER SECURITY ON YOUR NETWORK

Being responsible for a network containing more than one user is challenging. You can't reasonably expect to manage other users' activity within your network, especially when they use their own devices. However, there are some strategies that you can use to mitigate the risks associated with multiple users.

This chapter discusses the value of strong passphrases versus passwords, password managers, multifactor authentication, and privacy-protecting browser plug-ins. It should provide the information you need to have productive discussions about security with your users.

Passwords

Having strong passwords and using different credentials for every website are the best first steps to remaining safe online. Passphrases and password managers make it harder for adversaries to guess your passwords and easier for you to manage them. *Passphrases* consist of several words, such as *libertyextremecluecustodyjerky*. You can make

them more challenging to guess by adding uppercase letters, numbers, and special characters, but generally speaking, it's better to have longer passphrases that are easy to remember than complex passwords that aren't. The same rules for typical password security still apply. Don't use personally identifiable information, such as birthdays, pets' or relatives' names, or the schools you've attended. Refrain from including words that relate to the current month or season or the name of the company you work for. Basically, avoid constructing a passphrase from easy-to-guess elements.

Passphrases are longer than passwords, making them more resilient against the brute-force attacks adversaries use to crack them. In a *brute-force attack*, the attacker tries every possible combination of characters until they find the right one. They can do this programmatically, allowing for millions (or *billions*) of password guesses per second. The shorter the password and the smaller the *keyspace* (the number of character types—letters, numbers, and symbols—available), the less time it takes to crack. For example, an eight-character password consisting of lowercase letters and numbers would take less than two hours to crack on today's computing hardware. Adding one character increases that time to more than two days, and every additional character grows the time it takes to crack the password exponentially—a 30-character passphrase's cracking time approaches infinity with the computing power available today.

NOTE *Be sure to change any default passwords for your accounts and devices. Default passwords for devices such as routers and switches (such as username: admin, password: admin) are well-known and documented, so if you don't change those in your network, you're leaving the door wide open for adversaries to infiltrate your environment. Even if they aren't well known, they're easy to guess.*

Password Managers

Use a *password manager* (also called a *password safe* or *vault*) to securely store your passwords. A password manager can store hundreds of unique passphrases that are accessed by one master passphrase. This practice removes the temptation to write passphrases down, which is never a good idea. Several password managers are available, such as 1Password (***https://1password.com/***) or LastPass (***https://www.lastpass.com/***).

The best way to convey the value of a password manager is to discuss *credential stuffing*, an attack that exploits the fact that most people still use the same password across multiple services. When adversaries obtain a list of passwords and email addresses during or after a data breach, they try logging in with those credentials on various well-known sites and services, and they're often successful because a significant percentage of the password and email address combinations are reused on other sites. Users can prevent credential stuffing by using a different passphrase for every account and storing those passphrases in a password manager.

Password Breach Detection

The free service Have I Been Pwned (***https://haveibeenpwned.com/***) lets you enter your email address and immediately find out whether it's been identified in any data leaks or breaches. **Figure 11-1** shows an example of a report for a compromised email account.

***Figure 11-1**: Example report of a compromised email account*

The service also provides ongoing updates and monitoring; you can opt to receive a notification to change your password(s) if your email address is identified in future data breaches.

Multifactor Authentication

Once you've created strong passphrases, you should implement *multi-factor authentication* (sometimes called *two-factor authentication*, *2FA*, or *MFA*) on all accounts and services that offer it. While *single-factor authentication* typically requires a combination of only two things—your email address or username plus your passphrase—MFA requires two or more factors of authentication. Usually, the first factor is something you *know*, and the second is either something you *have*, like a hardware or software token, or something you *are*, like a fingerprint

or other biometric. By requiring a second or third authentication factor, adversaries will have an exponentially more difficult task when trying to gain access to your accounts and systems. Adding a second factor may introduce a minor inconvenience to you or your users, but you'll be much more secure.

One of the most common MFA solutions uses SMS as a second factor, sending the user a text message containing a code or one-time password; they then use this code to log in to their account or perform certain types of transactions, particularly if it's from a new or unknown device or location. Everyone can receive text messages regardless of their phone model or service provider, it's free or cheap, it's more or less instant, and it alerts you to suspicious activity if you aren't actively trying to log in. The main drawback is that SMS isn't a secure technology, and it's relatively trivial for an attacker to gain access to someone's phone number and text messages.

