HOWTO: Protect your small organization against electronic adversaries

Prof. Dan Wallach, CS Department, Rice University <dwallach@rice.edu>
Version 1.0.3, January 2018

Executive summary

If there's one thing we learned from the leaks of emails during recent political campaigns, it's this: *cyber-security matters*. These leaks influenced the process to the extent that any political campaign, any small non-profit, and any advocacy group has to now consider the possible impacts of cyber-attacks against their organizations. These could involve *espionage* (i.e., internal secrets being leaked) or *sabotage* (i.e., internal data being corrupted or destroyed). And your adversaries might be criminal hackers or foreign nation-state governments.

If you were a large multinational corporation, you'd have a dedicated team of security specialists to manage your organization. Unfortunately, you're not and you can't afford such a team. To help you, this document summarizes low-cost tactics you can take to reduce your vulnerabilities using simple techniques like two-factor authentication, so a stolen password isn't enough for an attacker to log into your account. This document also recommends particular software and hardware configurations that move your organization "into the cloud" where providers like Google or Microsoft have security professionals who do much of the hard work on your behalf.

New vocabulary? Want more details? There's a glossary in the back. Also, if you're looking at this document online, all the hyperlinks work. Click and enjoy. If you're looking at it offline, you can always find the latest version here: https://www.cs.rice.edu/~dwallach/howto-electronic-adversaries.pdf

Table of contents

1. Know your adversary

Generally speaking, there many sorts of adversaries that you need to defend yourself against:

1. Untargeted, remote (spammers, phishers, ransomware griefers, etc.)
2. Targeted, remote (spear phishers)
3. Targeted, in person (immigration agents, police, criminal trespass)

Everybody in the whole world has to deal with untargeted attacks. The former Nigerian prince who wants your bank account to help with transferring ill-gotten gains is spamming everybody and the defenses are pretty straightforward: learn to ignore them. Similarly, if you get a Facebook request from a friend of yours who you're *already Facebook friends with*, then it's entirely possible that somebody is trying to clone your friend so you should ignore the request and let your actual friend know. There are many variants on this attack. It's worth expressing a healthy skepticism about a fresh email from an "old friend" or a Facebook friend request when they arrive unexpectedly.

The recent attacks against prominent political figures appear to have been an example of #2 on this list. Notably, one such figure received a fake-but-convincing email telling him that his Gmail account had been compromised with a "click here" button to fix it. Here's a picture of it:

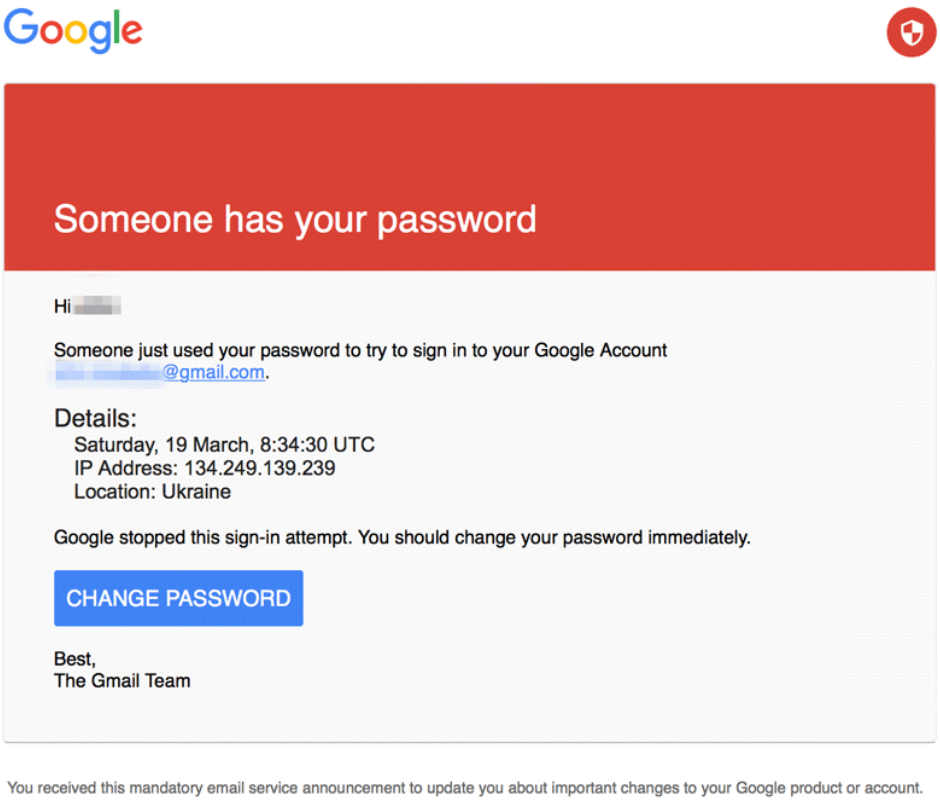

Figure 1: "Spear phishing" email from 2016.

There was nothing wrong with this user's Gmail account before he clicked the button, but afterward? Yeah, that was the problem. This is an example of a *spear phishing* attack, where the attacker was going after a very specific high value target. Such attacks can be quite pernicious and cleverly done (e.g., sending what looks to be W-2 tax forms from HR around the proper time of year, when users would be primed to expect such a communication).

