

Part 3

Protecting Yourself from Yourself

IN THIS PART ...

Understand how to secure your accounts.

Learn all about passwords, including how to create strong passwords that you can remember.

Protect yourself and your loved ones against social engineering.

Chapter 6

Securing Your Accounts

IN THIS CHAPTER

- » Understanding that you're a target
 - » Securing your various accounts from human error
-

The weakest link in the cybersecurity chain is almost always people, and the greatest threat to your own cybersecurity is likely yourself and the members of your family.

As such, all the technology and technical knowledge in the world won't deliver much value if you don't also address various human shortcomings.

Realizing That You're a Target

Perhaps the most significant first step in securing yourself digitally is to understand that you're a target and that nefarious parties have the desire to breach your computer systems, electronically accessible accounts, and anything else they can get their hands on.

Even if you already realize that you're a target, make sure to fully internalize such a notion. People who truly believe that criminals want to breach their computers and phones act differently than people who do not fully appreciate this reality and whose lack of skepticism sometimes leads them into trouble.



WARNING Because your family members can also impact your digital security, they also need to be aware that they are a potential targets. If your children take unwise risks online, they may inadvertently

inflict harm not only on themselves, but upon you and other members of the family as well. In some cases, attackers have managed to attack people's employers via remote connections that were compromised because children misused computers on the same networks as computers that the employees were using for working remotely.

The threat posed by such attacks is usually not that a criminal will directly steal someone's money or data, but rather that some party will seek to harm the target in some other manner — a manner that may ultimately translate into some form of financial, military, political, or other benefit to the attacker and (potentially) damage of some sort to the victim.

Securing Your External Accounts

[Chapter 4](#) discusses how you can acquire your own technology products. But using these products isn't enough to keep you cybersecure as you, no doubt, have digital data of significant value that is stored outside of your own physical possession — that is, outside of data systems and data stores under your control.

In fact, data about every person living in the western world today is likely stored on computer systems belonging to many businesses, organizations, and governmental agencies. Sometimes those systems reside within the facilities of the organizations to which they belong, sometimes they're located at shared data centers, and, sometimes the systems themselves are virtual machines rented from a third-party provider. Additionally, some such data may reside in cloud-based systems offered by a third party.

Such data can be broken down and divided into many different categories, depending on which aspects of it a person is interested in. One way of examining the data for the purposes of discovering how to secure it, for example, is to group it according to the following scheme:

- » Accounts, and the data within them, that a user established and controls
- » Data belonging to organizations that a user has willingly and knowingly interacted with, but the user has no control over the data
- » Data in the possession of organizations that the user has never knowingly established a relationship with

Addressing the risks of each type of data requires a different strategy.

Securing Data Associated with User Accounts

When you bank online, shop online, or even browse the web, you provide all sorts of data to the parties that you interact with.

When you establish and maintain an account with a bank, store, social media provider, or other online party, you gain control over significant amounts of data related to yourself that the party maintains on your behalf. Obviously, you can't fully control the security of that data because the data is not in your possession. That said, you obviously also have a strong interest in protecting that data — and, in not undermining the protections for the data that the party hosting the account has established.

While every situation and account has its unique attributes, certain strategies can help keep your data secure at third parties. Obviously, not all the ideas in the following sections apply to every situation, but applying the appropriate items from the menu to your various accounts and online behavior can dramatically improve your odds of remaining cybersecure.

Conduct business with reputable parties

There is nothing wrong with supporting small businesses — in fact, doing so is quite admirable. (It is also true that many large firms have suffered serious security breaches.) But if you search for the latest

electronic gizmo, for example, and one store that you have never heard of is offering it at a substantial discount from the prices offered at all well-known stores, be wary. There may be a legitimate reason for the discount — or there may be a scam in the works.



WARNING Always check the websites of stores that you're conducting business with to see whether something looks off — and beware if it does.

Use official apps and websites

Clones of official apps have been found in various app stores. If you install a banking, credit card, or shopping app for a particular company, make sure that you install the official app and not some malicious impersonator. Install apps only from reputable app stores, such as Google Play, Amazon AppStore, and Apple App Store.

Don't install software from untrusted parties

Malware that infects a computer can capture sensitive information from both other programs and web sessions running on the device. If a website is offering free copies of movies, software, or other items that normally cost money, not only may the offerings be stolen copies, but ask yourself how the operator is making money — it may be by distributing malware.

Don't root your phone

You may be tempted to *root your phone* — a process that allows you greater control over your device — but doing so undermines various security capabilities of the device and may allow malware to capture sensitive information from other apps on the device, leading to account compromises.

Don't provide unnecessary sensitive information

Don't provide private information to anyone who doesn't need that data. For example, don't give your Social Security number to any online

stores or doctors because they have no need for it.



REMEMBER Keep in mind that the less information about you that a specific party has, the less data that can be compromised, and correlated, in case of a breach.

Use payment services that eliminate the need to share credit card numbers with vendors

Services like PayPal, Samsung Pay, Apple Pay, and so on let you make online payments without having to give vendors your actual credit card number. If a vendor is breached, the information about your account that is likely to be stolen is significantly less likely to lead to fraud (and, perhaps, even various forms of identity theft) than if actual credit card data were stored at the vendor. Moreover, major payment sites have armies of skilled information security professionals working to keep them safe that vendors accepting such payments can rarely, if ever, match.

Use one-time, virtual credit card numbers when appropriate

Some financial institutions allow you to use an app (or website) to create disposable, one-time *virtual credit card numbers* that allow you to make a charge to a real credit card account (associated with the virtual number) without having to give the respective merchant your real credit card number. As seen in [Figure 6-1](#), some virtual credit card systems also allow you to specify the maximum allowable charge size on a particular virtual card number at a figure much lower than it would be on the real corresponding card.

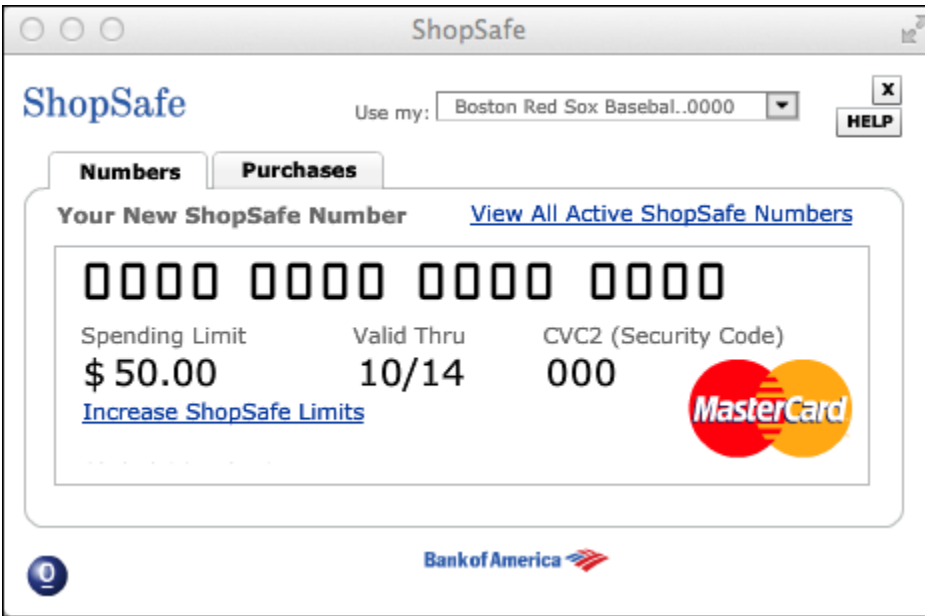


FIGURE 6-1: A (slightly edited image of) a one-time credit card number generator.

While creating one-time numbers takes time and effort and may be overkill when doing repeat deals with a reputable vendor in whose information-security practices you have confidence, virtual credit card numbers do offer benefits for defending against potential fraud and may be appropriately used when dealing with less familiar parties.

Besides minimizing the risk to yourself if a vendor turns out to be corrupt, virtual credit card numbers offer other security benefits. If criminals hack a vendor and steal your virtual credit card number that was previously used, not only can they not make charges with it, their attempts to do so may even help law enforcement track them down, as well as help forensics teams identify the source of the credit card number data leak.

Monitor your accounts

Regularly checking for any unrecognized activities on your payment, banking, and shopping accounts is a good idea.



TIP Ideally, do this check by not only looking at online transaction logs, but also by checking relevant monthly statements (no matter

the delivery method) for anything that does not belong.

Report suspicious activity ASAP



REMEMBER The faster a potential fraud is reported to the parties responsible for addressing it, the greater the chance of reversing it and preventing further abuse of whatever materials were abused in order to commit the first act of fraud. Also, the sooner the fraud is reported, the greater the chance of catching the parties committing it.

Employ a proper password strategy

While conventional wisdom may be to require complex passwords for all systems, such a password strategy fails in practice. Be sure to implement a proper password strategy. For more on choosing passwords, see [Chapter 7](#).

Utilize multifactor authentication

Multifactor authentication means authentication that requires a user to authenticate using two or more of the following methods:

- » Something that the user knows, such as a password
- » Something that the user is, such as a fingerprint
- » Something that the user has, such as a hardware token

For extremely sensitive systems, you should use forms of authentication that are stronger than passwords alone. The following forms of authentication all have their places:

- » **Biometrics**, which means using measurements of various human characteristics to identify people. Fingerprints, voiceprints, iris scans, the speed at which people type different characters on a keyboard, and the like are all examples of biometrics.

- » **Digital certificates**, which effectively prove to a system that a particular public key represents the presenter of the certificate. If the presenter of the certificate is able to decrypt messages encrypted with the public key in the certificate, it means that the presenter possesses the corresponding private key, which only the legitimate owner should have.
- » **One-time passwords**, or one-time tokens, generated by apps or sent via SMS to your cellphone.
- » **Hardware tokens**, which are typically small electronic devices that either plug into a USB port, display a number that changes every minute or so, or allow users to enter a challenge number and receive a corresponding response number back. Today, smartphone apps perform such functions, allowing, at least theoretically, the smartphone to assume the role of a hardware token. [Figure 6-2](#) shows you an example of using such an app to generate a one-time code for logging into Snapchat. (Note that smartphones can suffer from all sorts of security vulnerabilities that hardware tokens can't suffer from, so hardware tokens are still likely more appropriate for certain high-risk situations.)



- » **TIP Knowledge-based authentication**, which is based on real knowledge, not simply answering questions with small numbers of possible answers that are often guessable like “What color was your first car?” Note that technically speaking, adding knowledge-based authentication questions to password authentication doesn't create multifactor authentication since both the password and the knowledge-based answer are examples of things that a user knows. However, doing so certainly does improve security when the questions are chosen properly.

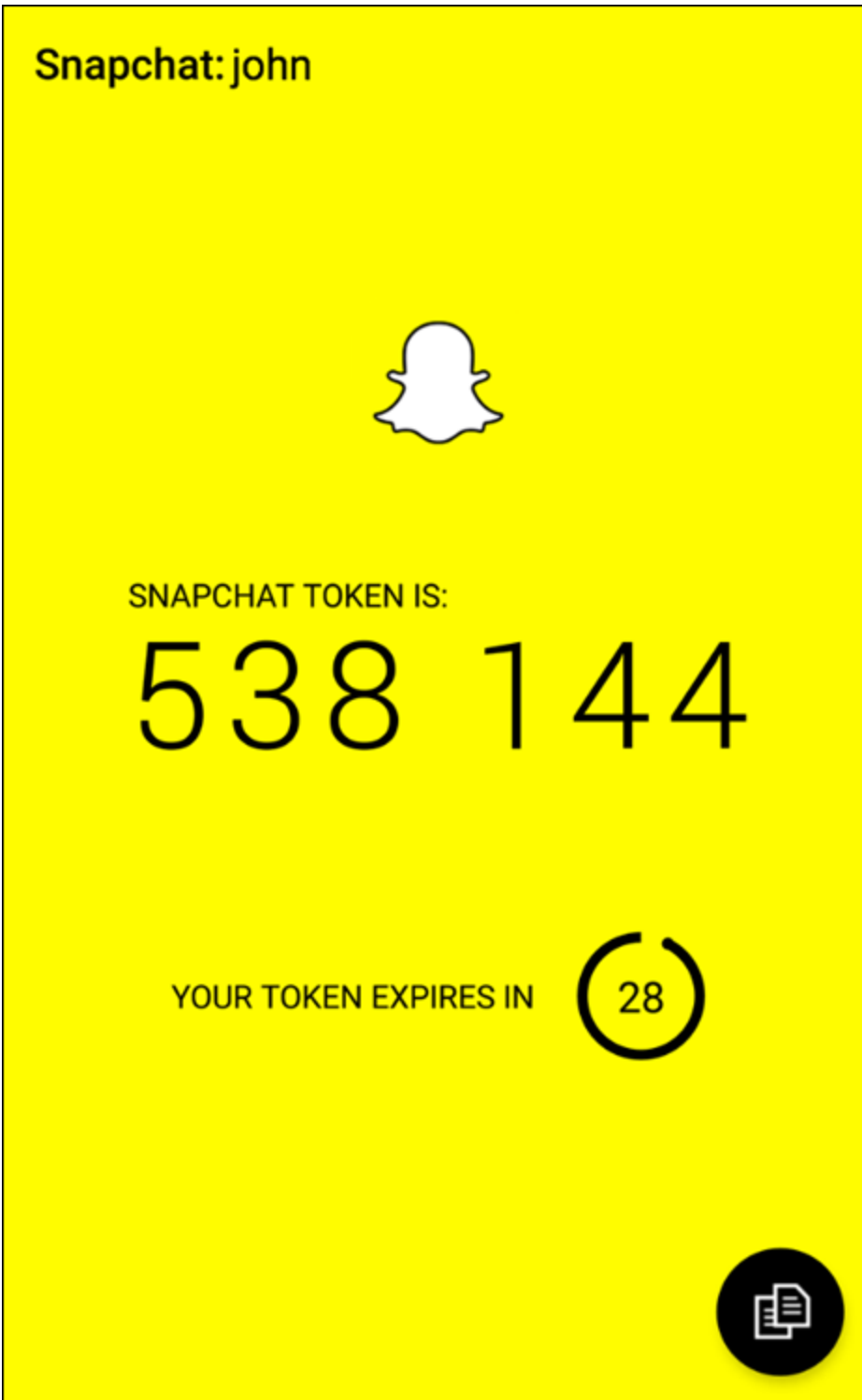


FIGURE 6-2: One-time password for Snapchat generated by the app Authy — an example of an app-generated multifactor authentication token.

