Security Advice

Version 1.0, 2019-03-04

by Joe Ganley, http://joeganley.com/

Pay attention to which accounts need the most protection. Your email is crucial – if an attacker gets into your email, they're a long way toward owning any other account you have. Banking is obviously important. Anything that stores a lot of Personally Identifying Information (PII), especially things like Social Security Numbers (SSNs) or dates of birth, requires extra protection.

Use different passwords between different logins. The best thing to do is to use a password manager and long random passwords (see below), but at a bare minimum append the name of the web site to your password (e.g. instead of "password" you'd use "passwordpaypal" for paypal, "passwordbofa" for Bank of America, etc.). This is weak, but it's *far* better than just using the same password everywhere. I don't trust the "save passwords" feature of web browsers, but even using that with different passwords for every web site is more secure than using the same password everywhere and not storing them.

Use long passwords that aren't words. Include numbers and symbols. Currently any 8-character password can be broken brute-force in a few hours on a regular computer.

Never share your passwords with anyone. Especially, never ever ever give your password to anyone who calls you on the phone or sends you email. These are common scams.

Change your passwords periodically. Again, if you use a password manager you can set it to remind you.

The main threat model here is a hacker breaching a service where you have an account. You have doubtless heard of many such breaches in the press (OPM, Anthem, Target, Home Depot, etc.), and your information is probably contained in at least some of them. Passwords are usually stored in hashed form - that is, passed through a function that turns them into random-looking garbage that can't be reversed back into a password. However, if an attacker has your hashed password, they can run guesses through the same hashing function, and when they get the same hash, they know they guessed your password. So… they've breached a company, and now they have your username and password hash. They will try to crack your password by running common passwords, dictionary words, and brute-force combinations of limited numbers of characters (as above, 8 or so characters is currently about the limit of current brute-force technology). So, you use long random passwords to try to make this cracking harder, you change your password periodically so that the password in the breach isn't good any more, and you use different passwords for different accounts so that if they do break one, they don't have your password for every system now. (By the way, in a few breaches the company had been storing passwords in the clear, not even hashed.)

There is a web site called haveibeenpwned.com where you can go and enter your email address, and it will tell you which known breaches that address appears in.

Use two-factor authentication when available. This is where in addition to your username and password, either they text you a code that you have to enter, or they ask for a code from an app like Google Authenticator. Now, even if bad guys get your username and password, getting into your account is *much* harder. Not quite impossible, but generally hard enough. As with all security, you don't have to be perfect, you just have to be harder to break into than other people. ("I don't have to outrun the bear, I just have to outrun you.")

Your PII is valuable. With enough pieces of information about you, hackers can convince a company that they are you sufficiently well to, say, reset your password, and then your account is owned.

When registering with web sites and companies, provide no information that isn't required. Where they do require information, if it isn't information that you think they need to provide the service you're engaging them for, provide fake information. (For example, if it's something that will involve them pulling a credit report, then they probably need my real date of birth; otherwise I give them a false one.)

Similarly, don't use real information in security questions. Ideally, make up different answers for every web site, but at a minimum have a single set of fake first pet's name, city of birth, etc. and use that instead of your real answers. It's quite easy for bad guys to learn the real answers to a lot of common security questions.

Be cautious what information you share on social media. Facebook is a gold mine for security-question answers. Many people also give Facebook their birth date (month and day), and there is typically a small range of reasonable guesses for the year. Here, too, I use fake information. Also lock down your privacy settings so that no one but your Facebook friends has access to this information. Check those settings periodically, as companies (Facebook is especially notorious) have a bad habit of changing the security defaults on occasion.

Never share PII with someone who called you on the phone or emailed you. If you think it might be legit, hang up and call/email the company back at a number/address that you look up, not one that the sender provides. No company will try to do legitimate sensitive business over the phone via a cold call.

Don't send sensitive information like SSNs or passwords over email. If you must share them (remember, you're not supposed to be sharing passwords at all!), best is to do so by voice call, and second-best is to do it by text. Delete the text when you're done and ask the recipient to do the same.

Don’t click links in email. Ideally, never. At a minimum, inspect the link (often the URL appears in your status bar if you hover over it) and make sure it is what it says it is. Again, instead of clicking a link, manually go to the web site yourself.

Don’t type anything sensitive, including passwords, over public WiFi (especially unsecured WiFi). A bad guy can easily set himself up at Panera and stand up a WiFi network called “Panera” that captures everything you send over it.