Next, there are software solutions, including Google Authenticator, Authy, Microsoft Authenticator, and even password vaults like 1Password that offer MFA tokens. Typically, you'll download the app to your smartphone and scan or type in a code from your service provider (such as your bank or social media) to set up the app. When you want to log in, you'll check the app for an authentication token that you'll use along with your passphrase. The tokens change every 60 seconds. This is a significant improvement on SMS as a second factor, as an adversary would have to physically access and unlock your mobile device to retrieve the token. The rolling tokens also mean the access window is minimal, unlike SMS where access windows can be a few minutes long. Software tokens such as these are the most convenient and secure MFA option for many users.

Finally, there are hardware tokens, like Yubikey and Google Titan Key. If the key isn't plugged in to your computer, you can't access the encrypted or protected data. Hardware tokens are considered the most hardcore of the MFA solutions because losing your hardware key

means you can't access your data. They offer the same or better protection as a software token, as an adversary needs physical access, but they are the least convenient; most people carry their phones with them, but it's easy to leave a hardware token at home when you need it at the office. Additionally, hardware tokens can't be phished; while SMS and other similar MFA tokens can be drawn out of a potential victim via social engineering and phishing attacks, an adversary can't access your hardware key remotely.

WEBCAM COVERS

An important aside when discussing computer security is the necessity of webcam covers. Adversaries can gain access to the webcam on your laptop or computer and surreptitiously monitor whatever may be happening in front of the computer without alerting you that the camera is on. To protect your own privacy and that of those around you, invest in some low-tech, opaque tape or a webcam cover (available inexpensively from many online stores).

Browser Plug-ins

All major internet browsers, such as Google Chrome, Mozilla Firefox, and Microsoft Edge, have several browser plug-ins or add-ons to block ads and trackers (see **Chapter 7** for more on trackers) and more generally improve user privacy. The plug-ins mentioned here have been vetted and are known to be legitimate or are created and maintained by well-known and trusted sources. Browser plug-ins are designed to provide additional functionality to a standard browser, and users can choose from a wide range of available plug-ins to improve their browsing experience. It's beneficial to discuss the pros and cons of these browser add-ons with your users to enable them to make educated decisions about which plug-ins to use and which to avoid.

Adblock Plus

Adblock Plus removes “unacceptable” or disruptive ads from websites. To install this plug-in, navigate to ***https://adblockplus.org/en/download*** and download the appropriate version for your browser or device. Once it’s installed, go to the **Settings** page for the plug-in (shown in **Figure 11-2**) and select **Block Additional Tracking**, **Block Social Media Icons Tracking**, and **Disallow Acceptable Ads**. You can also choose to allowlist specific websites if you choose.