Most financial institutions, social media companies, and major online retailers offer multifactor authentication — use it.

Also, note that while sending one-time passwords to users' smartphones via text messages theoretically verifies that a person logging in possesses the smartphone that the user is supposed to possess (something that the user has), various vulnerabilities undermine that supposition. It is possible, for example, for a criminal to intercept text messages even without possessing the phone.

Log out when you're finished

Don't rely on automatic timeouts, closing the browser, or shutting down a computer to log you out of accounts. Log out every time you're finished.

Don't leave yourself logged in between sessions unless you're on a device that you know with — as close as possible to — certainty will remain secure.

Use your own computer or phone

You don't know how well someone else has secured his or her device — it may have malware on it that can capture your passwords and other sensitive information or hijack sessions and perform all sorts of nefarious activities.

Furthermore, despite the fact that doing so is severely problematic, some applications and websites — to this day — cache data on endpoints that are used for accessing them. You don't want to leave other people souvenirs of your sensitive sessions.

Lock your computer

Lock any computer that you use for accessing sensitive accounts and keep it physically secure as well.

Use a separate, dedicated computer for sensitive tasks

Consider purchasing a special computer that you use for online banking and other sensitive tasks. For many people, a second computer isn't practical, but if it is, having such a machine — on which you never read

email, access social media, browse the web, and so on — offers security benefits.

Use a separate, dedicated browser for sensitive web-based tasks

If you can't obtain a separate computer, at least use a separate browser for sensitive tasks. Don't use the same browser that you use for reading the news, checking out blog posts, and most other activities.

Secure your access devices

Every phone, laptop, tablet, and desktop used for accessing secure systems should have security software on it, and that security software should be configured to regularly scan applications when they're added, as well as to run periodic general scans (see [Figure 6-3](#)). Also, make sure to keep that software up to date — most antivirus technology products perform far better against newer strains of malware when they're kept up to date than when they're not.

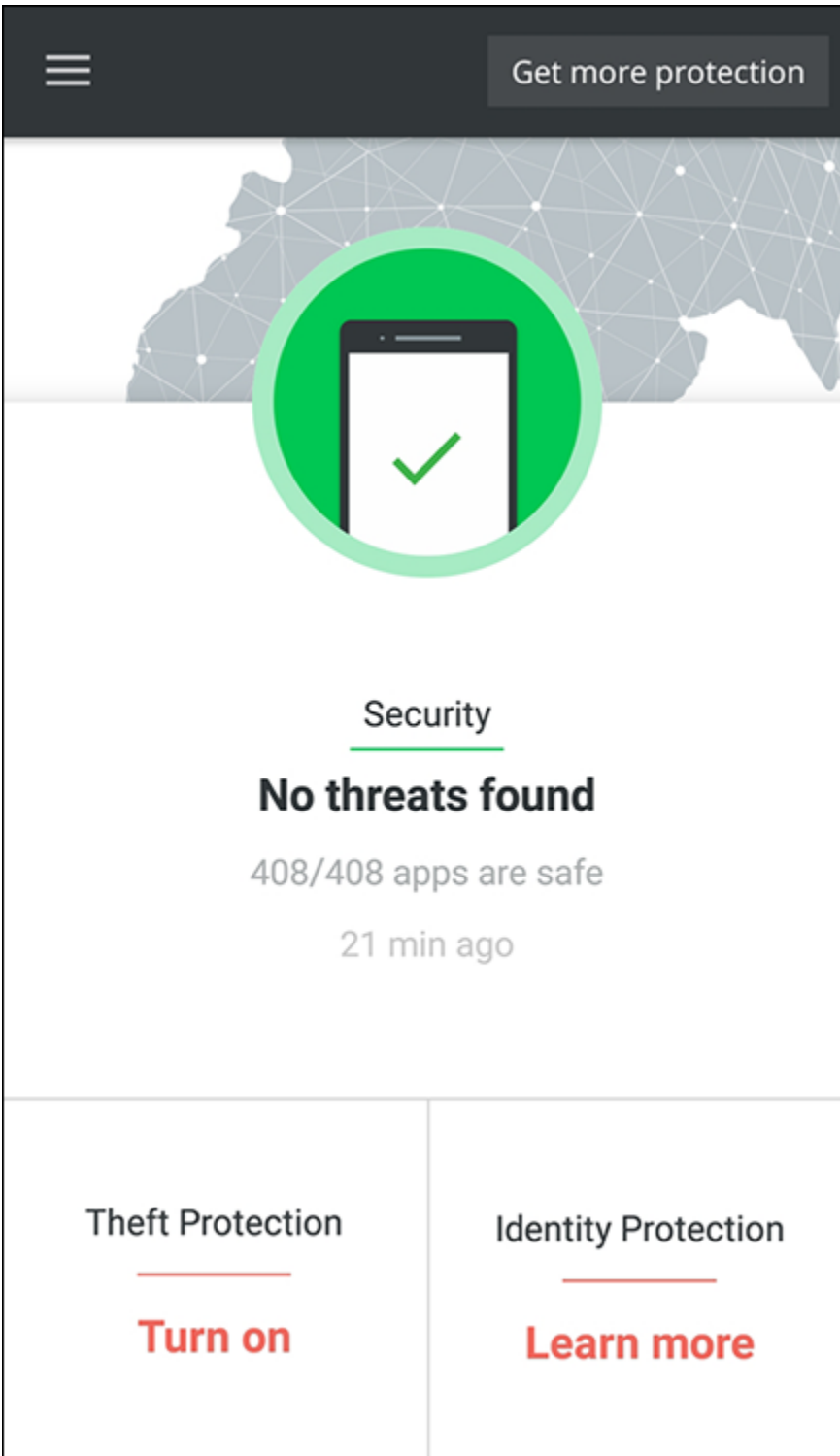


FIGURE 6-3: The results of a periodic scan of a phone's installed apps for malware.

Keep your devices up to date

Besides keeping your security software up to date, be sure to install operating system and program updates to reduce your exposure to vulnerabilities. Windows AutoUpdate and its equivalent on other platforms can simplify this task for you, as shown in [Figure 6-4](#).

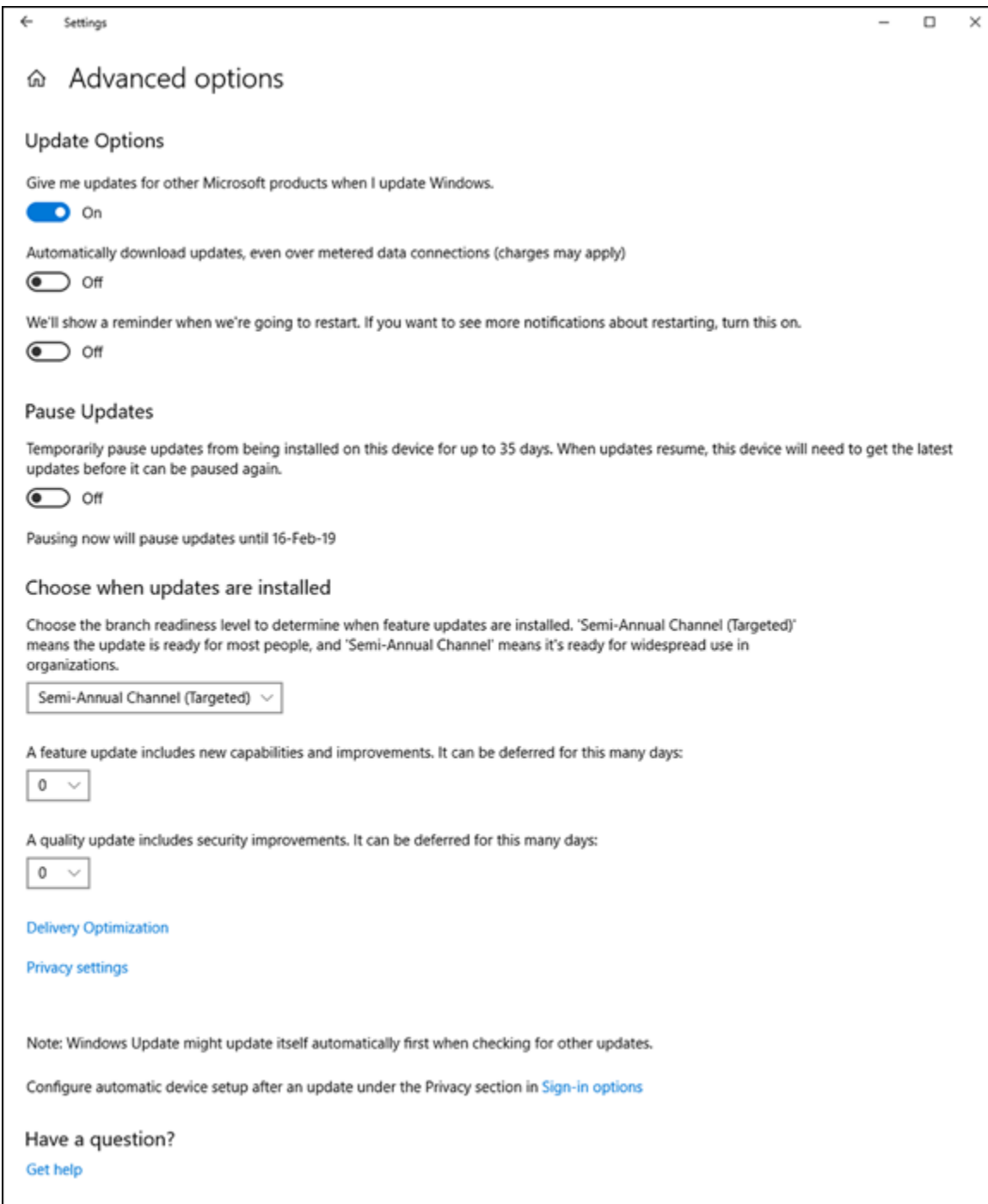


FIGURE 6-4: The AutoUpdate settings page in Windows 10.

Don't perform sensitive tasks over public Wi-Fi

If you must perform a sensitive task while you're in a location where you don't have access to a secure, private network, do what you need to do over the cellular system, not over public Wi-Fi. Public Wi-Fi simply poses too many risks. (To find out more about how to use public Wi-Fi safely, please see [Chapter 20](#).)

Never use public Wi-Fi for any purpose in high-risky places

Don't connect any device from which you plan to perform sensitive tasks to a Wi-Fi network in areas that are prone to *digital poisoning* — that is, to the hacking of, or distribution of malware, to devices that connect to a network.

Hacker conferences and certain countries, such as China, that are known for performing cyberespionage are examples of areas that are likely to experience digital poisoning. Many cybersecurity professionals recommend keeping your primary computer and phone off and using a separate computer and phone when working in such environments.

Access your accounts only when you're in a safe location

Even if you're using a private network, don't type passwords to sensitive systems or perform other sensitive tasks while in a location where people can easily watch what you type and see your screen.

Set appropriate limits

Various online venues let you set limits — for example, how much money can be transferred out of a bank account, the largest charge that can be made on a credit card with the card not physically present (as in the case of online purchases), or the maximum amount of goods that you can purchase in one day.



TIP

Set these limits. Not only will they limit the damage if a criminal does breach your account, but in some cases, they may trigger fraud alerts and prevent theft altogether.

Use alerts

If your bank, credit card provider, or a store that you frequent offers the ability to set up text or email alerts, you should seriously consider taking advantage of those services.

Theoretically, it is ideal to have the issuer send you an alert every time activity occurs on your account. From a practical standpoint, however, if doing so would overwhelm you and cause you to ignore all the messages (as is the case for most people), consider asking to be notified when transactions are made over a certain dollar amount (which may be able to be set to different thresholds for different stores or accounts) or otherwise appear to the issuer to be potentially fraudulent.

Periodically check access device lists

Some websites and apps — especially those of financial institutions — allow you to check the list of devices that have accessed your account. Checking this list each time that you log in can help you identify potential security problems quickly.

Check last login info

After you log in to some websites and via some apps — especially those of financial institutions — you may be shown information as to when and from where you last successfully logged in prior to the current session. Whenever any entity shows you such information, take a quick glance. If something is amiss and a criminal recently logged in while pretending to be you, it may stand out like a sore thumb.

Respond appropriately to any fraud alerts

If you receive a phone call from a bank, credit card company, or store about potential fraud on your account, respond quickly. But do not do so

by speaking with the party who called you. Instead, contact the outlet at a known valid number that is advertised on its website.

Never send any sensitive information over an unencrypted connection

When you access websites, look for the padlock icon (see [Figure 6-5](#)), indicating that encrypted HTTPS is being used. Today, HTTPS is ubiquitous; even many websites that do not ask users to submit sensitive data utilize it.