Make regular backups. The easiest way to do this is an online service like Carbonite, but those cost money (typically around $10/month). I do this for my wife’s business computer, but for our personal computers I just have an external hard drive to which I do a Time Machine backup every couple of weeks.

Install operating system and software updates as soon as they are available. This applies to computers and also phones. Often these updates are issued because a vulnerability has been discovered, so if you don’t install the update then you are susceptible to this newly-discovered vulnerability, which now the entire world knows about. Easiest is just to turn on automatic updates.

Run an antivirus program. On the Mac, I use the free versions of Avast and MalwareBytes. I imagine that there are cheap/free options on Windows too.

On your home WiFi router, change the default network name, turn on security (ideally WPA2), and change the router’s default admin password.

Secure your phone in some way – passcode, touch ID, face ID, whatever, but just don’t leave it wide open. Ideally use a passcode of 6 or more digits.

Always erase all devices completely before disposing of them.

When swiping a credit/debit card, inspect the device. Grab it and wiggle it. Bad guys install “skimmers”, devices that cover and look just like the real device but steal your info while you use them. Similarly, avoid janky ATMs like the ones you see in gas stations and such.

Avoid using debit cards. If a thief steals from your credit card, there are protections in place such that you won’t be liable for the fraudulent charges. If a thief steals from your debit card, that money may well be lost forever. If you must use debit cards, at least avoid using them at unattended points of sale like gas pumps.

Control your trash. Anything with PII on it, ideally get a shredder and shred it, otherwise at least tear it up, or at a bare minimum throw it in your own trash can and not a public one. This goes especially for credit-card offers, credit-card balance transfer checks, etc. BTW, if you don’t use them, you can call your credit-card companies and ask them not to send you those balance transfer checks.

Next Level

If you're doing all of the stuff above, these are the next things you should consider doing to secure your life even more.

Use a password manager. Generate different random long passwords for every account. I use KeePassX, and use 25-character passwords containing all four character classes (upper- and lowercase letters, numbers, and symbols). I set the expirations in KeePassX to remind me to change my passwords annually, and more often for especially sensitive accounts like banking. KeePassX also has a "notes" field for each account, where you can store (for example) your fake security-question answers. Password manager databases are encrypted, and secured with a password that you type into the password manager to open it. Use a very long, very secure password here, and don't store that password on your devices anywhere. **Be sure to back up your password-manager file!** Since you should be backing up your computer anyway, this file will be backed up that way. I also use MiniKeePass on my phone (which opens the same database), and AirDrop the file to my phone weekly, so that's another backup.

Clear your browser history periodically. Check every box to clear everything, all the way back to the beginning of time. This is a pain, as you will have to re-login to every web site, all of your autocompletes and saved passwords will be gone, etc. However, it will clear out all of the old stale logins, tracking cookies, and general personal detritus of web browsing.

Keep and use a separate credit card for online purchases, and another different one for all recurring direct debits. Don't carry that one around; keep it somewhere safe. That way you don't have to deal with the hassle of losing the card or having it stolen, and having to update all of those debit arrangements.

Make a guest WiFi network. Some routers will let you make both a regular and a guest network in the same router; otherwise you can get a second router to be the guest network (routers are cheap). Give the guest network's credentials to (duh) your guests, and keep the credentials for the real network secret among the members of your household. I also put all "Internet of Things" devices (cameras, Amazon Echos, Smart TVs, etc.) on the guest network, since such devices are notoriously insecure and easy to hack.

Turn off "Universal Plug and Play" (UPnP) on your router.

When you take photos with your phone, often those photos include a lot of metadata about where the photo was taken, the device it was taken with, etc. Consider stripping that metadata before posting photos online. There are free tools that do this.

Create an account on your computer with admin privileges, but don't give admin privileges to your normal everyday account. That way when a piece of software tries to do something to

your computer, you'll be prompted for the admin login. If it is trying to do something you didn't ask it to, now you know, as opposed to this action just silently succeeding if your normal account has admin privileges.

Turn off your phone's capabilities from the lock screen – Siri, replying to texts, etc.

Don't put social-media apps on your phone. Facebook, especially, is really bad about tracking your movements and actions, even when the app isn't running.

Consider getting a "burner" phone number from Google Voice or Hushed or other such services, and give that out to companies instead of your real phone number.