This style of attack is unfortunately common, and every government has teams of experts who do these sorts of attacks. Readers may enjoy this video of the NSA's chief of "tailored access operations". His message was that we attack others, and they attack us.

In-person attacks are probably the most difficult to defend against, because the threat actor has unfettered access to your phone or computer, whether by breaking into your hotel room or in the person of an border agent demanding such access. We'll discuss a variety of countermeasures below, but the short answer is that these cases require anticipating the threat in advance. Information you don't have with you is information that cannot be stolen from you.

2. Know your tech

The single most important technical measures you can take are to use *up-to-date equipment* and *best-of-breed cloud services*. Whether you've got a Mac or a PC, you should be running the latest version

of OS X or Windows 10. If you've got an ancient machine that won't accept a modern update, it's time to retire it and get a new one. This also applies to the applications on your computer. If, for example, your Mac is running Office 2008 or Office 2011, then it's time to upgrade to Office 2016. Why the upgrades? Because Apple and Microsoft have really improved their game. If you run the newest software, you'll be protected against the most recently discovered vulnerabilities. This also applies to your smartphones. Many cheap Android devices are running ancient versions of the Android system.

A. **Should you get a Google-branded Android device like a Nexus or Pixel or are third-party Android devices acceptable?** Google pushes monthly security updates to its own phones. For third-party devices, some manufacturers are better than others at rolling out these updates, particularly for older devices. If you're genuinely concerned about targeted threats, then using a Google-branded phone is likely to be more secure. If you're using a third-party device, check what version of Android you're running. If it's anything older than Android 7.0, it's time for a new phone. Not sure? Go into your Settings and select "About phone". Below are images from a current Google Pixel XL. Notice how the "kernel version" and "security patch level" dates are regularly updated? If your phone shows older dates, you need to replace your phone.

   Google lists dates for "no guaranteed security updates after" on its Nexus/Pixel support page. So, as of January 2018, a Nexus 5X, Nexus 6P or Pixel phone will still get security updates, but a Nexus 5 or Nexus 6 is unsupported and should be replaced. For other Android vendors, you should identify a comparable support page.

B. **Is an iPhone better than Android for security?** Apple and Google have both worked hard to improve their security chops; newer iPhones are definitely better than older ones. When comparing the latest Apple iPhone 7 or 8 with the latest Google Pixel or Pixel 2, I'd say it's a wash. Get the one that you prefer. At that point, your security will depend more on the apps you choose than on the phone platform. As with Google, Apple obsoletes its products over time. iOS11 requires an iPhone 5S or newer. If you're running an iPhone 5, 5C, or older, you need to replace it.

C. **What about Chromebooks?** If your needs can be satisfied with Google Chromebooks, you should seriously consider them instead of Windows or Apple laptops. Not only are they cheaper, but they only run a web browser and nothing else, making them much harder to compromise. Newer Chromebooks with touch-screens now also run Android apps, making them much more useful. Chromebooks are automatically updated by Google with the latest security patches and they have features that make it very hard for a hacker to install malware. *And, of course, if they're stolen, there's nothing really there for an attacker to steal.* All of the data is safely in the cloud.

   Some Chromebooks are old enough that they are no longer supported by Google. You can see the whole list online; this particular link discusses fixes specific to the "Spectre" and "Meldown" issues, but it also tells you dates when "auto update ends". If you've got a Chromebook old enough to be listed as "EoL" (end of life), it's time to get a new one.