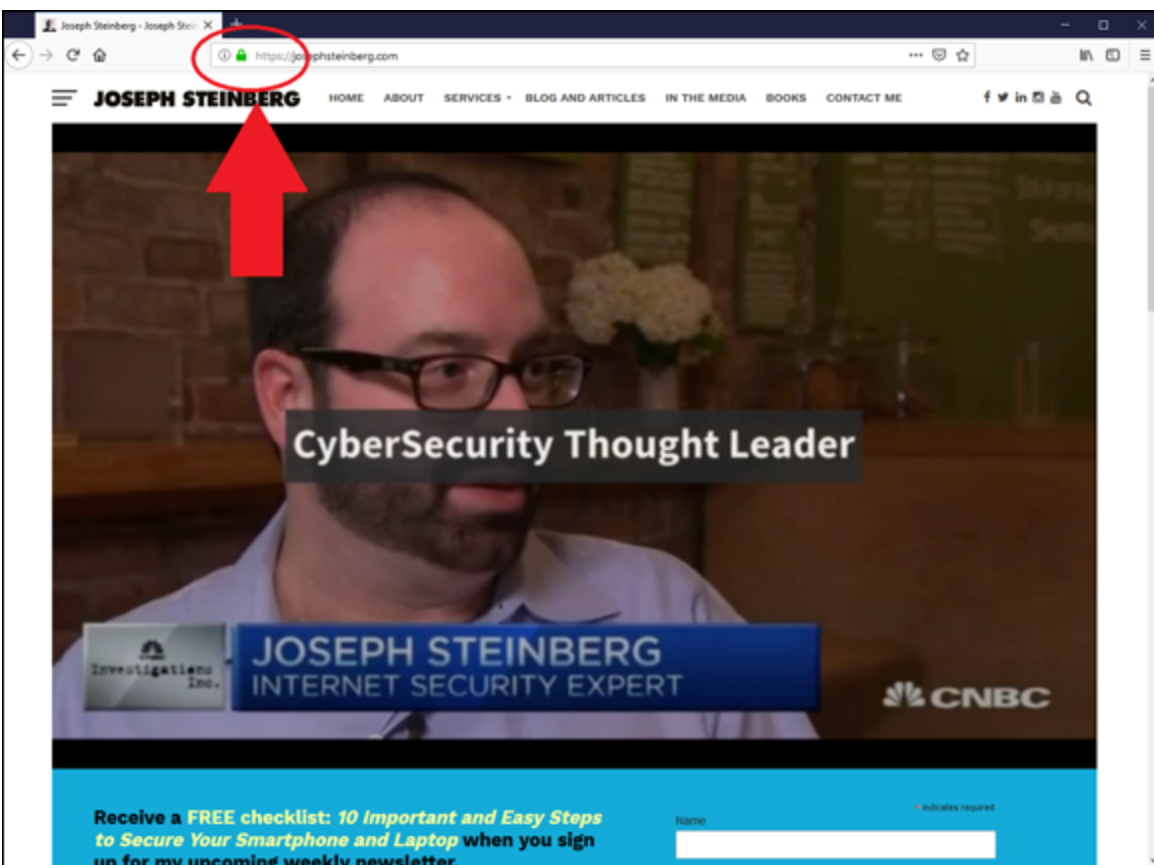


FIGURE 6-5: A secure website.

If you don't see the icon, unencrypted HTTP is being used. In such a case, don't provide sensitive information or log in.



TIP

The lack of a padlock on a site that is prompting for a login and password or handling financial transactions is a huge red flag that something is seriously amiss. However, contrary to what you've likely heard in the past, the presence of the lock doesn't necessarily mean that the site is safe.

Beware of social engineering attacks

In the context of cybersecurity, social engineering refers to the psychological manipulation by cyberattackers of their intended victims into performing actions that without such manipulation the targets would not perform or into divulging confidential information that they otherwise would not divulge.

To help prevent yourself from falling prey to social engineering attacks, consider any and all emails, text messages, phone calls, or social media communications from all banks, credit card companies, healthcare providers, stores, and so on to be potentially fraudulent.



WARNING

Never click on links in any such correspondence. Always connect with such parties by entering the URL in the URL bar of the web browser.

For more on social engineering attack prevention, see [Chapter 8](#).

Establish voice login passwords

Online access isn't the only path that a criminal can use to breach your accounts. Many crooks do reconnaissance online and subsequently social engineer their ways into people's accounts using old-fashioned phone calls to the relevant customer service departments at the target organizations.



TIP

To protect yourself and your accounts, establish voice login passwords for your accounts whenever possible — that is, set up passwords that must be given to customer service personnel in order for them to be able to provide any information from your accounts or to make changes to them. Many companies offer this capability, but relatively few people actually use it.

Protect your cellphone number

If you use strong authentication via text messages, ideally set up a forwarding phone number to your cellphone and use that number when giving out your cell number. Doing so reduces the chances that criminals will be able to intercept one-time passwords that are sent to your phone and also diminishes the chances of various other attacks succeeding.

For example, Google Voice, shown in [Figure 6-6](#), allows you to establish a new phone number that forwards to your cellphone so that you can give out a number other than your real cellphone number and reserve the real number for use within the authentication process.

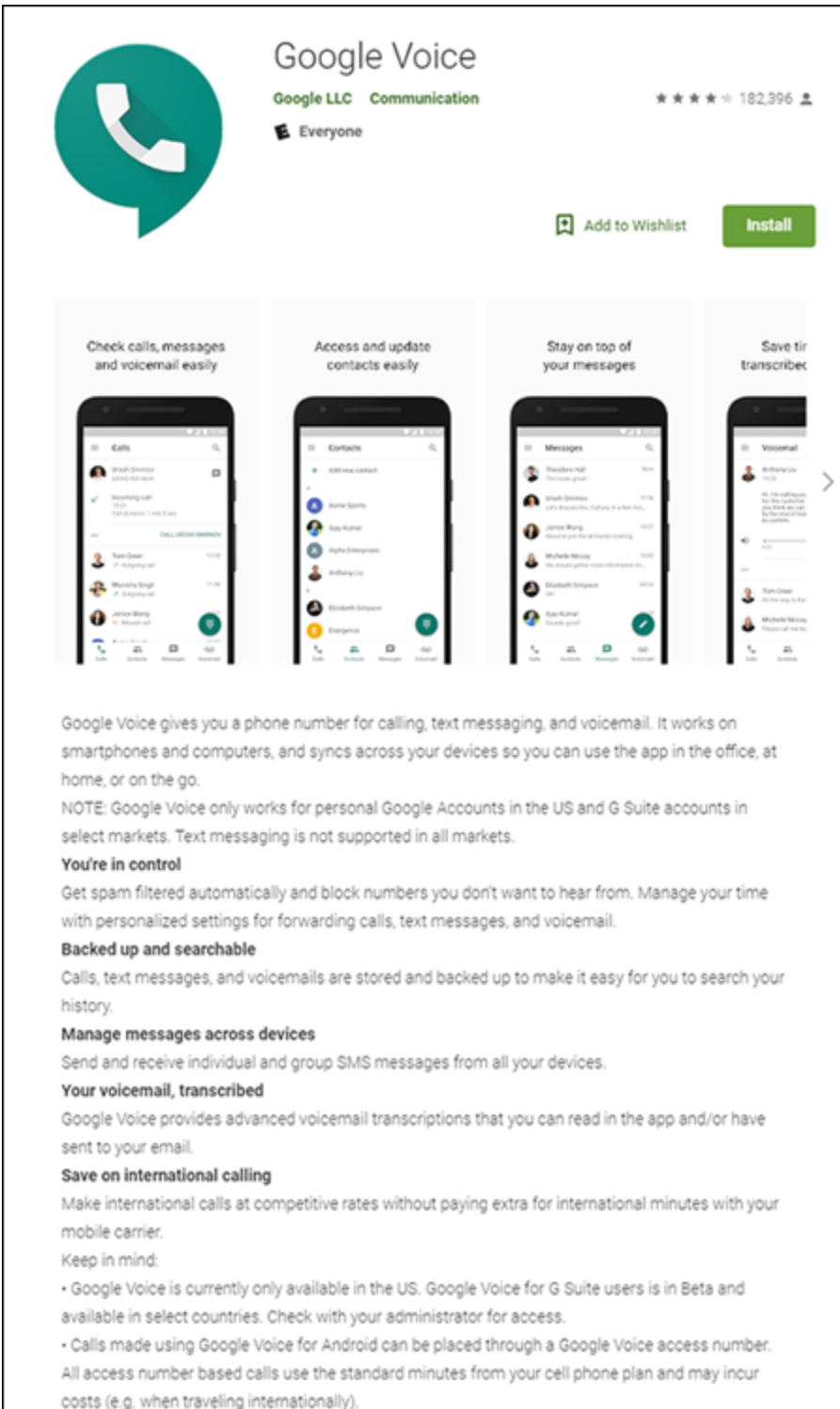


FIGURE 6-6: The Google Voice app as made available in the Google Play Store.

Don't click on links in emails or text messages

Clicking on links is one of the primary ways that people get diverted to fraudulent websites.

For example, I recently received an email message that contained a link. If I had clicked the link in the message shown in [Figure 6-7](#), I would have been brought to a phony LinkedIn login page that collects LinkedIn username and password combinations and provides them to criminals.

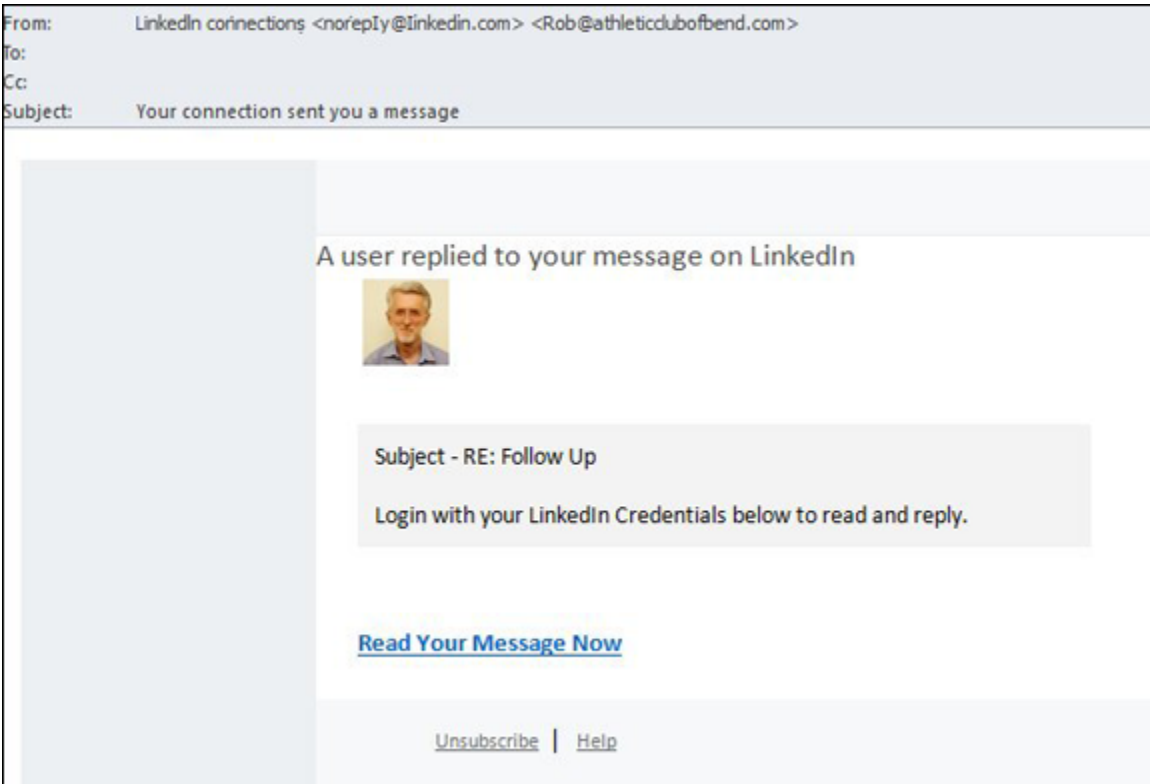


FIGURE 6-7: Email with a link to a phony page.

Don't overshare on social media

You don't want to provide criminals with the answers to challenge questions that are being used to protect your account or offer them information that they can use to social engineer their way into your accounts. See [Chapter 8](#) for more on preventing social engineering.

Pay attention to privacy policies

Understand what a site means if it says that it is going to share your data with third parties or sell your data to others.

Securing Data with Parties That You've Interacted With

When you interact online with a party, not all the data is under your control. If you browse a website with typical web browser settings, that site may track your activity. Because many sites syndicate content from third parties — for example from advertising networks — sites may even be able to track your behavior on other sites.

If you have an account on any sites that do such tracking and log in, all the sites utilizing the syndicated content may know your true identity and plenty of information about you — even though you never told them anything about yourself. Even if you don't have such an account or don't log in, profiles of your behavior may be established and used for marketing purposes, even without knowing who you are. (Of course, if you ever log in in the future to any site using the network, all the sites with the profiles may correlate them to your true identity.)

It is far more difficult to protect data about you that is in the possession of third parties but that is not under your control than it is to protect data in your accounts. That does not mean, however, that you're powerless. (Ironically, and sadly, most owners of such data likely do a better job protecting data about people than do the people themselves.)



TIP

Besides employing the strategies in the previous section, you may want to browse in private sessions. For example, by using a Tor browser — which, as shown in [Figure 6-8](#), automatically routes all your Internet traffic through computers around the world before sending it to its destination — you make it difficult for third parties to track you. As discussed in [Chapter 4](#), the Tor browser bundle is free and comes with all sorts of privacy-related features enabled, including blocking cookies and canvas fingerprinting, an advanced form of tracking devices.