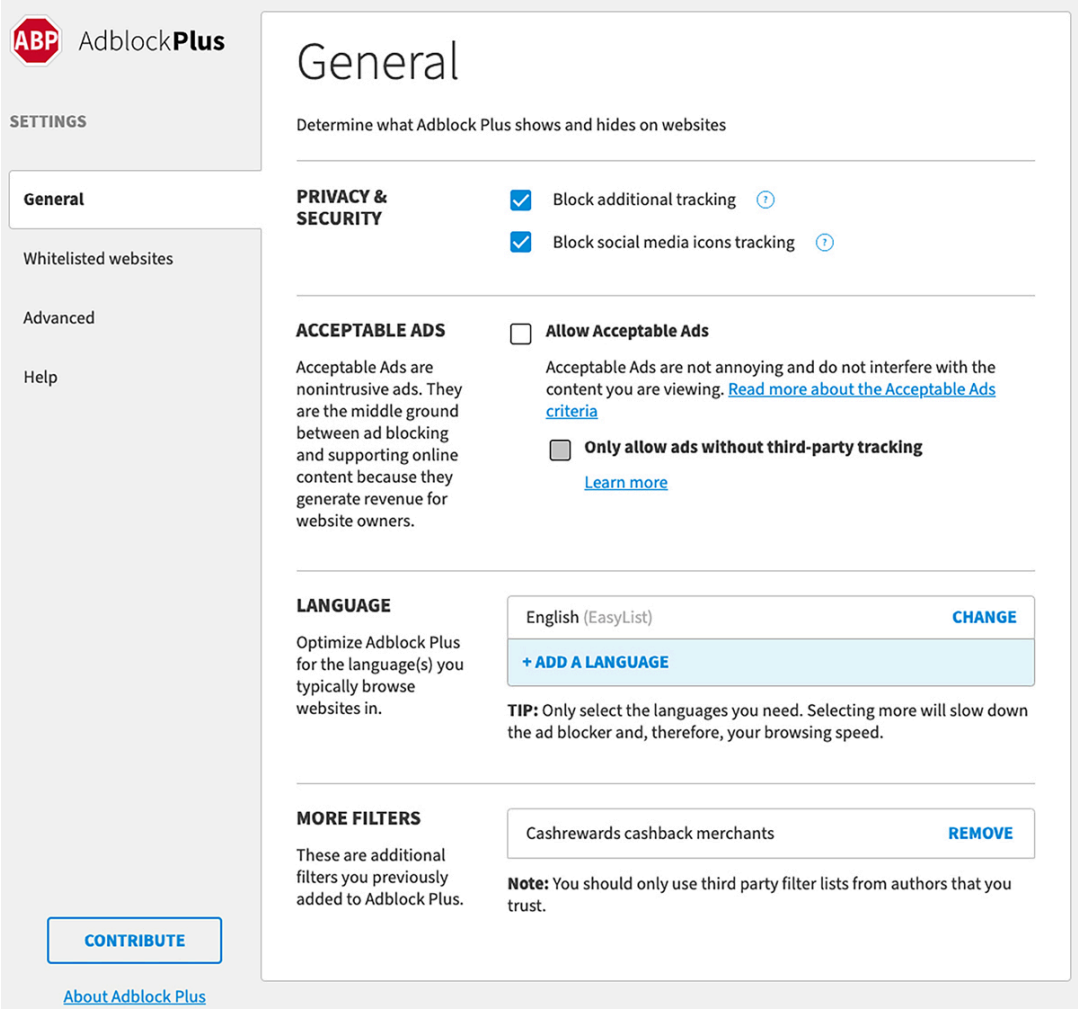

***Figure 11-2**: Adblock Plus settings*

Additional Tracking includes methods such as websites gathering your browsing habits. Blocking Social Media Icons Tracking keeps you from

being tracked by social media buttons across the websites you visit. Finally, Disallow Acceptable Ads removes all ads from websites (as much as possible anyway). All of this results in a cleaner, faster web-browsing experience.

Ghostery

Similar to Adblock Plus, Ghostery's mission is to improve user privacy by removing many user tracking capabilities on websites. To install Ghostery, browse to ***https://www.ghostery.com/*** and sign up for an account. Download and install the plug-in for your browser; once it's installed, the plug-in will function out of the box, but you can modify the settings from the plug-in menu if you so choose, as shown in **Figure 11-3**.