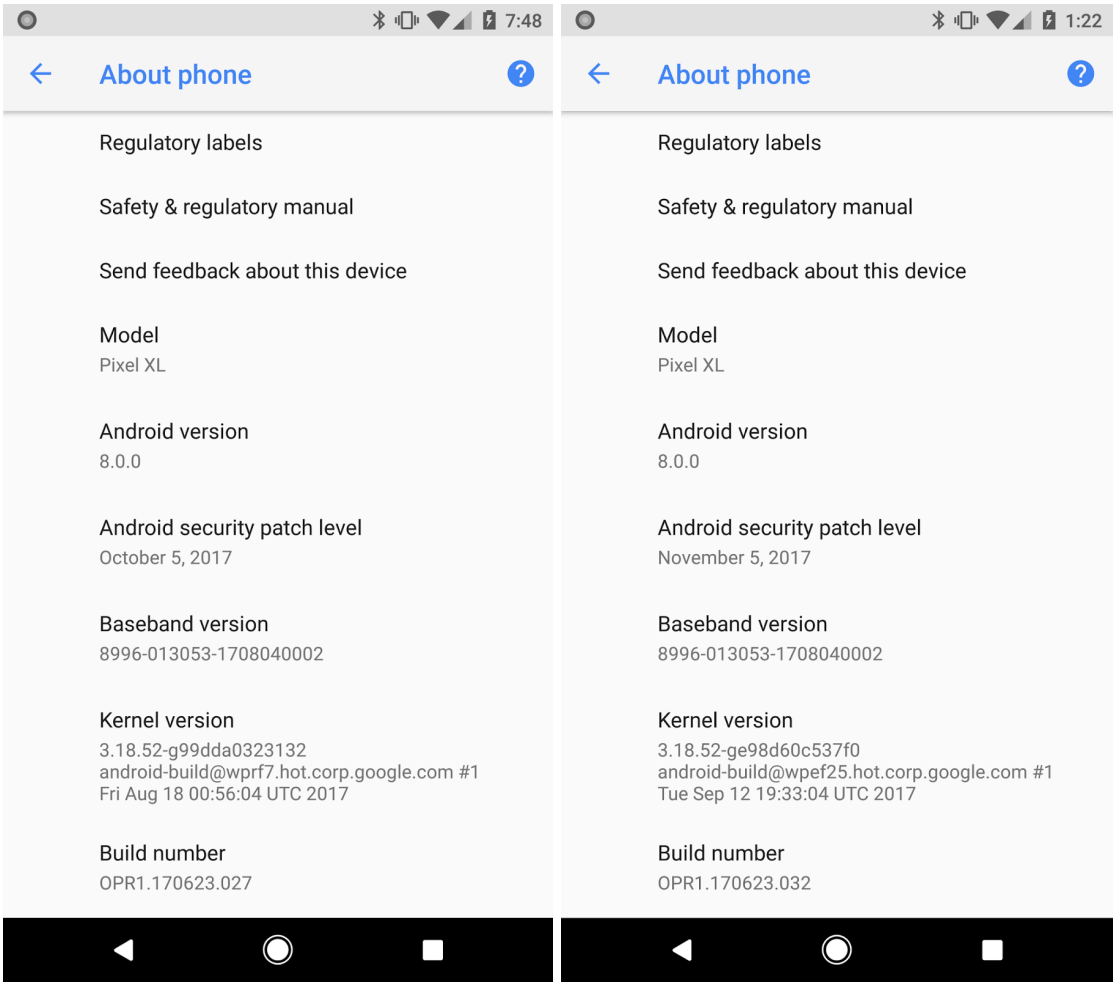

Figure 2: The Android "About phone" page from a Google Pixel XL in October and November 2017.

D. **Do I need third-party anti-virus software on my computer or phone?** Surprisingly, no. The most likely vector for which viruses might attack you is through email, and AV companies offer plugins for email servers. Cloud email providers like Gmail also have AV built-in. Windows 10 also comes with "Windows Defender" built-in, which is free and which serves the purpose. Conversely, there's increasing evidence that many third-party AV engines actually make your security worse. If your devices are running the latest software versions with the newest security patches, you'll protect yourself very well.

E. **What about the apps I install?** The fewer the better. When you install a popular app from a big company like Twitter, Facebook, etc., you can have some confidence that it's not out to get you. If you install games or whatnot, you have far less assurance. In some cases, even mobile web pages from sketchier parts of the web try to pretend that they're apps and will generate fake warnings that they've detected security vulnerabilities. (See Figure 3, below.) If you're installing an app which has a "free" and a "pay" version, where the latter has no advertisements, you significantly improve your security posture by paying the money. Ads are a vector for attacks into your phone.

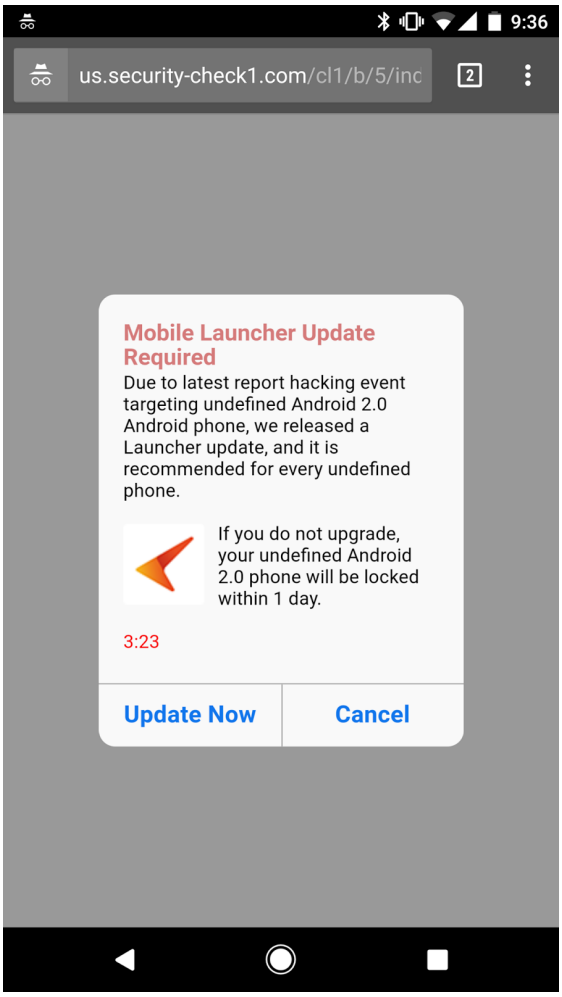

Figure 3: A typical mobile phishing attack.
Here, a web page attempts to imitate a native dialog.