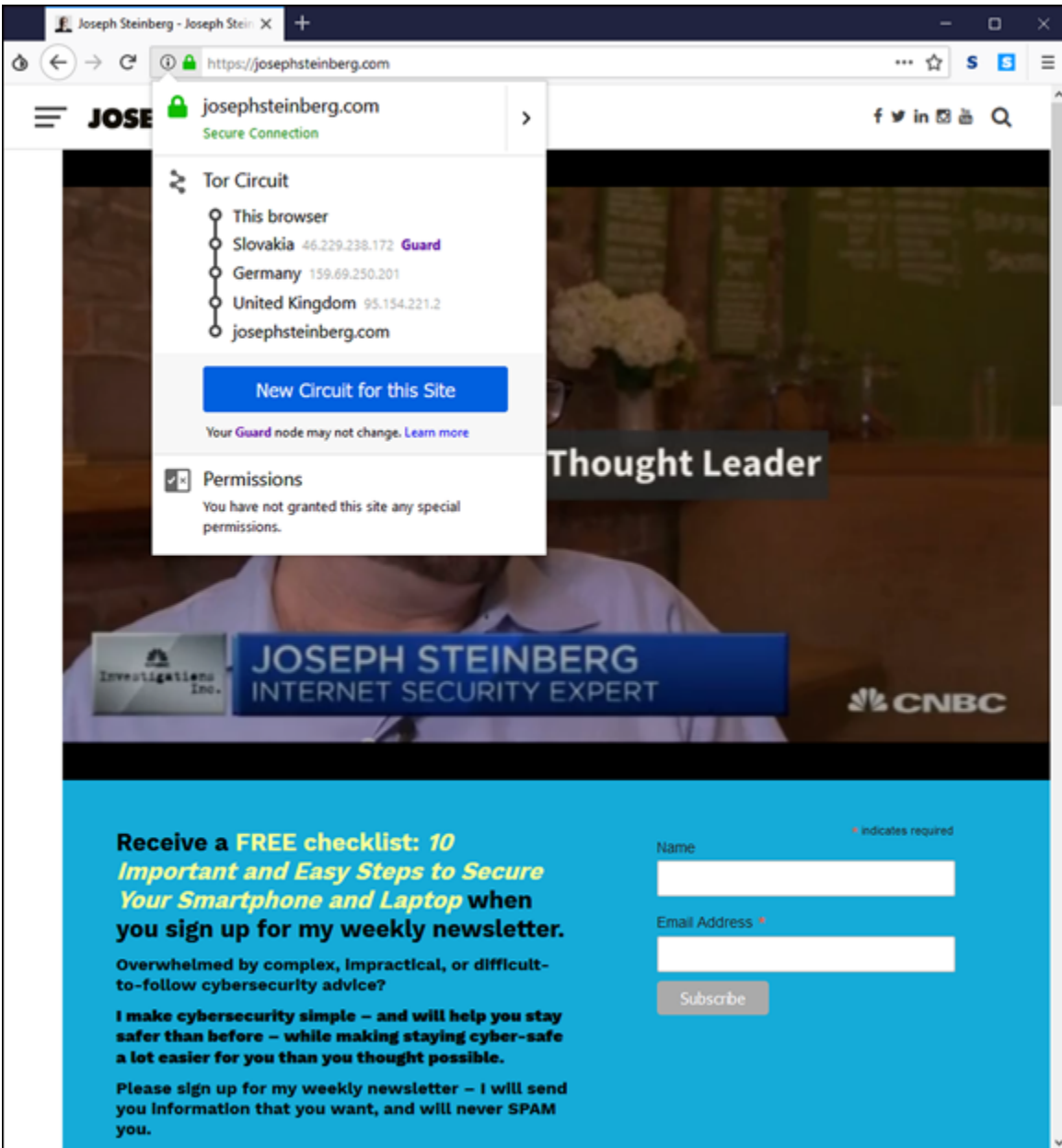


FIGURE 6-8: The author's website as seen in a Tor browser, with the Tor circuit information button clicked so as to show how Tor is hiding the user's point of origin. The image was generated with the Tor browser running on a computer in New Jersey, but, because of Tor's security features, appears to the web server as if it is in the United Kingdom.

If Tor seems complicated, you can also utilize a reputable VPN service for similar purposes.

By using browsing technology that makes it harder for sites to track you, they are less likely to establish as detailed profiles about you — and the less data about you that they have, the less data about you that can be

stolen. Besides, you may not want those parties to build profiles about you in the first place.



WARNING One technology that, despite its name, does not prevent tracking at anywhere near the level that do Tor or VPNs is the private mode offered by most web browsers. Unfortunately, despite its name, the private mode suffers from multiple serious weaknesses in this regard and does not come close to ensuring privacy.

Securing Data at Parties That You Haven't Interacted With

Numerous entities likely maintain significant amounts of data about you, despite the fact that you've never knowingly interacted with them or otherwise authorized them to maintain such information.

For example, at least one major social media service builds de facto profiles for people who don't have accounts with the service, but who have been mentioned by others or who have interacted with sites that utilize various social widgets or other related technologies. The service can then use these profiles for marketing purposes — even, in some cases, without knowing the person's true identity.

Furthermore, various information services that collect information from numerous public databases establish profiles based on such data — containing details that you may not even realize was available to the public.

Some genealogy sites utilize all sorts of public records and also allow people to update the information about other people. This ability can lead to situations in which all sorts of nonpublic information about you may be available to subscribers to the site (or people with free trial subscriptions) without your knowledge or consent. Such sites make

finding people's mothers' maiden names easy, which undermines the authentication scheme used by many organizations.

Besides family tree sites, various professional sites maintain information about folks' professional histories, publications, and so on. And, of course, credit bureaus maintain all sorts of information about your behavior with credit — such information is submitted to them by financial institutions, collection agencies, and so on.

While the Fair Credit Reporting Act may help you manage the information that the bureaus have about you, it can't help you remove negative information that appears in other venues, such as in old newspaper articles that are online. Besides the privacy implications of such, if any information in those articles provides the answer to challenge questions used for authentication, it can create security risks. In such cases, you may want to reach out to the provider of the data, explain the situation, and ask it to remove the data. In some cases, they will cooperate.

In addition, some businesses, such as insurance companies and pharmacies, maintain medical information about people. Typically, individuals have little control over such data.

Of course, this type of data, which isn't under your complete control, can impact you. The bottom line is that many entities likely maintain significant amounts of data about you, even though you have never directly interacted with them.

It is the duty of such organizations to protect their data stores, but, they do not always properly do so. As the Federal Trade Commission notes on its website, a data breach at the credit bureau Equifax, discovered in 2017, exposed the sensitive personal information of 143 million Americans.

And, the reality is, that other than in the cases in which you can manually update records or request that they be updated, you can do little to protect the data in such scenarios.

Chapter 7

Passwords

IN THIS CHAPTER

- » Selecting passwords
 - » Discovering how often you need to change passwords — or not
 - » Storing passwords
 - » Finding alternatives to passwords
-

Most people alive today are familiar with the concept of passwords and with their use in the realm of cybersecurity. Yet, there are so many misconceptions about passwords, and misinformation about them has spread like wildfire, often leading to people undermining their own security with poor password practices.

In this chapter, you discover some best practices vis-à-vis passwords. These practices should help you both maximize your own security and maintain reasonable ease of use.

Passwords: The Primary Form of Authentication

Password authentication refers to the process of verifying the identity of a user (whether human or computer process) by asking that user to supply a password — that is, a previously-agreed-upon secret piece of information — that ostensibly the party authenticating would only know if he or she were truly the party who it claimed to be. While the term password implies that the information consists of a single word, today's passwords can include combinations of characters that don't form words in any spoken or written language.

Despite the availability for decades of many other authentication approaches and technologies — many of which offer significant advantages over passwords — passwords remain de facto worldwide standard for authenticating people online. Repeated predictions of the demise of passwords have been proven untrue, and the number of passwords in use grows every day.

Because password authentication is so common and because so many data breaches have resulted in the compromise of password databases, the topic has received significant media attention, with reports often spreading various misleading information. Gaining a proper understanding of the realm of passwords is important if you want to be cybersecure.

Avoiding Simplistic Passwords

Passwords only secure systems if unauthorized parties can't easily guess them.

Criminals often guess passwords by

- » **Guessing common passwords:** It's not a secret that 123456 and password are common passwords — data from recent breaches reveals that they are, in fact, among the most common passwords used on many systems (see the nearby sidebar)! Criminals exploit such sad reality and often attempt to breach accounts by using automated tools that feed systems passwords one at a time from lists of common passwords — and record when they have a hit. Sadly, those hits are often quite numerous.
- » **Launching dictionary attacks:** Because many people choose to use actual English words as passwords, some automated hacker tools simply feed all the words in the dictionary to a system one at a time. As with lists of common passwords, such attacks often achieve numerous hits.
- » **Credential stuffing:** *Credential stuffing* refers to when attackers take lists of usernames and passwords from one site — for example,

from a site that was breached and whose username password database was subsequently posted online — and feed its entries to another system one at a time in order to see whether any of the login credentials from the first system work on the second.

Because many people reuse username and password combinations between systems, credential stuffing is, generally speaking, quite effective.

THE MOST COMMON PASSWORDS OF 2018

Since 2011, password manager app vendor SplashData has released a list of the 25 most common passwords that it assembles from various sources. Here is the list from 2018:

123456	password	123456789	12345678	12345
111111	1234567	sunshine	qwerty	iloveyou
princess	admin	welcome	666666	abc123
football	123123	monkey	654321	!@#\$%^&*
Charlie	aa123456	donald	password1	qwerty123

As you can see, criminals benefit from the fact that many people use weak, easily guessable passwords.

Password Considerations

When you create passwords, keep in mind that more complex isn't always better, and that the password strength that you choose should depend on how sensitive the data and system are that the password protects. The following sections discuss easily guessable passwords, complicated passwords, sensitive passwords, and password managers.

Easily guessable personal passwords

Criminals know that many people use the name or birth date of their significant other or pet as a password, so crooks often look at social media profiles and do Google searches in order to find likely passwords. They also use automated tools to feed lists of common names to targeted systems one by one, while watching to see whether the system being attacked accepts any of the names as a correct password.

Criminals who launch targeted attacks can exploit the vulnerability created by such personalized, yet easily guessable, passwords. However, the problem is much larger: Sometimes, reconnaissance is done through automated means — so, even opportunistic attackers can leverage such an approach.

Furthermore, because, by definition, a significant percentage of people have common names, the automated feeders of common names often achieve a significant number of hits.

Complicated passwords aren't always better

To address the problems inherent in weak passwords, many experts recommend using long, complex passwords — for example, containing both uppercase and lowercase letters, as well as numbers and special characters.

Using such passwords makes sense in theory, and if such a scheme is utilized to secure access to a small number of sensitive systems, it can work quite well. However, employing such a model for a larger number of passwords is likely to lead to problems that can undermine security:

- » Inappropriately reusing passwords
- » Writing down passwords in insecure locations
- » Selecting passwords with poor randomization and formatted using predictable patterns, such as using a capital for the first letter of a complicated password, followed by all lowercase characters, and then a number

Hence, in the real world, from a practical perspective, because the human mind can't remember many complex passwords, using significant

numbers of complex passwords can create serious security risks.

According to *The Wall Street Journal*, Bill Burr, the author of NIST Special Publication 800-63 Appendix A (which discusses password complexity requirements), recently admitted that password complexity has failed in practice. He now recommends using passphrases, and not complex passwords, for authentication.

Passphrases are passwords consisting of entire phrases or phrase-length strings of characters, rather than of simply a word or a word-length group of characters. Sometimes passphrases even consist of complete sentences. Think of passphrases as long (usually at least 25 characters) but relatively easy to remember passwords.

Different levels of sensitivity

Not all types of data require the same level of password protection. For example, the government doesn't protect its unclassified systems the same way that it secures its top-secret information and infrastructure.

In your mind or on paper, classify the systems for which you need secure access.

Then informally classify the systems that you access and establish your own informal password policies accordingly.

On the basis of risk levels, feel free to employ different password strategies. Random passwords, passwords composed of multiple words possibly separated with numbers, passphrases, and even simple passwords each have their appropriate uses. Of course, multifactor authentication can, and should, help augment security when it's both appropriate and available.



TIP

Establishing a stronger password for online banking than for commenting on a blog on which you plan to comment only once in a blue moon makes sense. Likewise, your password to the blog should probably be stronger than the one used to access a free news site that requires you to log in but on which you never post anything and at which, if your account were compromised, the breach would have zero impact upon you.

Your most sensitive passwords may not be the ones that you think

When classifying your passwords, keep in mind that while people often believe that their online banking and other financial system passwords are their most sensitive passwords, that is not always the case. Because many modern online systems allow people to reset their passwords after validating their identities through email messages sent to their previously known email addresses, a criminal who gains access to someone's email account may be able to do a lot more than just read email without authorization: He or she may be able to reset that user's passwords to many systems, including to some financial institutions.

Likewise, many sites leverage social-media-based authentication capabilities — especially those provided by Facebook and Twitter — so a compromised password on a social media platform can lead to unauthorized parties gaining access to other systems as well, some of which may be quite a bit more sensitive in nature than a site on which you just share pictures.

You can reuse passwords — sometimes

You may be surprised to read this statement in an information security book: You don't need to use strong passwords for accounts that you create solely because a website requires a login, but that does not, from your perspective, protect anything of value. If you create an account in order to access free resources, for example, and you have nothing whatsoever of value stored within the account, and you don't mind

getting a new account the next time you log in, you can even use a weak password — and use it again for other similar sites.



