Feb 1st, 10:40 AM - 11:25 AM

Hack the Planet! -- Cybersecurity Tips to Keep You, Your Data, and Your Clients Safe

Jason Tubinis
University of Georgia School of Law Library, jtubinis@uga.edu

Hack the Planet! – Cybersecurity Tips to Keep You, Your Data, and your Client Safe

Jason Tubinis, J.D.
Information Technology Librarian
Alexander Campbell King Law Library
University of Georgia School of Law
Athens, Georgia

Table of Contents

Introduction

Here's a couple good news/bad news scenario regarding you (yes, you) that you may or may not be familiar with. First, the Bad News: your Social Security Number has already been stolen. You were diligent, did your best to keep it secret, but ultimately it got out there. Bummer. But don't worry, the Good News is that it's not your fault! This may be cold comfort, having such an important piece of personally identifying information out there and available to the world, but there really wasn't much you could do about it. As a result of numerous high-profile hacks of companies like Target, Home Depot, and Equifax, millions of Americans have had SSNs, financial information, medical records, and other sensitive pieces of data stolen. Chances are, you're one of those million (don't worry, I am too).

Ready for more good news/bad news? Let's flip the script on this one, so I'll start with the Good News: unless you have something the bad guys really want, you don't really have to worry about being the target of an explicit hack. Cyber-crimes, like most crimes, are acts of opportunity, so unless you leave yourself largely unprotected, most hackers will pass individuals over for more desirable targets. Of course, the Bad News being that lawyers and law firms are in a three way tie (along with health care providers and financial institutions) as being some of the most desirable targets.

But enough doom and gloom. Here's some Good News with no Bad News attached: it is really easy to make you, your practice, and your clients safe from being the victims of a cyber-crime. This paper will discuss some tips, tricks, and considerations you can implement quickly, safely, and on the cheap. These are relatively simple suggestions, though. You should be able to implement most of these practices within an

hour, and while they will save you from the most common security flaws Bad Guys are looking to exploit. For more in-depth cybersecurity recommendations for attorneys, I highly recommend "Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security" by John Bandler, "The ABA Cybersecurity Handbook: A Resources for Attorneys, Law Firms, and Business Professionals" by Jill D. Rhodes and Robert S. Litt. The State Bar of Georgia also maintains a Software Library[1] for evaluation and testing purposes as part of their Law Practice Management Program, including security, encryption, and secure communications software.

Personal Security Practices

Encrypt Your Phone – As you may recall from the 2015 San Bernardino attack, there was a very significant and public kerfuffle between Apple and the FBI regarding the iPhone 5C used by one of the shooters. The dispute arose whether Apple would hand over the software keys necessary to unlock the data encrypted on the device because they were unable to do so themselves. Setting aside the specifics of the nature of the disagreement between the two parties, it should be telling that the FBI was unable to crack the standard encryption used on a piece of consumer electronics. Modern data encryption is just that strong. Which is good, because nothing spells catastrophe for an organization like the loss of a device storing a bunch of sensitive information.

Fortunately enough, as long as you are using some kind of security measure to access your device (like a password, PIN, or fingerprint scanner), encryption is enabled

[1] https://www.gabar.org/committeesprogramssections/programs/lpm/library/software-library.cfm

by default on current Android and Apple devices. First of all, if you aren't already, please use some kind method to unlock your device. I die a little on the inside when I see anyone that accesses the functionality of their device with a simple swipe. For Apple devices:

> "On devices running iOS 4–iOS 7, you can do this by going to the General settings, and choosing Passcode (or iTouch & Passcode). As for iOS 8-9, Passcode (or "Touch ID & Passcode") has its own section in the Settings app. Follow the prompts to create a passcode. You should set the "Require passcode" option to "Immediately," so that your device isn't unlocked when you are not using it. Disable Simple Passcode so that you can use a code that's longer than 4 digits… Once you've set a passcode, scroll down to the bottom of the Passcode settings page. You should see a message that says "Data protection enabled." This means that the device's encryption is now tied to your passcode, and that most data on your phone will need that code to unlock it."[2]