F. **Can I protect myself by moving to the cloud?** Consider switching away from local infrastructure (e.g., Microsoft Office and local file servers) and using a managed cloud solution (e.g., Google Docs). One of the benefits of moving to cloud services is that the vendors who run them offer you a variety of security features that are hard to set up on your own. Google's Gmail, for example, has top-notch anti-virus, anti-spam, and anti-phishing defenses. Furthermore, if you go wholeheartedly to the cloud, then you can replace your computers with Chromebooks (see Question C, above).

While you could run a small organization on personal Gmail accounts, it's much better to pay for a "G-Suite" domain. At that point, you can have the familiar Gmail and Google Docs with your own custom domain-name. The security win is that you can centrally manage your users, making it easy to add and remove staff. As the administrator of a G-Suite domain, you can require all your users to use two-factor authentication (see below), making everybody more secure. Also, a

G-Suite administrator can limit which third-party apps your users can use, eliminating the attack shown in Figure 4. (We discuss alternatives to G-Suite later in this document.)

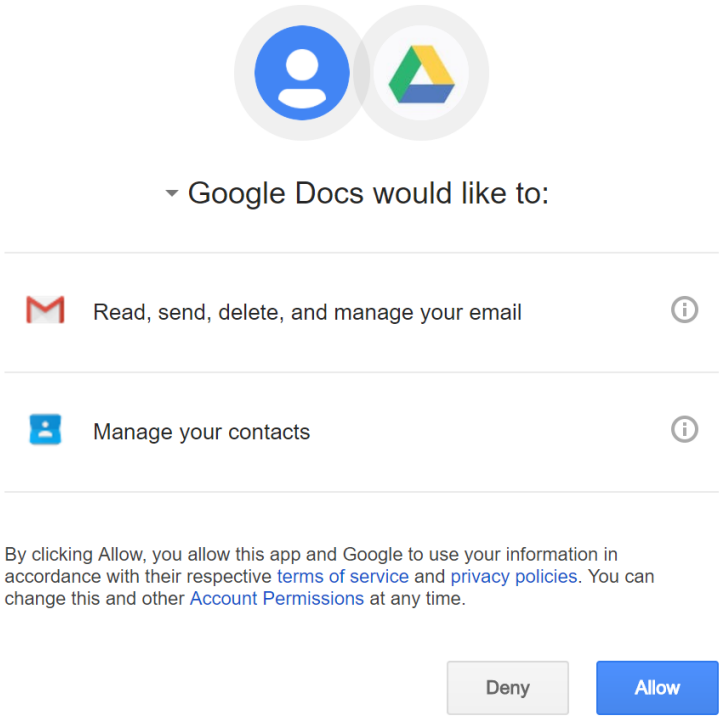

Figure 4: A "delegation" attack against Google Docs. If you click on the down-arrow next to "Google Docs", only then would you see that it names the attacker.

G. **What about my web browser?** Even if you completely "move to the cloud", your browser now becomes a battlefield, where one web page might try to attack another one. You protect yourself by running the latest browsers. Google's Chrome started the trend, and now any browser worth using automatically updates itself -- an important security defense. Also, a growing vector of security attacks come from Internet advertising. (Yeah, really.) As such, installing a good advertisement blocker like uBlock Origin not only makes the web a more quiet and pleasant place, but it also defends you against some ugly attacks. Chrome is probably the most security-focused web browser today, closely followed by Microsoft's Edge and the latest versions of Apple's Safari.

Of course, your users can still be attacked through the web. One recent email phishing attack made it look like Google was innocently asking you for permission for Google Docs to read your own documents. Figure 4 has a picture of the dialog box that users saw. Google has taken several steps to address this attack, including new features for G-Suite administrators to eliminate the problem entirely (see above).

H. **What about the cool new fingerprint readers?** Many smartphones now have fingerprint readers as do a few laptop computers like the newest MacBook Pro. The nice thing about a fingerprint reader is that somebody can't just shoulder-surf your PIN or password. That's a big win. The downside of a fingerprint reader is that you leave your fingerprints everywhere you go, *including on the fingerprint reader itself*; it's surprisingly easy for somebody to make a fake plastic finger that will fool your fingerprint reader. Note that most devices will require you to enter your PIN/password after they've been turned off or if you haven't unlocked your device in a while. **If you're going through a border crossing or something similar, just turn your phone off beforehand** and don't turn it on again until you're all the way through. Do also make sure that your PIN or password isn't visible from an on-screen smudge. You can then affirmatively deny somebody access to your device. Similarly, if you're leaving your phone in your room while heading out for a night on the town, turn it off before you leave.

I. **How about two-factor authentication (2FA)?** It's now considered an industry best practice to combine passwords ("something you know") with physical tokens ("something you have") and it's easy to do. Many web sites let you associate an app like Google's Authenticator with them as part of the login process. You have to enter your password, then you run the app and type in a 6-digit code. Google and others also support "Fido U2F" ("universal second factor") keyfobs. Just put it on your physical keychain and plug it into your computer when prompted. If you're using G-Suite, you can even make these things *mandatory* for all your users. Had the user who received the spear phishing email in Figure 1 been using 2FA like this, then divulging his password to his attackers would not have allowed them log into his account.

Figure 5: Fido U2F keyfobs from Yubikey (left) and Feitian (right). The Feitian keyfob supports computers with USB and also supports mobile phones with Bluetooth and NFC.