TIP Essentially, think about it like this: If the requirement to register and log in is solely for the benefit of the site owner — to track users, market to them, and so on — and it doesn't matter one iota to you whether a criminal obtained the access credentials to your account and changed them, use a simple password. Doing so will preserve your memory for sites where password strength matters. Of course, if you use a password manager, you can use a stronger password for such sites.

Consider using a password manager

Alternatively, you can use a password manager tool, shown in [Figure 7-1](#), to securely store your passwords. Password managers are software that help people manage passwords by generating, storing, and retrieving complex passwords. Password managers typically store all their data in encrypted formats and provide access to users only after authenticating them with either a strong password or multifactor authentication.

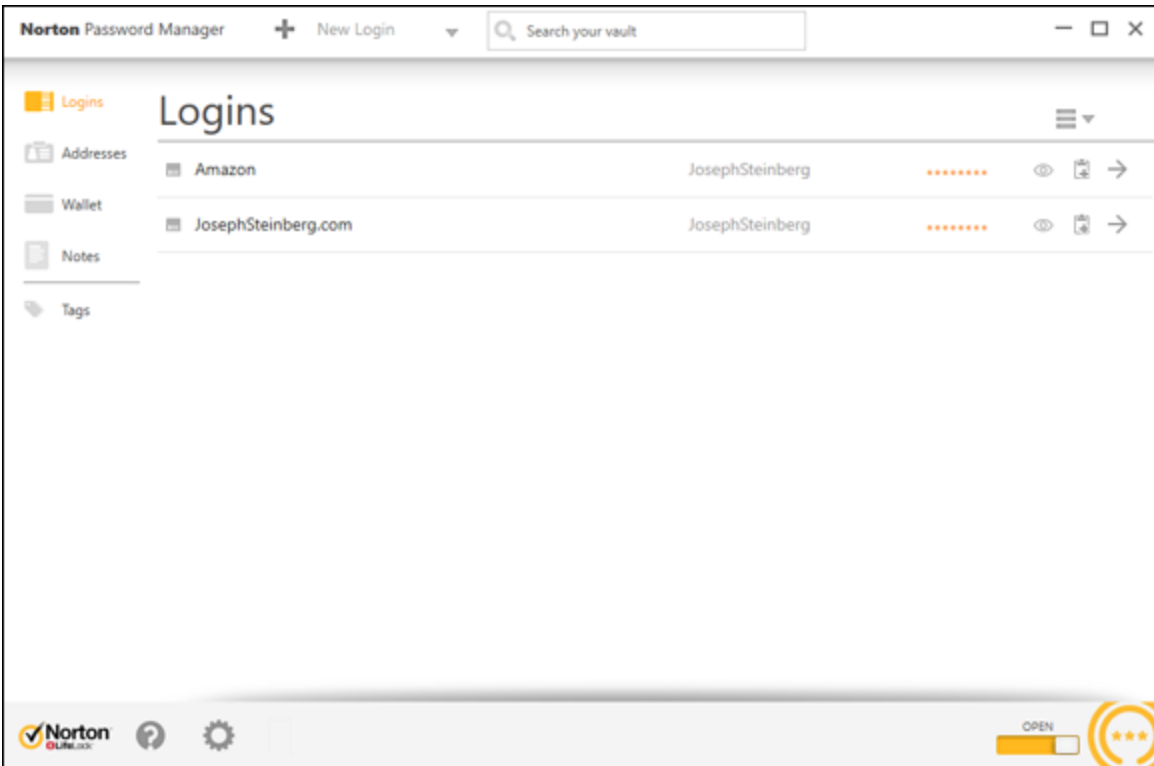


FIGURE 7-1: A password manager.



WARNING Such technology is appropriate for general passwords, but not for the most sensitive ones. Various password managers have been hacked, and if something does go wrong when all your eggs are in one basket, you may have a nightmare on your hands.

Of course, be sure to properly secure any device that you use to access your password manager.

Many password managers are on the market. While all utilize encryption to protect the sensitive data that they store, some store passwords locally (for example, in a database on your phone), while others store them in the cloud.

Many modern smartphones come equipped with a so-called *secure area* — a private, encrypted space that is *sandboxed*, or separated, into its own running environment. Ideally, any password information stored on a mobile device is stored protected in the secure area (see [Figure 7-2](#)).

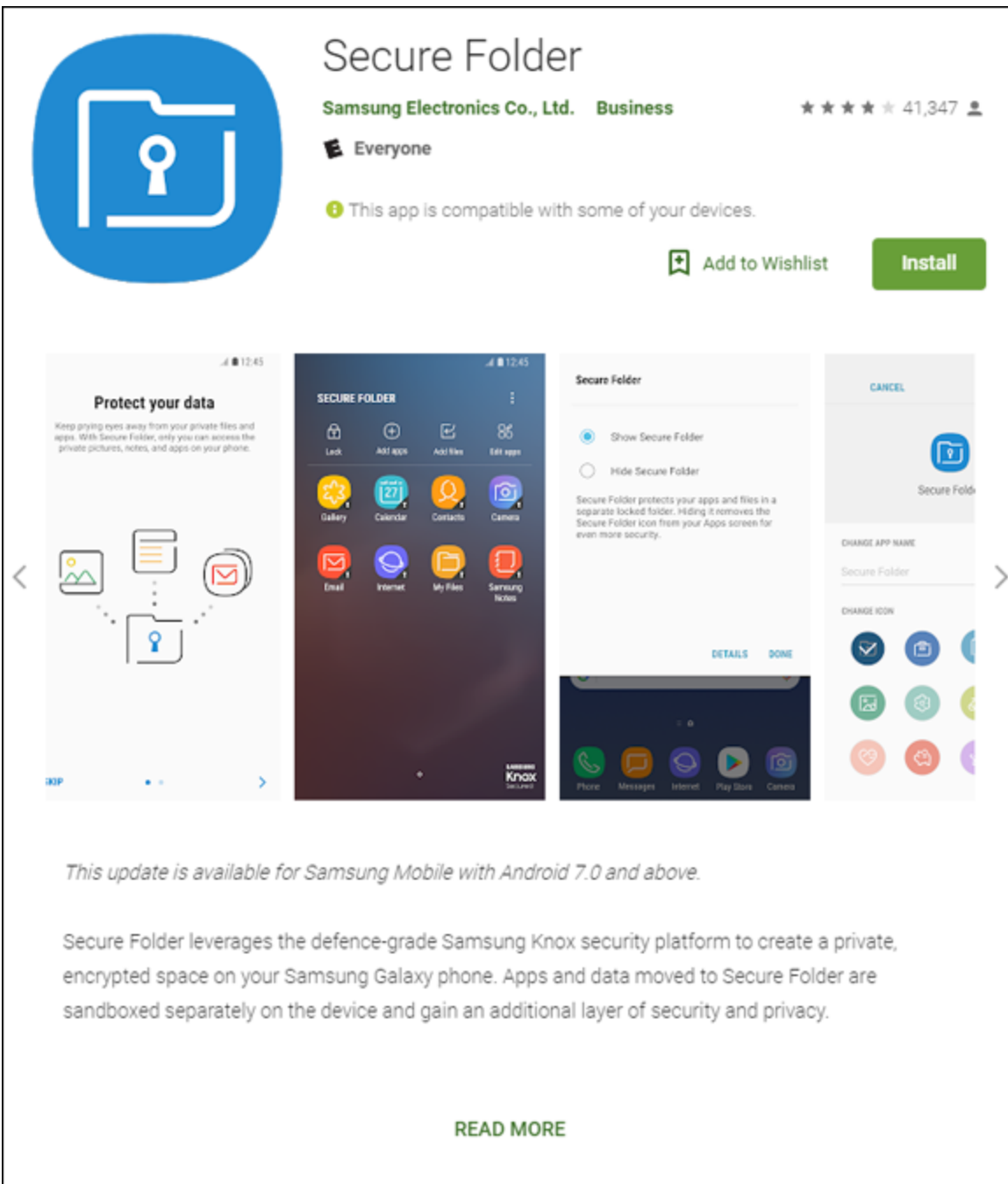


FIGURE 7-2: Secure Folder, the secure area app provided by Samsung for its Android series of phones, as seen in the Google Play Store.

Data that is stored in the secure area can't be accessed unless a user enters the secure area, usually by running a secure area app and entering a special password. Devices also typically display some special symbol somewhere on the screen when a user is working with data or an app located in the secure area.

Creating Memorable, Strong Passwords

The following list offers suggestions that may help you create strong passwords that are, for most people, far easier to remember than a seemingly random, unintelligible mix of letters, numbers, and symbols:

- » **Combine three or more unrelated words and proper nouns, with numbers separating them.** For example, laptop2william7cows is far easier to remember than 6ytBgv%j8P. In general, the longer the words you use within the password, the stronger the resulting password will be.
- » **If you must use a special character, add a special character before each number; you can even use the same character for all your passwords.** (If you use the same passwords as in the previous example and follow this advice, the password is laptop%2william%7cows.) In theory, reusing the same character may not be the best way to do things from a security standpoint, but, doing so makes memorization much easier, and the security should still be good enough for purposes for which a password is suitable on its own anyway.
- » **Ideally, use at least one non-English word or proper name.** Choose a word or name that is familiar to you but that others are unlikely to guess. Don't use the name of your significant other, best friend, or pet.
- » **If you must use both capital and lowercase letters (or want to make your password even stronger), use capitals that always appear in a particular location throughout all your strong passwords.** Make sure, though, that you don't put them at the start of words because that location is where most people put them. For example, if you know that you always capitalize the second and third letter of the last word, then laptop2william7kALb isn't harder to remember than laptop2william7kalb.

Knowing When to Change Your Password

Conventional wisdom — as you have likely heard many times — is that it is ideal to change your password quite frequently. The American Association of Retired Persons (AARP), for example, recommends on its website that people (including the disproportionately older folks who comprise its membership) “change critical passwords frequently, possibly every other week.”

Theoretically, such an approach is correct — frequent changes reduce risks in several ways — but, in reality, it’s bad advice that you shouldn’t follow.

If you have a bank account, mortgage, a couple credit cards, a phone bill, high speed Internet bill, utility bills, social media accounts, email accounts, and so on, you may easily be talking about a dozen or so critical passwords. Changing them every two weeks would mean 312 new critical passwords to remember within the span of every year — and you likely have many more passwords on top of that figure. For many people, changing important passwords every two weeks may mean learning a hundred new passwords every month.

Unless you have a phenomenal, photographic memory, how likely is it that you’ll remember all such passwords? Or will you simply make your passwords weaker in order to facilitate remembering them after frequent changes?

The bottom line is that changing passwords often makes remembering them far more difficult, increasing the odds that you’ll write them down and store them insecurely, select weaker passwords, and/or set your new passwords to be the same as old passwords with minute changes (for example, password2 to replace password1).



REMEMBER

So, here is the reality: If you select strong, unique passwords to begin with and the sites where you've used them aren't believed to have been compromised, the cons of frequently changing the passwords outweigh the pros. Changing such passwords every few years may be a good idea. In reality, if a system alerts you of multiple failed attempts to log in to your account and you're not alerted of such activity, you can likely go for many years with no changes without exposing yourself to significant risk.

Of course, if you use a password manager that can reset passwords, you can configure it to reset them often. In fact, I've worked with a commercial password-management system used for protecting system administration access to sensitive financial systems that automatically reset administrators' passwords every time they logged on.

Changing Passwords after a Breach

If you receive notification from a business, organization, or government entity that it has suffered a security breach and that you should change your password, follow these tips:

- » Don't click any links in the message because most such messages are scams.
- » Visit the organization's website and official social media accounts to verify that such an announcement was actually made.
- » Pay attention to news stories to see whether reliable, mainstream media is reporting such a breach.
- » If the story checks out, go to the organization's website and make the change.



TIP

Do not change all your passwords after every breach. Ignore experts who cry wolf and tell you to do so after every single breach as a matter of extra caution. Doing so isn't necessary, uses up your brainpower, time, and energy, and dissuades you from changing passwords when you actually need to do so. After all, if you do make such password changes and then find out that your friends who fared no worse than you after a breach, you may grow weary and ignore future warnings to change your password when doing so is actually necessary.

If you reuse passwords on sites where the passwords matter — which you should not be doing — and a password that is compromised somewhere is also used on other sites, be sure to change it at the other sites as well. In such a case, also take the opportunity when resetting passwords to switch to unique passwords for each of the sites.

Providing Passwords to Humans

On its website, the United States Federal Trade Commission (FTC) recommends the following:

*Don't share passwords on the phone, in texts, or by email.
Legitimate companies will not send you messages asking for your password.*

That sounds like good advice, and it would be, if it were not for one important fact: Legitimate businesses do ask you for passwords over the phone!

So, how do you know when it is safe to provide your password and when it is not?

Should you just check your caller ID?

No. The sad reality is that crooks spoof caller IDs on a regular basis.

What you should do is never provide any sensitive information — including passwords, of course — over the phone unless you initiated the call with the party requesting the password and are sure that you called the legitimate party. It is far less risky, for example, to provide an account’s phone-access password to a customer service representative who asks for it during a conversation initiated by you calling to the bank using the number printed on your ATM card than if someone calls you claiming to be from your bank and requests the same private information in order to “verify your identity.”

Storing Passwords

Ideally, don’t write down your passwords to sensitive systems or store them anywhere other than in your brain.

For less sensitive passwords, use a password manager or store them in an encrypted form on a strongly-secured computer or device. If you store your passwords on a phone, use the secure area. (For more on password managers and your phone’s secure area, see the section “[Consider using a password manager](#),” earlier in this chapter.)

Transmitting Passwords

Theoretically, you should never email or text someone a password. So, what should you do if your child texts you from school saying that he or she forgot the password to his or her email, or the like?