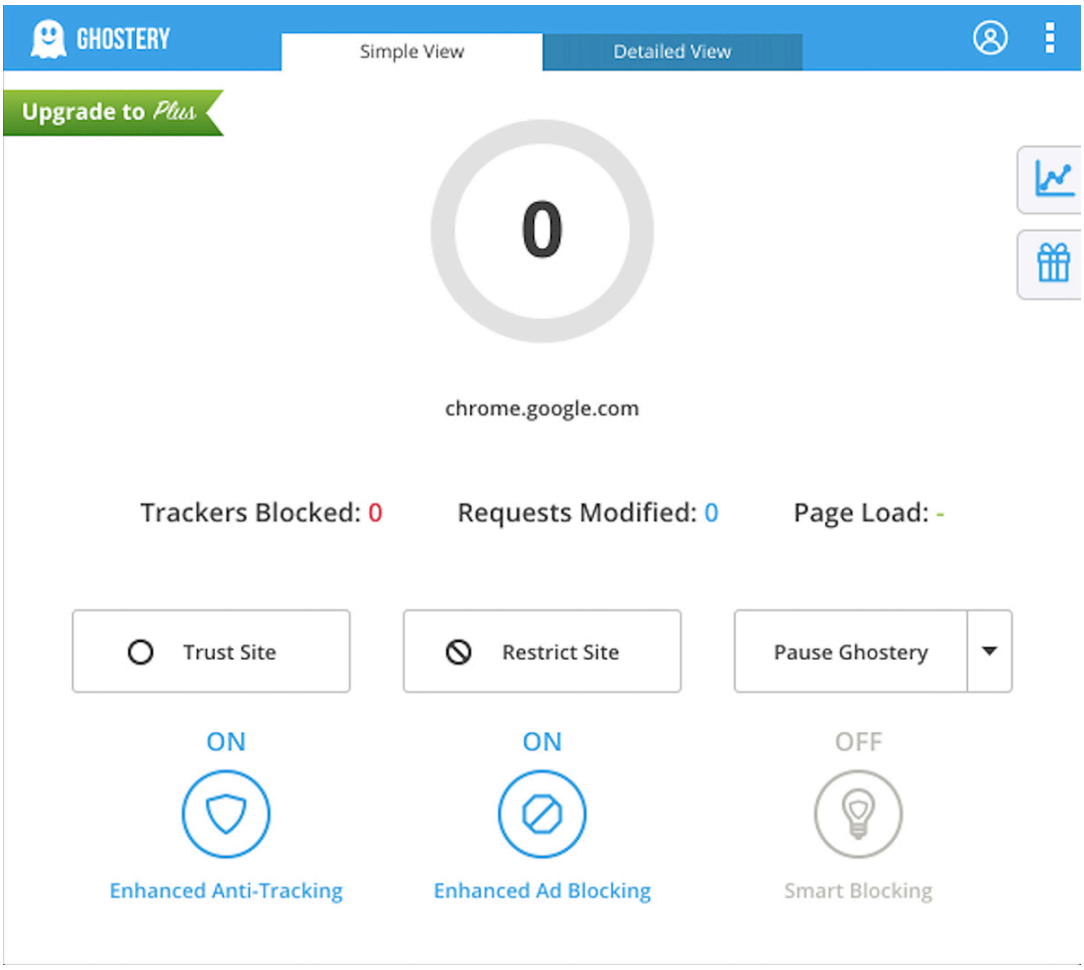

***Figure 11-3**: Ghostery settings*

If you want to manually allow or disable a specific website and pause or resume Ghostery, you can do so from this menu.

HTTPS Everywhere

HTTPS is the secure internet protocol preceded by the insecure HTTP protocol. HTTPS uses SSL/TLS to secure your internet traffic while you browse the internet. Using encryption protects your traffic so adversaries can't intercept it and decrypt it. Unfortunately, not all websites provide encryption for their users. This is where a plug-in like HTTPS Everywhere comes in handy; it provides the encryption layer for you, keeping you secure no matter what you're doing in your browser.

To install this plug-in, browse to ***https://www.eff.org/https-everywhere/*** and download and install it. From here, the options are simple: on or off (as shown in **Figure 11-4**).