The way Fido U2F keys work, there's no way for an attacker to trick a user into divulging a PIN or password, so they're more resistant to phishing attacks than two-factor apps. Some web sites try to send you an SMS text as a form of 2FA, but this is now considered insecure and is not recommended for use. A single Fido U2F key in your pocket works safely with multiple web sites at the same time, including Google, Facebook, GitHub, Dropbox, and FastMail.

J. **What about Google's Advanced Protection?** In short, "advanced protection" requires you to do many of the things you might have done on your own, like setting up 2FA. More broadly, "advanced protection" removes anything from your account that you might be tricked into handing out, like password recovery questions, leaving only your "strong" login mechanisms like Fido U2F keyfobs. As part of the setup process, you should have one keyfob that you plan to keep with you, and another that that you place in your safety deposit box or equivalent; Google recommends you buy one Yubikey and one Feitian device as shown in Figure 5. "Advanced protection" also turns off some of Google's OAuth features (see Question F and Figure 4, both above), removing functionality that most users don't need in return for better security. More importantly, as the years go by and Google inevitably adds more features to its systems, an "advanced protection" account will have its security settings automatically adjusted by Google to favor your security.

When you have a G-Suite account, your G-Suite administrator has a variety of configuration options that are, in effect, the same as what "advanced protection" does for a regular consumer account. Since many people maintain a "professional" account as well as a "personal" account, it's sensible to protect your personal account with "advanced protection" and to protect your professional account with the equivalent features that G-Suite offers.

"Advanced protection" does come with some restrictions. For example, the only way to access your email and calendar is through Google apps, which support 2FA directly, versus the iOS mail and calendar apps, which don't support it.

K. **What about password managers (LastPass, etc.)?** Password sharing across sites is a big problem. If one web site gets hacked, then your "leaked" password lets somebody log into every one of your accounts. Password managers act as browser plugins and will generate strong, random passwords, separately for each and every account. Of course, as with anti-virus systems (discussed above), these password managers themselves might come under attack. As such, it's hard to offer good advice here. One approach, which only makes sense if you're doing 2FA with Google, is to have your users maintain Google Docs with usernames and passwords that they use for your various web services. For example, your social media manager may maintain a Google Doc with Twitter, Facebook, and other usernames/passwords. You can then use seriously complicated passwords (mash your fingers, type way more than 8 characters!). You should also enable 2FA on your social media accounts.

While this advice is not a great general-purpose solution, for a small organization where one person might need to jump in and do another's job on short notice, it's not a bad way to go. Under normal circumstances, Chrome will remember these passwords, giving you many of the benefits of a dedicated password manager.

(Better websites won't require you to have a separate password with them but will instead let you "Login with Google" or "Login with Facebook". This sort of thing, sometimes called "federated login", is a great technology but is rolling out far too slowly.)

L. **What about web servers and other public-facing infrastructure?** Just like you should be using up-to-date software on your personal computers, you need to do the same thing with your web infrastructure. If you're a small organization without a full-time administrator for your systems, then you should be using a cloud provider that does the security for you like Weebly or Wix. Let's say you've got a "donate now!" button on your web site. You want to protect your donors' credit cards from theft as well as protecting the privacy of your donor list. You should certainly use a third-party payment processor (e.g., PayPal) such that you're never directly handling credit cards. For the rest, there's a giant industry of companies that offer services to help you. To the extent possible, you want to avoid having custom infrastructure that you need to manage, and you want to evaluate your cloud providers on the basis of the strength of their security team and on how little you need to customize. If somebody provides a template where you only need to add text and images, and they do all the rest, that's potentially a big win.

M. **Domain names.** One thing you may not know is that you can connect one domain-name to multiple services. So you can easily have email to YourCampaign.org hosted by Google's G-Suite while the web-site for YourCampaign.org is hosted by Weebly or Wix. The company from which you bought your domain-name can set these up separately for you. It's also worth noting that your domain-name, itself, is something that an attacker might try to steal from you. When you hear about Anonymous or some other hacker group "hijacking" a web site, that's sometimes what they're doing; if it happens to you, your entire organization is dead in the water.

   Even if you've already bought your domain-name from one DNS (domain name system) registrar, it's straightforward to transfer it to another. Who's the best game in town? One large vendor that takes DNS security seriously is Cloudflare. They also offer sophisticated services to keep your web site available even if it's under sustained "denial of service" attacks from the darkest corners of the Internet. Their "pro" service is $20/month and is something you layer in front of an existing web provider like Weebly or Wix.

   Maybe you conclude that Cloudflare is overkill for your needs, but you still want to make it hard for somebody to hijack your DNS records. Google Domains is $12/year, and it's got all the same security features to make it hard for an attacker to log into your account (e.g., Google's "advanced protection" if it's enabled on that account; see Question J, above).

   For what it's worth, the process of transferring a domain name can be a bit daunting (see, for example, the instructions for moving a domain name to Google Domains), but the good news is that you do this once and you've protected yourself from some serious downside risk. There is a ton of technical jargon in the world of DNS, so you should make sure you've got somebody in the know to help set this up and get it right for you.