TIP

Ideally, if you need to give someone a password, call him or her and don’t provide the password until you identify the other party by voice. If, for some reason, you must send a password in writing, choose to use an encrypted connection, which is offered by various chat tools. If no such tool is available, consider splitting the password and sending some via email and some via text.

Obviously, none of these methods are ideal ways to transmit passwords, but they certainly are better options than what so many people do, which is to simply text or email people passwords in clear text.

Discovering Alternatives to Passwords

On some occasions, you should take advantage of alternatives to password authentication. While there are many ways to authenticate people, a modern user is likely to encounter certain types:

- » Biometric authentication
- » SMS-based authentication
- » App-based one-time passwords
- » Hardware token authentication
- » USB-based authentication

Biometric authentication

Biometric authentication refers to authenticating using some unique identifier of your physical person — for example, your fingerprint.

Using biometrics — especially in combination with a password — can be a strong method of authentication, and it certainly has its place. Two popular forms used in the consumer market are fingerprints and iris-based authentication.

In many cases, though, you may be better off using a strong password. Before using biometric authentication, consider the following points:

- » **Your fingerprints are likely all over your phone.** You hold your phone with your fingers. How hard would it be for criminals who steal the phone to lift your prints and unlock the phone if you enable fingerprint based authentication using a phone's built-in fingerprint reader (see [Figure 7-3](#))? If anything sensitive is on the device, it may

be at risk. No, the average crook looking to make a quick buck selling your phone is unlikely to spend the time to unlock it — he or she will more than likely just wipe it — but if someone wants the data on your phone for whatever reason, and you used fingerprints to secure your device, you may have a serious problem on your hands (pun intended).

- » **If your biometric information is captured, you can't reset it as you can a password.** Do you fully trust the parties to whom you're giving this information to properly protect it?
- » **If your biometric information is on your phone or computer, what happens if malware somehow infects your device?** What happens if a server where you stored the same information is breached? Are you positive that all the data is properly encrypted and that the software on your device fully defended your biometric data from capture?
- » **Cold weather creates problems.** Fingerprints can't be read even through smartphone-compatible gloves.
- » **Glasses, as worn by millions of people, pose challenges to iris scanners.** Some iris readers require a user to take off his or her glasses in order to authenticate. If you use such authentication to secure a phone, you may have difficulty unlocking your phone when you're outdoors on a sunny day.
- » **Biometrics can undermine your rights.** If, for some reason, law enforcement wants to access the data on your biometric-protected phone or other computer system, it may be able to force you to provide your biometric authentication, even in countries like the United States where you have the right to remain silent and not provide a password. Likewise, the government may be able to obtain a warrant to collect your biometric data, which, unlike a password, you can't reset. Even if the data proves you innocent of whatever the government suspects you have done wrong, do you trust the government to properly secure the data over the long term?
- » **Impersonation is possible.** Some quasi-biometric authentication, such as the face recognition on some devices, can be tricked into

believing that a person is present by playing to them a high-definition video of that person.

- » **Voice-based authentication is useful for voice phone calls.** This type of authentication is especially useful when used in combination with other forms of authentication, such as a password. Many organizations use it to authenticate customers who call in — sometimes without even telling customers. That said, voice authentication can't be used for online sessions without inconveniencing users.

As such, biometrics have their place. Using a fingerprint to unlock features on your phone is certainly convenient but think before you proceed. Be certain that in your case the benefits outweigh the drawbacks.



FIGURE 7-3: A phone fingerprint sensor on a Samsung Galaxy S9 in an Otterbox case. Some phones have the reader on the front, while others, like the S9, have it on the back.

HACKERS VERSUS SENSOR

How long did it take hackers to defeat a new fingerprint sensor? Less than 24 hours.

Within 24 hours of the release of the first iPhone with a fingerprint reader, hackers claimed to have defeated it. Furthermore, several years ago, the Discovery Channel television show *Myth Busters* demonstrated how simple it can be for someone to defeat a fingerprint authentication system. Technology has improved since then — but so have criminals' capabilities.

SMS-based authentication

In *SMS (text message)-based authentication*, a code is sent to your cellphone. You then enter that code into a web or app to prove your identity. This type of authentication is, in itself, not considered secure enough for authentication when true multifactor authentication is required. Sophisticated criminals have ways of intercepting such passwords, and social engineering of phone companies in order to take over people's phone numbers remains a problem.

That said, SMS one-time passwords used in combination with a strong password are a step above just using the password.



WARNING Keep in mind, however, that, in most cases, one-time passwords are worthless as a security measure if you send them to a criminal's phishing website instead of a legitimate site. The criminal can replay them to the real site in real time.

App-based one-time passwords

One-time passwords generated with an app running on a phone or computer are a good addition to strong passwords, but they should not be used on their own. App-based one-time passwords are likely a more secure way to authenticate than SMS-based one-time passwords (see preceding section), but they can be inconvenient; if you get a new phone, for example, you may need to reconfigure information at every one of the sites where you're using one-time passwords created by the generator app running on your smartphone.

As with SMS-based one-time passwords, if you send an app-generated one-time password to a criminal's phishing website instead of a legitimate site, the criminal can replay it to the corresponding real site in real time, undermining the security benefits of the one-time password in their entirety.

Hardware token authentication

Hardware tokens (see [Figure 7-4](#)) that generate new one-time passwords every x seconds are similar to the apps described in the preceding section with the major difference being that you need to carry a specialized device that generates the one-time codes. Some tokens can also function in other modes — for example, allowing for challenge-response types of authentication in which the site being logged into displays a challenge number that the user enters into the token in order to retrieve a corresponding response number that the user enters into the site in order to authenticate.



FIGURE 7-4: An RSA SecureID brand one-time password generator hardware token.

Although hardware token devices normally are more secure than one-time generator apps in that the former don't run on devices that can be infected by malware or taken over by criminals remotely, they can be inconvenient. They are also prone to getting lost and are not always waterproof — and sometimes get destroyed when people do their laundry after leaving the devices in their pants pockets.

USB-based authentication

USB devices that contain authentication information — for example, digital certificates — can strengthen authentication. Care must be exercised, however, to use such devices only in combination with trusted machines — you don't want the device infected or destroyed by some device, and you want to be sure that the machine obtaining the certificate, for example, doesn't transmit it to an unauthorized party.

Many modern USB-based devices offer all sorts of defenses against such attacks. Of course, you can connect USB devices only to devices and apps that support USB-based authentication. You also must carry the device with you and ensure that it doesn't get lost or damaged.

Chapter 8

Preventing Social Engineering

IN THIS CHAPTER

- » Being aware of the various forms of social engineering attacks
 - » Discovering the strategies that criminals use to craft effective attacks
 - » Realizing how overshared information can help criminals
 - » Recognizing phony social media accounts
 - » Protecting yourself and your loved ones from social engineering attacks
-

Most, if not all, major breaches that have occurred in recent years have involved some element of social engineering. Do not let devious criminals trick you or your loved ones. In this chapter, you find out how to protect yourself

Don't Trust Technology More than You Would People

Would you give your online banking password to a random stranger who asked for it after walking up to you in the street and telling you that he worked for your bank?

If the answer is no — which it certainly should be — you need to exercise the same lack of trust when it comes to technology. The fact that your computer shows you an email sent by some party that claims to be your bank instead of a random person approaching you on the street and making a similar claim is no reason to give that email your trust any more than you would give the stranger.

In short, you don't give offers from strangers approaching you on the street the benefit of the doubt, so don't do so for offers communicated electronically — they may be even more risky.

Types of Social Engineering Attacks

Phishing attacks are one of the most common forms of social engineering attacks. (For more on phishing and social engineering, see [Chapter 2](#).) [Figure 8-1](#) shows you an example of a phishing email.

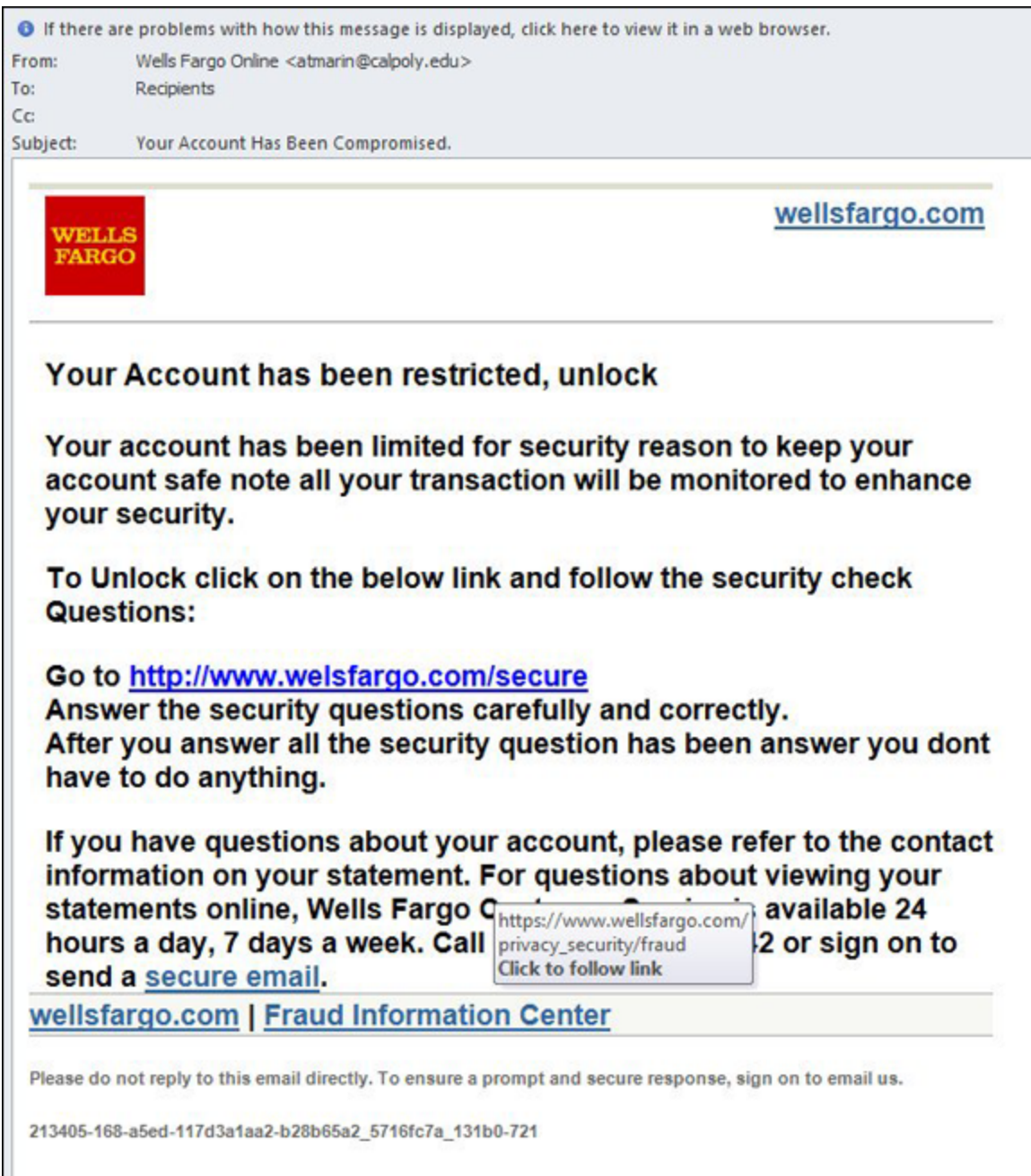


FIGURE 8-1: A phishing email.

Phishing attacks sometimes utilize a technique called *pretexting* in which the criminal sending the phishing email fabricates a situation that both gains trust from targets as well as underscores the supposed need for the intended victims to act quickly. In the phishing email shown in [Figure 8-1](#), note that the sender, impersonating Wells Fargo bank, included a link

to the real Wells Fargo within the email, but failed to properly disguise the sending address.

[Chapter 2](#) discusses common forms of social engineering attacks, including spear phishing emails, smishing, spear smishing, vishing, spear vishing, and CEO fraud. Additional types of social engineering attacks are popular as well:

- » **Baiting:** An attacker sends an email or chat message — or even makes a social media post that promises someone a reward in exchange for taking some action — for example, telling a target that if she completes a survey, she will receive a free item (see [Figure 8-2](#)). Sometimes such promises are real, but often they're not and are simply ways of incentivizing someone to take a specific action that she would not take otherwise. Sometimes such scammers seek payment of a small shipping fee for the prize, sometimes they distribute malware, and sometimes they collect sensitive information. There is even malware that baits.



WARNING Don't confuse baiting with *scambaiting*. The latter refers to a form of vigilantism in which people pretend to be gullible, would-be victims, and waste scammers' time and resources through repeated interactions, as well as (sometimes) collect intelligence about the scammer that can be turned over to law enforcement or published on the Internet to warn others of the scammer.