For Android devices it's either a lot easier or quite a bit trickier. If your phone came with Android version 7.x pre-installed (so purchased sometime after September 2016), congratulations! You have some very stout file-based encryption. Otherwise, you'll have to jump through some hoops, the very first being the understanding that when you enable encryption on an Android device, **it will perform a factory data reset of your device**. In other words, your device will go back to being a blank slate. So beforehand, go to Settings > System > Backup and Reset, and make sure the "Backup my data" option is enabled and it's linked to a Google Account. This will reload your apps and settings after you reset your phone. Next:

> "Once you've backed up your data (seriously, do it), you'll need to enable the Android Developer Options if you haven't already. Do this by navigating to Settings > About phone, scrolling to the bottom of the screen, and tapping the Build number entry seven times. You'll be presented with a congratulatory message — "You are now a developer!"

[2] https://ssd.eff.org/en/module/how-encrypt-your-iphone

> You can now find a new menu full of hidden wonders at Settings > Developer options… There are a lot of fun options to play with here, and a lot of ways to break things. In general, I don't recommend just randomly flipping toggles unless you actually understand what they do — or, as in this case, Some Guy On The Internet tells you that it's okay. We're interested in the entry titled Convert to file encryption. Go ahead and tap it."[3]

From there, it's time for your phone to wipe itself clean, prepare the phone for encryption, and then use the backup data to restore the phone to its original working condition.

Turn on Two-Factor Authentication – Have you ever had Google ask you for your phone number? Did you actually give it to them? Probably not; Google has already gobbled up enough information about us as it is, so why do they need your digits as well? Actually, there's a really good reason called "two-factor authentication." The name is self-explanatory: you're basically use two different passwords to get into an account. The first passwords is the one you're used to, but the second password isn't one you'll always know. Instead, a service using two-factor authentication will send you a special password that will only show up in a place you can access it, like a text-message on your phone, an email account, or a special device (like a key fob). This way it's impossible for someone to access your accounts with just a password.

While this seems obnoxious, having to log in twice and with a special code that's been texted to you, most services using two-factor authentication will only require the two passwords when they notice weird things going on with your account. For example, I had given my phone number to Google just to see what would happen. About a year of completely normal logins later, I was suddenly prompted for second password. Not five

[3] https://yourtechexplained.com/2016/12/08/explained-android-nougat-file-based-encryption/

seconds of confused head-scratching later, a text popped up with a short code that I plugged into Gmail. It proceeded to explain in detail how it appeared that someone in a small prefecture in China was attempting to log into my email and that was how this had been triggered. I promptly changed passwords to something far stronger and proceeded to enable two-factor authentication for every service that offered it. So don't worry what these services and sites are doing with your phone number or email address, it's well worth the peace of mind.

Use a Password Manager – Good passwords are tough. We're supposed to have unique, challenging passwords for every account and website we interact with, so that if one service were to be hacked, only that service would be potentially compromised. Of course, who does that? Most people probably only use a handful of passwords with minor variations over all their myriad accounts. We can recognize how that could be a problem, but for the sake of our sanity and actually using these services, we lapse into poor habits. And that's where a host of different apps come to save the day. Password managers are simply browser plug-ins and apps that will collect your account information and manage the process of logging in. They'll also help you identify weak or duplicate passwords, generate secure password replacements (for the aforementioned weak ones), sync this information across devices and computers, and offer two-factor authentication for access to the manager. If you'd like to test out the use of a password manager, there are free products like LastPass and LogMeOnce Password Management Suite that will familiarize you with how they work. There are also password managers that offer more robust features, but are either 1-time purchases or have a monthly subscription. Highly rated paid apps include Dashlane, Sticky Password, and Keeper Password Manager & Digital Vault.