N. **What about the infrastructure that supports our office (routers, printers, and other such devices)?** As with everything else, you want devices where security is part of the package. Just as it's important for your phone to have the latest security updates, the same applies for your routers,

printers, WiFi access points, and other devices. If you run a small shop with consumer-grade Internet service, one attractive solution is Google's new Google WiFi. You can combine that with "dumb" switches (see, e.g., this Netgear ProSafe switch) and wire up your office for very little money. Google has invested a remarkable amount of engineering effort to make sure that their devices are secure, and they automatically update themselves with security patches when necessary. Most other home networking gear does not auto-update.

If you're running a bigger organization, then you're going to need a commercial provider who can set up and manage your infrastructure for you. Increasingly, these sorts of services are also available from cloud providers and some ISPs. You want to interview them based not only on price, but on their ability to detect when a device on your network behaves strangely and what they'll be able to do about it. (The technical terms are "intrusion detection" and "intrusion prevention".)

Printers are a bit messy, with recent work showing a variety of problems. Needless to say, you don't want your adversary being able to see copies of everything you print. In short, if you've got personal printers, connected via USB directly to your computer, then you don't have to worry about them being hacked over the Internet. If you've got Ethernet or WiFi-connected workgroup printers on your network, and you've got a small organization, then you're also in pretty good shape. If you're running a bigger organization, then it gets trickier. You want to limit the number of devices that can see your printers, which probably means shunting smartphones onto a separate "guest WiFi" which cannot see your printers, while your normal laptops' WiFi can see them. (Google WiFi can support this sort of configuration without requiring you to spend any extra money.)

Also worth mentioning are webcams and other "Internet of things" devices. You may be tempted to set up cheap webcams, to monitor the physical security of your premises, with convenient cloud-based recording, so you can review the footage later if need be. Cheap no-name webcams turn out to be a giant security nightmare; 1.5 million of them were recently hijacked into a giant coordinated web attack machine. The best practice is to go with a name-brand webcam (e.g., NestCam) where you might hope that the parent company (Google, in this case) is paying attention to the underlying security of the device. In larger networks, you might also segment your network such that your security cameras can't see your computers (and vice versa).

O. **Wow, all this setup stuff sounds hard**. If you can't afford to have the in-house expertise, there are plenty of security and IT consultants out there who you can retain to help you set everything up. Interviewing your security consultant is a difficult endeavor. You're obviously looking for somebody with a lot of experience, but you're also looking for somebody who has a lot of connections, so they can refer you to other more specialized experts once they realize they're in over their head. If you're running a small shop on a tight budget, then you want to have as little gear in-house as possible, outsourcing to good cloud providers.

P. **I just heard about a really nasty vulnerability…** In mid-October, we learned about a vulnerability in WPA2 (the cryptographic protocol used to secure a WiFi connection) and another vulnerability that impacts certain cryptographic 2FA tokens. Similarly, in January we learned about a pair of attacks ("Spectre" and "Meltdown") which rely on some unusual security issues in Intel and other CPUs. Significant attacks like these don't occur every day, but they're a regular feature of the computer security landscape.

These security issues and others are why it's so important that all your devices are getting current security patches (see Questions A and N, above). Luckily, it turns out that the "U2F" functionality you would be using with a Yubikey or Feitian device isn't impacted by this specific vulnerability, but if it were, your cloud provider would almost certainly be issuing warnings to help you upgrade. Similarly, all of the major OS vendors (Microsoft, Apple, Linux, Google's Android, etc.) have released security patches to address Spectre and Meltdown. And if you're running a device too old to get security patches, it's time to get a new device.

3. How to communicate online and elsewhere

A. **Basic organizational functions**. Earlier in this document, we talked about G-Suite, Google's version of Gmail, Docs, and so forth that's meant for enterprise usage. There are a variety of other enterprise offerings, like Slack for group texting, or Expensify for expense reporting. As you evaluate these providers and their competitors, make sure you understand more than their dense legally worded security and privacy policies. Interview them about their security practices. Look for their ability to support two-factor authentication or, even better, to connect to authentication services provided by somebody else. Think: "Login with Google". Every time you can get such a "federated login" or "single sign-on" feature, it's one less place where you need to add and remove an account every time somebody joins or departs your organization.

This also means that you want to discourage your users from communicating with personal email addresses, text from their phones, etc. The extent to which you can manage and control your users' communications is directly related to the extent to which you can protect them from being leaked or tampered. Consider what might happen if you need to fire an employee / staffer / volunteer. You want to be able to pull the plug on them, all at once, killing off their access to email, cloud documents, everything. You can't do that if you're using personal Gmail, but you can if you're using G-Suite.

That said, if your organization is less organized, say it's nothing more than a group of people planning and organizing political protests, then none of this advice is particularly helpful. At that point, the best you're going to do are "secret groups" on Facebook (i.e., invitation-only groups that are not publicly visible). You can also set up a free account on Slack, but you don't get some of the cooler features, e.g., Slack only lets you require 2FA on a paid account. You can at least set up 2FA on a personal Gmail account, preferably using the U2F tokens discussed above.