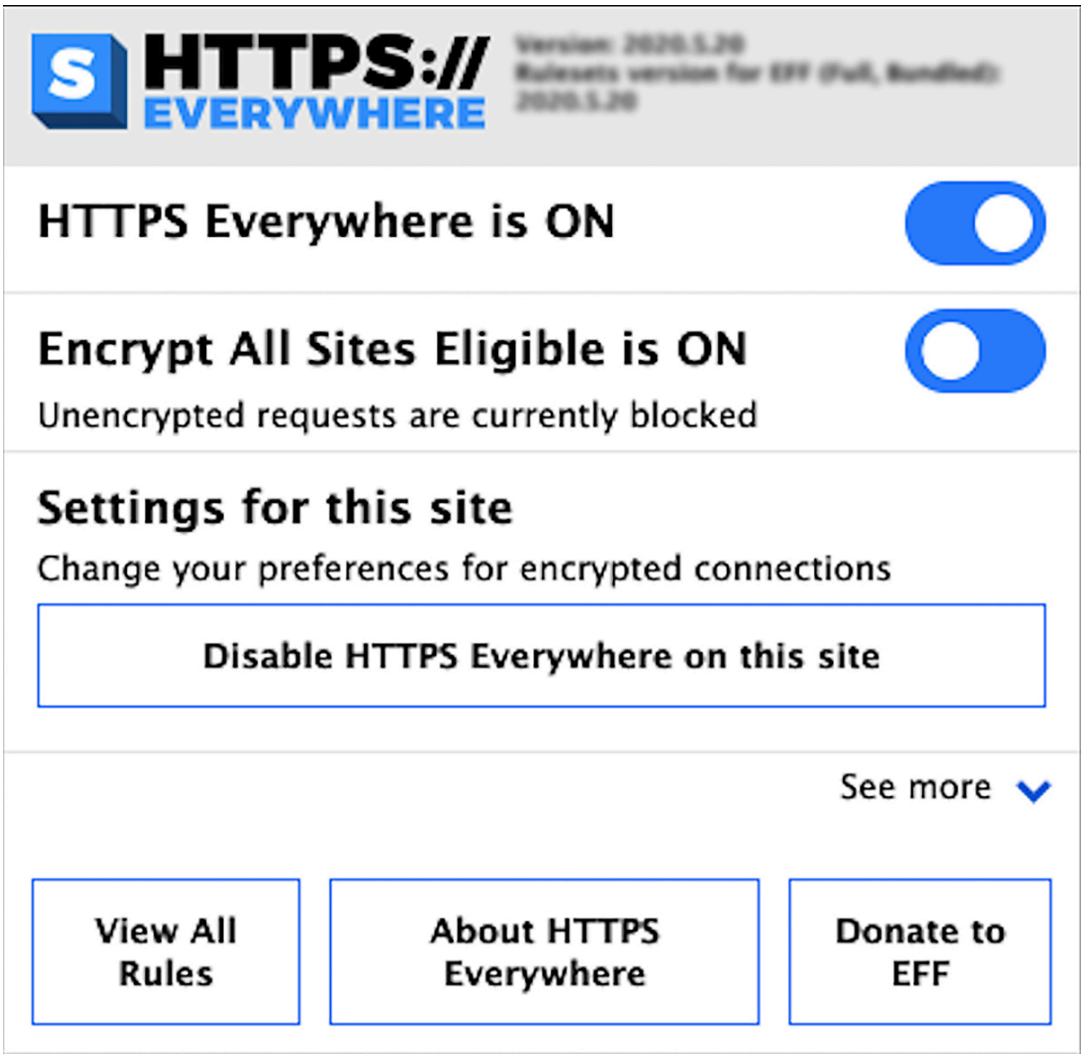

***Figure 11-4**: HTTPS Everywhere settings*

With this plug-in installed and running, you can feel safe knowing all of your browser traffic is being encrypted.

Internet of Things Considerations

We discussed internet of things devices like Google Home and Amazon Alexa and the methods by which you can mitigate the risks of smart devices using network segmentation in detail in **Chapter 2**. However, there are still risks associated with devices with always-on cameras and/or microphones that need to be considered.

Whether it's a laptop of desktop computer, a gaming console, or a smart home device, many modern endpoints have a microphone or camera (or both) built in. For a determined adversary, these devices can be used to spy on you and those around you. Therefore, wherever possible, it's best to invest in smart home devices that have a physical off switch or button for these features. If that isn't possible, consider using a webcam cover (available cheaply from many online stores) or even a piece of opaque tape to cover your web cameras when not in use. Doing so is one of the best ways to protect your privacy.

Besides covering any cameras, consider where you place and use smart home devices. In the case of smart speakers, you might choose to use them only in common areas, away from private areas like bedrooms or private offices. Consider the activities and conversations that might take place in range of the microphone and place devices accordingly.

Additional Resources

This book has been an introduction to the fundamentals of cybersecurity and ideally has enabled you to think more deeply about the security of your network and users and implement solutions to help protect your privacy. However, there are so many more resources available that delve further into these topics than could be covered here. The first I'd like to mention is ***https://chrissanders.org/***. Chris has written several books and online courses covering topics such as network security monitoring, intrusion detection, and advanced use of the ELK stack, which we briefly discussed in **Chapter 10**. If you'd like more information on any of these topics, this is a great place to start.

Another fantastic resource for anyone interested in cybersecurity, digital forensics, or incident response is ***https://dfir.training/***. This website contains a wealth of information related to tools, training courses (free and commercial), practice materials, and other resources to add to your knowledgebase and improve your security maturity.

Finally, SANS is a research and training organization with a focus on cybersecurity. At ***https://www.sans.org/***, you can find more information on their training courses, but also several resources and research papers related to tools and techniques for securing networks and endpoints, from both a defensive and offensive viewpoint.

Summary

Ultimately, your online privacy and security can be as well-protected as you like. The trade-off for being secure on the internet is one of compromising privacy, security, or both, for convenience. At the cost of slightly less convenience, you'll receive a better overall experience on the internet and enjoy a higher level of security and privacy, whether it's yours alone or shared with your users. The benefits of being secure far outweigh the inconvenience of implementing these solutions.