If you'd like to take password management seriously but don't want to invest in a password manager, consider using a passphrase instead. Passphrases differ from passwords in that passwords are 6 to 10 character long words with the occasional number or special character thrown in. Passphrases are 6 to 10 words together, either randomly chosen or a complete sentence. Being longer and more complex, passphrases are significantly more challenging to guess or to use computers to just keep guessing ("brute force"). Using modern computing technology, it takes about four months to brute force a 10 character password, but that time frame is always dropping as computers get faster and faster. A random 10 word passphrase, however, currently takes so long that the heat death of the universe would occur before a computer could hack it.

Be Wary of Free Wi-Fi – No one likes to dip into their data plan when there's a perfectly good Wi-Fi hotspot available. But is that hotspot legit, or is someone hoping to find your email password? Let's talk about the Republican National Convention for a bit. As an experiment, in 2016 security researchers from Avast (a cybersecurity software company), went to the RNC site in Cleveland and set up a few open hotspots around the convention center and airport. Over the course of the convention, 1.6 gigabytes of data was transferred over the unsecured Wi-Fi connections and about 70% of the users' identities were exposed as they connected.[4] There was some pretty interesting information revealed, but it was ultimately a harmless experiment that highlighted a gaping hole in our device usage. For example, if I was a Bad Guy, I would sit in a coffee place a block from a big firm, set up an open Wi-Fi hotspot called something like

[4] https://www.helpnetsecurity.com/2016/07/22/wi-fi-hack-experiment-republican-national-convention/

"Google Starbucks", harvest data for a week, and see what emails, accounts, and passwords I had collected.

For casually browsing, connecting to free Wi-Fi is sketchy, but fine. You never want to expose yourself to something malicious, but if all you're doing is checking the weather or football scores, it's hard for a Bad Guy to do much with that information. But as soon as any account or financial information is being transmitted, exercise some diligence. Eating into your data might not be ideal, but it's better than having sensitive information plucked out of the ether. If you'd like to go the extra step to secure your Wi-Fi connections as well, consider investing in a Virtual Private Network (aka a VPN).

Update Update Update – Devices, computers, apps, programs, etc.; if it's connected to the Internet, keep it updated. Full stop. I recognize how obnoxious updates can be: they happen all the time, they take forever to download and install, you have to stop what you're doing while the whole process happens, new versions add annoying new features or remove/change favorite features, and so on. But more often than not, updates are fixing security issues, and that's always worth your time. This was the entire flaw behind the Equifax hack: Equifax was using an outdated piece of software that had a very well documented and publicly acknowledged security flaw. The publishers of the software fixed the problem almost immediately after it was discovered, but the information technology folks at Equifax failed to update and left the program sit unpatched for four to five months.

The only time you should entertain the notion of keeping something from being updated is if it will break the functionality of another very important program. There are many programs developed for older versions of the Windows operating system that

don't have an analogous program that work on newer Windows computers. In these circumstances, one should definitely consider removing the computer from the network.

Understand What Your Apps and Programs Are Doing –Be wary of free apps. Sometimes free apps are just a version of the app with some ads slapped on or certain key features locked behind a paid version. And while these are annoying, they're not terribly offensive or troublesome. The more concerning apps are the ones that have very minimal advertising (or none at all) while still providing a measure of usefulness. Very few developers maintain robust apps or programs without some way of supporting development. Ads and locked features are one way, but letting the app quietly collect data about you for the developer to sell is another way. Part of the agreement you agree to for many apps gives the developer free reign to collect all sorts of information about you: GPS data, phone call and text data, sites you browse, products you buy, other apps installed, your contact list, etc. If you're okay with that information being collected and sold, that's fine, but realize that information about you partners, business associates, and clients can be collected as well. Depending on how that information ultimately gets used might

Practice Related Security

Types of Security Breaches – There's more to hacking than someone sitting in a dark room furiously banging away on a keyboard as lines of random code cascade down their monitor until they mutter "I'm in." There's three types of hacks that you should be familiar with: "traditional" hacking, physical intrusion, and social engineering. Traditional hacking is basically using a software exploit to gain unauthorized access. This accounts for most of the really high-profile, wide ranging

attacks that make it into the news. Typically this is because a business is using outdated software, so I will take this moment to reiterate: keep your stuff updated! Very rarely is someone using an all new, never-before-seen exploit for the purpose of hacking as single entity. Such exploits are worth far more on the black market than the data that can be accessed from a single target, so being hacked by something that isn't widely known is very uncommon unless you're a supremely valuable target.