- » **Quid pro quo:** The attacker states that he needs the person to take an action in order to render a service for the intended victim. For example, an attacker may pretend to be an IT support manager offering assistance to an employee in installing a new security software update. If the employee cooperates, the criminal walks him through the process of installing malware.
- » **Social media impersonation:** Some attackers impersonate people on social media in order to establish social media connections with their victims. The parties being impersonated may be real people or

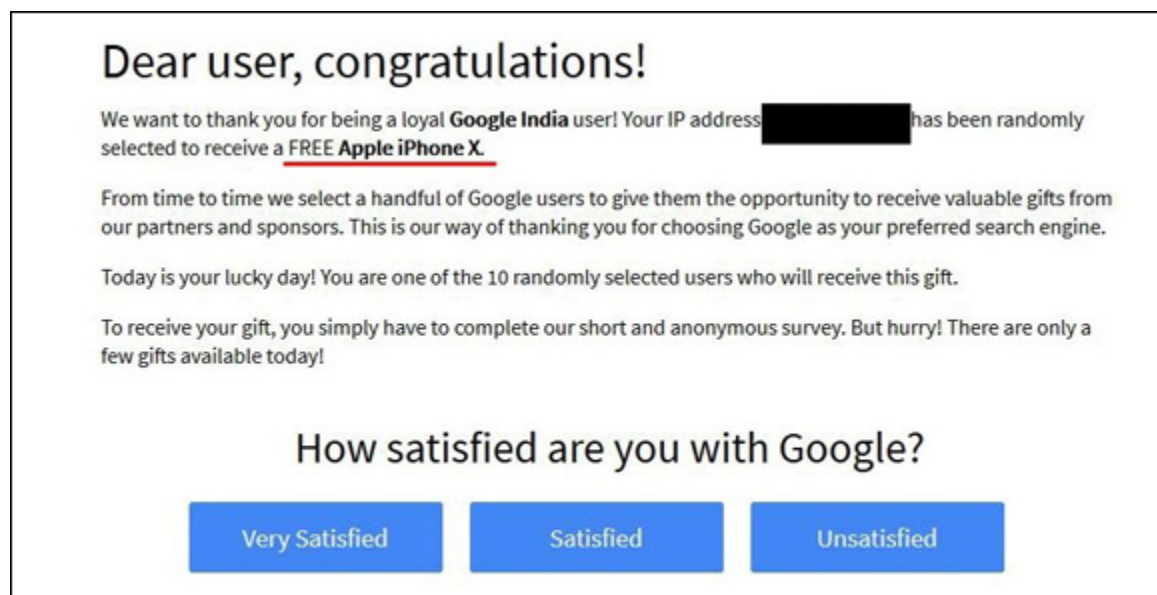
nonexistent entities. The scammers behind the impersonation shown in [Figure 8-3](#) and many other such accounts frequently contact the people who follow the accounts, pretending to be the author, and request that the followers make various “investments.” (To find out how you can protect yourself from social media impersonation, see the section “[General Cyberhygiene Can Help Prevent Social Engineering](#),” later in this chapter.)

- » **Tantalizing emails:** These emails attempt to trick people into running malware or clicking on poisoned links by exploiting their curiosity, sexual desires, and other characteristics.
- » **Tailgating:** *Tailgating* is a physical form of social engineering attack in which the attacker accompanies authorized personnel as they approach a doorway that they, but not the attacker, are authorized to pass and tricks them into letting him pass with the authorized personnel. The attacker may pretend to be searching through a purse for an access card, claim to have forgotten his card, or may simply act social and follow the authorized party in.
- » **False alarms:** Raising false alarms can also social engineer people into allowing unauthorized people to do things that they should not be allowed to. Consider the case in which an attacker pulls the fire alarm inside a building and manages to enter normally secured areas through an emergency door that someone else used to quickly exit due to the so-called emergency.
- » **Water holing:** Water holing combines hacking and social engineering by exploiting the fact that people trust certain parties, so, for example, they may click on links when viewing that party’s website even if they’d never click on links in an email or text message. Criminals may launch a watering hole attack by breaching the relevant site and inserting the poisoned links on it (or even depositing malware directly onto it).
- » **Virus hoaxes:** Criminals exploit the fact that people are concerned about cybersecurity, and likely pay undeserved attention to messages that they receive warning about a cyberdanger. Virus hoax emails may contain poisoned links, direct a user to download software, or

instruct a user to contact IT support via some email address or web page. These attacks come in many flavors — some attacks distribute them as mass emails, while others send them in a highly targeted fashion.

Some people consider scareware that scares users into believing that they need to purchase some particular security software (as described in [Chapter 2](#)) to be a form of virus hoax. Others do not because scareware’s “scaring” is done by malware that is already installed, not by a hoax message that pretends that malware is already installed.

- » **Technical failures:** Criminals can easily exploit humans’ annoyance with technology problems to undermine various security technologies.



Dear user, congratulations!

We want to thank you for being a loyal **Google India** user! Your IP address [REDACTED] has been randomly selected to receive a FREE Apple iPhone X.

From time to time we select a handful of Google users to give them the opportunity to receive valuable gifts from our partners and sponsors. This is our way of thanking you for choosing Google as your preferred search engine.

Today is your lucky day! You are one of the 10 randomly selected users who will receive this gift.

To receive your gift, you simply have to complete our short and anonymous survey. But hurry! There are only a few gifts available today!

How satisfied are you with Google?

Very Satisfied Satisfied Unsatisfied

FIGURE 8-2: Example of a baiting message.



FIGURE 8-3: An example of an Instagram account impersonating the author, using his name, bio, and primarily photos lifted from his real Instagram account.

For example, if a criminal impersonating a website that normally displays a security image in a particular area places a “broken image

symbol” in the same area of the clone website, many users will not perceive danger, as they are accustomed to seeing broken-image symbols and associate them with technical failures rather than security risks.

Six Principles Social Engineers Exploit

Social psychologist Robert Beno Cialdini, in his 1984 work published by HarperCollins, *Influence: The Psychology of Persuasion*, explains six important, basic concepts that people seeking to influence others often leverage. Social engineers seeking to trick people often exploit these same six principles, so I provide a quick overview of them in the context of information security.



TIP

The following list helps you understand and internalize the methods crooks are likely to use to try to gain your trust:

- » **Social proof:** People tend to do things that they see other people doing.
- » **Reciprocity:** People, in general, often believe that if someone did something nice for them, they owe it to that person to do something nice back.
- » **Authority:** People tend to obey authority figures, even when they disagree with the authority figures and even when they think what they’re being asked to do is objectionable.
- » **Likeability:** People are, generally speaking, more easily persuaded by people who they like than by others.
- » **Consistency and commitment:** If people make a commitment to accomplish some goal and internalize that commitment, it becomes part of their self-image, and they’re likely to attempt to pursue the

goal even if the original reason for pursuing the goal is no longer at all relevant.

- » **Scarcity:** If people think that a particular resource is scarce, regardless of whether it actually is scarce, they will want it, even if they don't need it.

Don't Overshare on Social Media

Oversharing information on social media arms criminals with material that they can use to social engineer you, your family members, your colleagues at work, and your friends.

If, for example your privacy settings allow anyone with access to the social media platform to see your posted media, your risk increases. Many times, people accidentally share posts with the whole world that they intended for only a small group of people.

Furthermore, in multiple situations, bugs in social media platform software have created vulnerabilities that allowed unauthorized parties to view media and posts that had privacy settings set to disallow such access.

Also, consider your privacy settings. Family-related material with privacy settings set to allow nonfamily members to view it may result in all sorts of privacy-related issues and leak the answers to various popular challenge questions used for authenticating users, such as "Where does your oldest sibling live?" or "What is your mother's maiden name?"



WARNING Don't rely on social media privacy settings to protect truly confidential data. Some social media platforms allow for granular protection of posted items, while others do not.

Certain items, if shared, may help criminals social engineer you or someone you know. This list isn't meant to be comprehensive. Rather, it's meant to illustrate examples to stimulate your thinking about the

potential risks of what you intend to post on social media before you go ahead and post it.

The following sections describes information you should be cautious of sharing on social media.



REMEMBER Numerous other types of social media posts than the ones I list in the following sections can help criminals orchestrate social engineering attacks. Think about potential consequences before you post and set your posts' privacy settings accordingly.

SOCIAL MEDIA WARNING SYSTEMS

Tools are available to warn people if they are oversharing on social media, including one which the author helped design. A snippet of a configuration screen appears in the figure

System Rules Business Rules Custom Rules Ignore Rules

- ☒ Financial institutions
Warn if the names of financial institutions are mentioned in your social media. Notifying people of where a person has accounts can help criminals commit fraud.
- ☐ Sins
Flag mentions of sex, alcohol, and drugs - public discussion of which is viewed in a negative light.
- ☐ Vulgarities
Warn if vulgarities are used.
- ☒ Doctors
Warn if the various types of doctors are mentioned. Often, it is possible for people to discern that a person has a specific medical condition from the type of doctor that they see; hence, this typ...
- ☒ Medical terminology
Warn if the various medical terms are mentioned. Often, it is possible for people to discern that a person has a specific medical

Your schedule and travel plans

Details of your schedule or someone else's schedule may provide criminals with information that may help them set up an attack. For example, if you post that you'll be attending an upcoming event, such as a wedding, you may provide criminals with the ability to *virtually kidnap* you or other attendees — never mind incentivizing others to target your home with a break-in attempt when the home is likely to be empty. (*Virtual kidnapping* refers to a criminal making a ransom demand in exchange for the same return of someone who the criminal claims to have kidnapped, but who in fact, the criminal has not kidnapped.)

Likewise, revealing that you'll be flying on a particular flight may provide criminals with the ability to virtually kidnap you or attempt CEO-type fraud against your colleagues. They may impersonate you and send an email saying that you're flying and may not be reachable by phone for confirmation of the instructions so just go ahead and follow them anyway.

Also, avoid posting about a family member's vacation or trip, which may increase risks of virtual kidnapping (and of real physical dangers to that person or his belongings).

Financial information

Sharing a credit card number may lead to fraudulent charges, while posting a bank account number can lead to fraudulent bank activity.

In addition, don't reveal that you visited or interacted with a particular financial institution or the locations where you store your money — banks, crypto-exchange accounts, brokerages, and so forth. Doing so can increase the odds that criminals will attempt to social engineer their way into your accounts at the relevant financial institution(s). As such, such sharing may expose you to attempts to breach your accounts, as well as targeted phishing, vishing, and smishing attacks and all sorts of other social engineering scams.

Posting about potential investments, such as stocks, bonds, precious metals, or cryptocurrencies, can expose you to cyberattacks because criminals may assume that you have significant money to steal. (If you

encourage people to invest or make various other forms of posts, you may also run afoul of SEC, CFTC, or other regulations.) You may also open the door to criminals who impersonate regulators and contact you to pay a fine for posting information inappropriately.

Personal information

For starters, avoid listing your family members in your Facebook profile's About section. That About section links to their Facebook profiles and explains to viewers the nature of the relevant family relationship with each party listed. By listing these relationships, you may leak all sorts of information that may be valuable for criminals. Not only will you possibly reveal your mother's maiden name (challenge question answer!), you may also provide clues about where you grew up. The information found in your profile also provides criminals with a list of people to social engineer or contact as part of a virtual kidnapping scam.

Also you should avoid sharing the following information on social media, as doing so can undermine your authentication questions and help criminals social engineer you or your family:

- » Your father's middle name
- » Your mother's birthday
- » Where you met your significant other
- » Your favorite vacation spot
- » The name of the first school that you attended
- » The street on which you grew up
- » The type, make, model, and/or color of your first car or someone else's
- » Your or others' favorite food or drink

Likewise, never share your Social Security number as doing so may lead to identity theft.

Information about your children



WARNING Sharing information about your children can not only set you up for attacks, but put your children at great risk of physical danger. For example, photos of your children may assist a kidnapper. The problem may be exacerbated if the images contain a timestamp and/or *geotagging* — that is, information about the location at which a photograph was taken.

Timestamps and geotagging do not need to be done per some technical specification to create risks. If it is clear from the images where your kids go to school, attend after-school activities, and so on, you may expose them to danger.

In addition, referring to the names of schools, camps, day care facilities, or other youth programs that your children or their friends attend may increase the risk of a pedophile, kidnapper, or other malevolent party targeting them. Such a post may also expose you to potential burglars because they'll know when you're likely not to be home. The risk can be made much worse if a clear pattern regarding your schedule and/or your children's schedule can be extrapolated from such posts.

Also avoid posting about a child's school or camp trip.

Information about your pets

As with your mother's maiden name, sharing your current pet's name or your first pet's name can set you or others who you know up for social engineering attacks because such information is often used as an answer to authentication questions.

Work information

Details about with which technologies you work with at your present job (or a previous job) may help criminals both scan for vulnerabilities in your employers' systems and social engineer your colleagues.

Many virus hoaxes and scams have gone viral — and inflicted far more damage than they should have — because criminals exploit people's fear of cyberattacks and leverage the likelihood that many people will share

posts about cyber-risks, often without verifying the authenticity of such posts.

Information about a moving violation or parking ticket that you received not only presents yourself in a less-than-the-best light, but can inadvertently provide prosecutors with the material that they need to convict you of the relevant offense. You may also give crooks the ability to social engineer you or others — they may pretending to be law enforcement, a court, or an attorney contacting you about the matter — perhaps even demanding that a fine be paid immediately in order to avoid an arrest.

In addition to helping criminals social engineer you in a fashion similar to the moving violation case, information about a crime that you or a loved one committed may harm you professionally and personally.

Medical or legal advice

If you offer medical or legal advice, people may be able to extrapolate that you or a loved one has a particular medical condition, or involved in a particular legal situation.

Your location

Your location or *check-in* on social media may not only increase the risk to yourself and your loved ones of physical danger, but may help criminals launch virtual kidnapping attacks and other social engineering scams.

A happy birthday message to anyone may reveal the person's birthday. Folks who use fake birthdays on social media for security reasons have seen their precautions undermined in such a fashion by would be well-wishers. Anything that is "sin-like" may lead not only to professional or personal harm, but to blackmail-like attempts as well as social engineering of yourself or others depicted in such posts or media.