B. **Am I safe using a public WiFi in a coffee shop or airport?** The short answer is that you're safer now than you were in years past. Most web sites you might use these days are encrypted; look for the "https" in their URL. Similarly, most apps on your phone will encrypt your data before connecting to their cloud servers. If you're using a Chromebook or a recent smartphone, as discussed above, then you're unlikely to be successfully attacked. If you're using an older Windows laptop or an older Mac without the latest security patches, then a public WiFi service might have unacceptable risks for you.

C. **Are there risks from social networks like Facebook?** The biggest risk is to your privacy. *Assume everything you say or do will be visible to the public*. It's just too easy to post something that you mean to be private and accidentally have it be visible to the whole world. "Private groups" on Facebook are somewhat better, but any group with thousands of members might well have somebody you don't trust, just waiting for you to say something inappropriate and make a copy of it for later use.

   Related: be cautions of all these online surveys and quizzes. *Find out which Game of Thrones character you would be!* Please don't do these. You're telling marketers about yourself so they can target you with advertisements.

4. Legally authorized attacks

If you think your organization is going to run afoul of law enforcement, or if you're concerned that your government (or, really, *anybody else's government*) might find a way to legally compel companies like Google and Facebook to divulge things that you wrote with an expectation of confidentiality, then you need a completely different set of tools to protect yourself. If you're doing corporate G-Suite or Slack or whatever, and the police show up at those organizations with a court order, they *may* fight the court order, and you *might or might not* have a chance to defend yourself. If your cloud provider acquiesces to such an order, then all the two-factor authentication tools and other good practices that you've conducted will be meaningless. Of course, this isn't supposed to happen here in the U.S. unless you're being accused of a serious crime, but you should have some understanding of how to defend yourself.

First, if you're still using Yahoo, AOL, or any other legacy web-mail providers, now's the time to move to an organization that takes security more seriously. Google has consistently put its users first, even explicitly warning users when they detected what they believe to be nation-state adversaries attempting to compromise their accounts. (Microsoft, Twitter, and Facebook also issue warnings like these.)

But even Google has limits. The next step? **Signal** provides an app for iOS and Android which supports sophisticated "end to end" cryptography for texting, voice calls, and video calls, such that even if somebody served Signal with a court order demanding they release everything, they'd have nothing to release. The company behind Signal literally has no idea what you're writing to each other. Signal supports group text chat and voice calls. Make sure you and your cohort are careful to set it up properly. Practice with it in person before expecting it to work remotely.

If and when you don't even trust your Internet Service Provider (not as much an issue in the U.S., but definitely an issue in many foreign countries where you're buying your net connection from a state-owned company), then it's time to understand how to use Tor, which hides your traffic from anybody who's watching.

But wait, you ask, how do I know whether my cloud provider (Google or otherwise) has been compelled to operate against my interests? Suffice to say that it's hard to really know. So long as we're talking about U.S.-based organizations being attacked by foreign nation-state adversaries, then "legal attacks" are largely not an issue. But once your own state becomes hostile to your interests, or if you're traveling abroad, then your threat profile also changes. To pick an example from 2009, consider the case of a cellular phone carrier in the United Arab Emirates; Etisalat tried to install malware on any Blackberry connected to its network. It's at best unclear how well modern smartphones can resist comparable attacks.

5. If it really matters, don't do it on the computer (i.e., old-school operational security)

Long before people had computers, they still communicated: on paper and in person. Consider this to be a very sketchy guide.

- Doing the exact opposite of the previous advice here, you could have a computer that's never, ever, connected to a network. Write to your heart's content, then print your documents with an old-school printer for sharing. Maintaining a computer that's entirely offline can be a huge pain. How can you safely get data in or out? Not with a USB stick, since the stick might also be a vector for somebody attacking your computer! You could burn CD-ROMs and use those to courier data, but CD burners are largely going out of fashion and were never particularly reliable. Yeah, this is tricky stuff.
- Spies have long uses a variety of sneaky techniques like dead drops: leaving hidden messages such that the two parties are never seen in the same place at the same time. This is valuable if you want to have a conversation with somebody without observers even being able to know that you're talking at all. Needless to say, this is difficult to sustain, but if it's necessary, old-school dead drops might be the way to go.

6. And some seemingly basic operational security advice

There are many simple things that people do wrong. You can up your game.

- If you find a USB stick sitting around, perhaps in a parking lot, or maybe somebody you don't know gives one to you at a tradeshow, *don't put it in your computer*. This also goes for USB-powered devices (e.g., desk fans or vaping pens). If you need power for something with a USB plug, use a dedicated charger rather than the external ports on your computer. A wide variety of chargers are available. (See, e.g., this 6-port charger from AmazonBasics.)

- Charge your phone with your charger, not by plugging it into your computer. Keeping your phone and your computer physically separate helps prevent an attack on one side from spreading to the other.
- If you're near a computer or phone, *assume the microphone and camera are on*. For very sensitive conversations, you can have a meeting in the middle of a field while eating a nice picnic lunch, leaving your electronics in the car; it's much harder for somebody to eavesdrop on you from a distance.
- Pay attention to your surroundings. Don't have a sensitive conversation while on the subway, in a taxi, or on a crowded elevator. Similarly, be cognizant of shoulder surfers who might wish to read your computer screen from next to you on an airplane. If you must use your computer in public, get a 3M privacy screen for it; also available for phones.
- Make sure your computers and phones are doing backups. Android phones can do this to your Google account. iPhones can do backups to iCloud. For laptops, you can purchase backup services from many companies including BackBlaze or CrashPlan. Backups protect you against equipment failure as well as nasty "ransomware" attacks that try to encrypt your files and then blackmail you into paying a ransom to get your files back.