That's not to say individuals or specific companies can't be the targets of hacking; hackers will just use less sophisticated, but arguably more effective, means of hacking. These types of "hacks" involve physical acquisition and social engineering. Physical acquisition is just that: they'll steal your laptop or phone and use that as a way to access your data. It's about as low-tech as you can get, but it works. Especially phones and tablets, which are easy to misplace and easy to grab. Simply exercise a healthy amount of caution about how you handle your devices and make sure they're encrypted should the worst still occur. A special note should be made about disposing of old devices: even if you delete everything on a device or computers, chances are there is still data on it. Computers don't actually "erase" anything when you delete something; the computer simply marks that part of its hard drive as usable for something else. If something never actually gets used in that spot, the old data still sits there. So when you're trashing an old laptop or computer, do a Google search for "secure hard drive wipe". Depending on if you have an old-style HDD with spinning magnetic platters or a new SSD with a mass of memory, your practices will vary. The "clean" way is to use a software tool to re-write all the data on the hard drive many times over with alternating data. The "dirty", and arguably more effective (and fun!) way to dispose of a hard drive is to remove the drive from the device and to beat it with a hammer until it shatters. Power drills work too

(putting three holes into any hard drive will render it useless to all but the most devoted of hackers), but nothing renders data inaccessible and exorcises your frustrations with modern technology like getting medieval on an old laptop.

Finally, the most simple and effective hacking technique targets the weakest part of every piece of technology: the user. Known as "social engineering", this hack targets the users to give the hacker access or information. The problem with this technique is that it is so varied and difficult to monitor for. And while social engineering works on a very small and personal scale, it's also the most frightening. If you're on the receiving end of social engineering, it means you're being specifically targeted by someone who is very motivated. Social engineering will be customized to specifically target the weaknesses in your organization. Most anyone can spot a phishing email at glance: an email from someone you've never heard of, with spelling and grammar errors, and an offer that's either too-good-to-be-true or disproportionately alarming. Efforts to socially engineer you through email will (seemingly) come from someone you communicate with regularly, be completely innocuous in tone, and will ask you to do something relatively benign (proofread a document, check out a website, resend an attachment, etc.). And that's just emails. Other common social engineering tasks include impersonating IT support, stealing garbage, and leaving infected USB drives for people to pick up.

Adequately protecting from this kind of hack can be the most troublesome to prepare for since it will require both technological competence but also rigorous training and adherence to security practices. Which is to say, really tough when you're trying to do everything else an attorney does on a regular basis. So while you can practice cybersecurity for yourself and maintain it as a core principle of your practice, to really shore up your practice related security, you should definitely…

Rely on Experts – Realize that the most important thing about navigating the swift-moving world of technology is to back off when you're out of your league. I fancy myself a fairly tech-savvy dude, but the bleeding edge of technology is developing faster all the time and staying aware of everything is beyond any one person.

As Steve Jobs was fond of saying, here's One More Thing:

Backup your Data – Like Nike says, "Just Do It". Do it yourself, pay someone to do it, find willing relative that can help you out, watch some Youtube videos about it, etc. Back your stuff up. Hard drives will fail, apps will get compromised or shut down, ransomware will strike, power surges will turn high-priced electronics into high-priced paperweights, floods will whoosh a server right down the street, and so on. Nothing lasts forever, so keep a couple copies. And keep them updated. Once a month is great, but bi-annually isn't bad either. Do it as part of your Daylight Savings routine: change your clocks, replace your smoke/CO detector batteries, and backup your data.