In addition, an image of you in a place frequented by people of certain religious, sexual, political, cultural, or other affiliations can lead to criminals extrapolating information about you that may lead to all sorts of social engineering. Criminals are known, for example, to have

virtually kidnapped a person who was in synagogue and unreachable on the Jewish holiday of Yom Kippur. They knew when and where he would be walking on his way to the temple, and called family members (at a time that they knew he would be impossible to reach) claiming to have kidnapped the person. The family members fell for the virtual kidnapping scam because the details were right and they were unable to reach the “victim” by telephone in the middle of a synagogue service.

Leaking Data by Sharing Information as Part of Viral Trends

From time to time, a *viral trend* occurs, in which many people share similar content. Posts about the ice bucket challenge, your favorite concerts, and something about you today and ten years ago are all examples of viral trends. Of course, future viral trends may have nothing to do with prior ones. Any type of post that spreads quickly to large numbers of people is said to have “gone viral.”



WARNING While participating may seem fun — and “what everyone else is doing” — be sure that you understand the potential consequences of doing so. For example, sharing information about the concerts that you attended and that you consider to be your favorites can reveal a lot about you — especially in combination with other profile data — and can expose you to all sorts of social engineering risks.

Identifying Fake Social Media Connections

Social media delivers many professional and personal benefits to its users, but it also creates amazing opportunities for criminals — many people have an innate desire to connect with others and are overly trusting of social media platforms. They assume that if, for example, Facebook sends a message that Joseph Steinberg has requested to become a friend, that the real “Joseph Steinberg” has requested as such — when, often, that is not the case.

Criminals know, for example, that by connecting with you on social media, they can gain access to all sorts of information about you, your family members, and your work colleagues — information that they can often exploit in order to impersonate you, a relative, or a colleague as

part of criminal efforts to social engineer a path into business systems, steal money, or commit other crimes.

One technique that criminals often use to gain access to people's "private" Facebook, Instagram, or LinkedIn information is to create fake profiles — profiles of nonexistent people — and request to connect with real people, many of whom are likely to accept the relevant connection requests. Alternatively, scammers may set up accounts that impersonate real people — and which have profile photos and other materials lifted from the impersonated party's legitimate social media accounts.

How can you protect yourself from such scams? The following sections offer advice on how to quickly spot fake accounts — and how to avoid the possible repercussions of accepting connections from them.



REMEMBER Keep in mind that none of the clues in the following sections operates in a vacuum or is absolute. The fact that a profile fails when tested against a particular rule, for example, doesn't automatically mean that it is bogus. But applying smart concepts such as the ones I list in the following sections should help you identify a significant percentage of fake accounts and save yourself from the problems that can ultimately result from accepting connection requests from them.

Photo

Many fake accounts use photos of attractive models, sometimes targeting men who have accounts that show photos of women and women whose accounts have photos of men. The pictures often appear to be stock photos, but sometimes are stolen from real users.



WARNING If you receive a social media connection request from someone who you don't remember ever meeting and the picture is of this

type, beware. If you're in doubt, you can load the image into Google's reverse image search and see where else it appears.

You can also search on the person's name (and, if appropriate, on LinkedIn) or title to see whether any other similar photos appear online. However, a crafty impersonator may upload images to several sites.

Obviously, any profile without a photo of the account holder should raise red flags. Keep in mind, though, that some people do use emojis, caricatures, and so on as profile photos, especially on nonprofessional-oriented social media networks.

Verification

If an account appears to represent a public figure who you suspect is likely to be verified (meaning it has a blue check mark next to the user's account name to indicate that the account is the legitimate account of a public figure), but it is not verified, that is a likely sign that something is amiss.

Likewise, it is unlikely that a verified account on a major social media platform is fake. However, there have been occasions on which verified accounts of such nature have been taken over temporarily by hackers.

Friends or connections in common

Fake people are unlikely to have many friends or connections in common with you, and fake folks usually will not even have many secondary connections (Friends of Friends, LinkedIn second level connections, and so on) in common with you either.



WARNING Don't assume that an account is legitimate just because it has one or two connections in common with you; some of your connections may have fallen for a scam and connected with a fake person, and your contact's connecting with the fake account may be how the criminal found out about you in the first place. Even in such a scenario, the number of shared connections is likely to be relatively small as compared with a real, mutual connection, and the human relationship between the friends who did connect with the crook's profile may seem difficult to piece together.

You know your connections better than anyone else — exercise caution when someone's connection patterns don't make sense. You may want to think twice, for example, if someone trying to connect with you seems to know nobody in the industry in which she works, but knows three of your most gullible friends who live in three different countries and who do not know one another.

Relevant posts

Another huge red flag is when an account is not sharing material that it should be sharing based on the alleged identity of the account holder. If someone claims to be a columnist who currently writes for *Forbes*, for example, and attempts to but has never shared any posts of any articles that he or she wrote for *Forbes*, something is likely amiss.

Number of connections

A senior-level person, with many years of work experience, is likely to have many professional connections, especially on LinkedIn. The fewer connections that an account ostensibly belonging to a senior level person has on LinkedIn (the further it is from 500 or more), the more suspicious you should be.

Of course, every LinkedIn profile started with zero connections — so legitimate, new LinkedIn accounts may seem suspicious when they truly are not — but practical reality comes into play: How many of the

real, senior-level people who are now contacting you didn't establish their LinkedIn accounts until recently? Of course, a small number of connections and a new LinkedIn account isn't abnormal for a person who just started his first job or for people working in certain industries, in certain roles, and/or at certain companies — CIA secret agents don't post their career progress in their LinkedIn profiles — but if you work in those industries, you're likely aware of this fact already.

Contrast the number of connection with the age of an account and the number of posts it has interacted with or has shared — a person who has been on Facebook for a decade and who posts on a regular basis, for example, should have more than one or two Friends.

Industry and location

Common sense applies vis-à-vis accounts purporting to represent people living in certain locations or working in certain industries. If, for example, you work in technology and have no pets and receive a LinkedIn connection request from a veterinarian living halfway across the world whom you have never met, something may be amiss.

Likewise, if you receive a Facebook friend request from someone with whom you have nothing in common, beware.



WARNING Don't assume that any claims made in a profile are necessarily accurate and that if you share a lot in common, the sender is definitely safe. Someone targeting you may have discerned your interests from information about you that is publicly available online.

Similar people

If you receive multiple requests from people with similar titles or who claim to work for the same company and you don't know the people and aren't actively doing some sort of deal with that company, beware. If those folks don't seem to be connected to anyone else at the company

who you know actually works there, consider that a potential red flag as well.



REMEMBER You can always call, text, or email a real contact and ask whether she sees that person listed in a staff directory.

Duplicate contact

If you receive a Facebook friend request from a person who is already your Facebook friend, verify with that party that she is switching accounts. In many cases, such requests come from scammers.

Contact details

Make sure the contact details make sense. Fake people are far less likely than real people to have email addresses at real businesses and rarely have email addresses at major corporations. They're unlikely to have physical addresses that show where they live and work, and, if such addresses are listed, they rarely correspond with actual property records or phone directory information that can easily be checked online.

LinkedIn Premium status

Because LinkedIn charges for its Premium service, some experts have suggested that Premium status is a good indicator that an account is real because a criminal is unlikely to pay for an account.

While it may be true that most fake accounts don't have Premium status, some crooks do invest in obtaining Premium status in order to make their accounts seem more real. In some cases, they are paying with stolen credit cards, so it doesn't cost them anything anyway. So, remain vigilant even if an account is showing the Premium icon.

LinkedIn endorsements

Fake people are not going to be endorsed by many real people. And the endorsers of fake accounts may be other fake accounts that seem suspicious as well.

Group activity

Fake profiles are less likely than real people to be members of closed groups that verify members when they join and are less likely to participate in meaningful discussions in both closed and open groups on Facebook or LinkedIn. If they are members of closed groups, those groups may have been created and managed by scammers and contain other fake profiles as well.

Fake folks may be members of many open groups — groups that were joined in order to access member lists and connect with other participants with “I see we are members of the same group, so let’s connect” type messages.



WARNING In any case, keep in mind that on any social platform that has groups, being members of the same group as someone else is not, in any way, a reason to accept a connection from that person.

Appropriate levels of relative usage

Real people who use LinkedIn or Facebook heavily enough to have joined many groups are more likely to have filled out all their profile information. A connection request from a person who is a member of many groups but has little profile information is suspicious.

Likewise, an Instagram account with 20,000 followers but only two posted photos that seeks to follow your private account is suspicious for the same reason.

Human activities

Many fake accounts seem to list cliché-sounding information in their profiles, interests, and work experience sections, but contain few other details that seem to convey a true, real-life human experience.

Here are a few signs that things may not be what they seem:

- » On LinkedIn, the Recommendations, Volunteering Experience, and Education sections of a fake person may seem off.
- » On Facebook, a fake profile may seem to be cookie cutter and the posts generic enough in nature that millions of people could have made the same post.
- » On Twitter, they may be retweeting posts from others and never share their own opinions, comments, or other original material.
- » On Instagram the photos may be lifted from other accounts or appear to be stock photos — sometimes none of which include an image of the actual person who allegedly owns the accounts.



TIP

The content within a user's social media profile may provide terms and phrases that you can search for in Google along with the person's name to help you verify whether the account truly belongs to a human being whose identity the profile alleges to represent.

Likewise, if you perform a Google image search on someone's Instagram images and see that they belong to other people, something is amiss.

Cliché names

Some fake profiles seem to use common, flowing American names, such as Sally Smith, that both sound overly American and make performing a Google search for a particular person far more difficult than doing so would be for someone with an uncommon name.



TIP

More often than occurs in real life, but certainly not always, bogus profiles seem to use first and last names that start with the same letter. Perhaps, scammers just like the names or, for some reason, find them funny.

Poor contact information

If a social media profile contains absolutely no contact information that can be used to contact the person behind the profile via email, telephone, or on another social platform, beware.

Skill sets

If skill sets don't match someone's work or life experience, beware.

Something may seem off when it comes to fake accounts. For example, if someone claims to have graduated with a degree in English from an Ivy League university, but makes serious grammatical errors throughout his profile, something may be amiss.

Likewise, if someone claims to have two PhDs in mathematics, but claims to be working as a gym teacher, beware.

Spelling

Spelling errors are common on social media. However, something may be amiss if someone misspells her own name or the name of an employer, or makes errors of this nature on LinkedIn (a professionally oriented network).

Suspicious career or life path

People who seem to have been promoted too often and too fast or who have held too many disparate senior positions, such as VP of Sales, then CTO, and then General Counsel, may be too good to be true.

Of course, real people have moved up the ladder quickly and some folks (including myself) have held a variety of different positions throughout the course of their careers, but scammers often overdo it when crafting the career progression or role diversity data of a bogus profile. People may shift from technical to managerial roles, for example, but it is extremely uncommon for someone to serve as a company's VP of Sales, then as its CTO, and then as its General Counsel — roles that require different skill sets, educational backgrounds, and potentially, different certifications and licenses.



TIP

If you find yourself saying to yourself “no way” when looking at someone’s career path, you may be right.

Level or celebrity status

LinkedIn requests from people at far more senior professional levels than yourself can be a sign that something is amiss, as can Facebook requests from celebrities and others about whose connection request you’re flattered to have received.

It is certainly tempting to want to accept such connections (which is, of course, why the people who create fake accounts often create such fake accounts), but think about it: If you just landed your first job out of college, do you really think the CEO of a major bank is suddenly interested in connecting with you out of the blue? Do you really think that Ms. Universe, whom you have never met, suddenly wants to be your friend?

In the case of Facebook, Instagram, and Twitter, be aware that most celebrity accounts are verified. If a request comes in from a celebrity, you should be able to quickly discern if the account sending it is the real deal.

Using Bogus Information

Some experts have suggested that you use bogus information as answers to common challenge questions. Someone — especially someone whose mother has a common last name as her maiden name — may establish a new mother’s maiden name to be used for all sites that ask for such information as part of an authentication process. There is truth to the fact that such an approach somewhat helps reduce the risk of social engineering.

What it does even stronger, though, is reveal how poor challenge questions are as a means of authenticating people. Asking one’s mother’s

maiden name is effectively asking for a password while providing a hint that the password is a last name!

Likewise, because in the era of social media and online public records, finding out someone's birthday is relatively simple, some security experts recommend creating a second fake birthday for use online. Some even recommend using a phony birthday on social media, both to help prevent social engineering and make it harder for organizations and individuals to correlate one's social media profile and various public records.

While all these recommendations do carry weight, keep in mind that, in theory, there is no end to such logic — establishing a different phony birthday for every site with which one interacts offers stronger privacy protections than establishing just one phony birthday, for example.

In general, however, having one fake birthday, one fake mother's maiden name, and so on is probably worthwhile and doesn't require much additional brainpower and mindshare over using just the real one. Be sure, however, not to mislead any sites where providing accurate information is required by law (for example, when opening a credit card account).

Using Security Software

Besides providing the value of protecting your computer and your phone from hacking, various security software may reduce your exposure to social engineering attacks. Some software, for example, filters out many phishing attacks, while other software blocks many spam phone calls. While using such software is wise, don't rely on it. There is a danger that if few social engineering attacks make it through your technological defenses, you may be less vigilant when one does reach you — don't let that happen.

While smartphone providers have historically charged for some security features, over time they have seen the value to themselves of keeping their customers secure. Today, basic versions of security software,

including technology to reduce spam calls, are often provided at no charge along with smartphone cellular-data service.

General Cyberhygiene Can Help Prevent Social Engineering

Practicing good cyberhygiene in general can also help reduce your exposure to social engineering. If your children, for example, have access to your computer but you encrypt all your data, have a separate login, and don't provide them with administrator access, your data on the machine may remain safe even if a criminal social engineers his way into your child's account.

Likewise, not responding to suspicious emails or providing information to potential scammers who solicit it can help prevent all sorts of social engineering and technical attacks.