7. Aren't you being a bit biased in favor of Google here?

A common concern, when recommending Google products, is a pushback that Google is watching everything you do, selling it to third-parties, etc. Google does indeed take its users' privacy seriously. It's also important to note that Google has invested a huge amount of effort into securing its devices and services. Google has similarly invested effort in finding bugs in other products like Microsoft Windows and has gone to great lengths to improve security for open source software. Google was very early to support 2FA and offers it for free to any user. Perhaps most notably, Google detects and warns its users when it detects nation-state attacks. If you work for a large corporation with a top-notch IT department, they will do all these same things, hopefully as well, but if you're a small non-profit or community organization, Google is the only way you can reasonably afford this level of sophistication.

Yeah, but if you're not the customer, then you're the product. So be a customer! Google's G-Suite is $5/user/month, with all the same tools you know (Docs, Sheets, Gmail, etc.) and further features to help manage your users (e.g., 24/7 customer support). If you're running a political campaign, that's chump change compared to what you spend on everything else, and you're getting some of the best security people in the world working on your behalf.

The closest comparable service is Microsoft Office 365 Business Premium, which costs $12.50/user/month. Other vendors like Zoho also compete in this space, and maybe they're the right move for some organizations. But if you need best-of-breed cloud-service security for the cheapest possible price, Google seems to be the way to go.

8. Additional reading

EFF has a detailed series of tips, tools, and how-to's for security. Let's say you're running a small NGO and you or some of your staff are planning to attend a protest. Make sure you read EFF's advice before you go. See also, the Chayn DIY Online Safety Guide.

9. Checklist

Since there are so many things here, it's helpful to provide a concise checklist.

- ❏ Update your users' phones to something manufacturered in the past year. Apple's iPhones and Google's Pixel phones are recommended because they get frequent security updates. Consider keeping "work" and "personal" equipment separate.

- ❏ Most of your users only need cheap Chromebooks rather than expensive laptops. Among other benefits, a stolen Chromebook means you worry less about data from your organization leaking.

- ❏ For your users who operate in the field, make sure they've got 3M privacy shields on their laptops.

- ❏ Set up centralized email for your organization, via Google's G-Suite or other comparable service, rather than using a mix of personal email services.

- ❏ With G-Suite or equivalent, set up mandatory two-factor authentication and buy your users Fido U2F keyfobs. This helps you protect your users from a variety of attacks. Along these same lines, encourage your users to set up Google's "advanced protection" on their personal accounts.

- ❏ For social media accounts, maintain a shared document (e.g., via Google Docs) where you can have very strong passwords safely written down. Also, enable 2FA on those social media accounts, if possible.

- ❏ For public-facing web sites you might create, make sure your DNS registrar takes security seriously (Google and Cloudflare are easy recommendations; you may need an expert to help set you up).

- ❏ Train your users. Sure, they have limited time and attention, but a little bit can go a long way. A weekly rotating reminder, on the wall in a break room, might be a good start.

10. Glossary

Anti-virus (AV): Tools that seek to limit the damage that malware can cause to your computer. AV typically is one of the functions performed by email servers and the use of third-party AV software is not typically recommended any more for desktop computers or smartphones.

Authentication: The process wherein you convince a computer, or another person, of your proper identity. In the physical world, this often involves identity cards. In the online world, it can involve a number of means, ranging from usernames and passwords to biometrics or other devices. The absence of good authentication, particularly in the world of email, makes it easy for someone to be impersonated, often as part of a phishing or spear phishing attack.

Biometrics: While traditional computer authentication is conducted with usernames and passwords, in the physical world we recognize each other by how we look and how we sound. The human visual system is particularly good at facial recognition. For our computers, fingerprint readers are growing in popularity, either as an alternative to passwords or as a "second factor" to add beyond just passwords alone. Particularly for a smartphone, a fingerprint reader offers resistance to shoulder surfing.

Domain Name System (DNS): This is a global database that takes a domain name like Google.com and points your browser or email program to the right computer server, wherever it might be. There are a ton of other terms that go along with DNS that are beyond the scope of this document, along with several entire online glossaries dedicated to DNS (see, e.g., Digital Ocean's introduction to DNS).

Espionage: One of the two broad classes of attacks that any organization might face, espionage refers to attempts by an attacker to exfiltrate or steal sensitive data. This could be email or any other sort of document. Espionage attacks, by their nature, try to remain hidden as long as possible.

Malware: A broad term encompassing viruses, worms, and any form of software that intends to do harm to you and/or your computer. Generally speaking, malware can be broken down by *how it gets in* and then *what it does once it's in*. Malware often takes advantage of weaknesses in the software on your platform. For example, Adobe's Acrobat PDF viewing software has had a long history of vulnerabilities, versus the typical assumption that PDF is "safe" to view at any time. As to what malware does, there are two broad categories: espionage (i.e., stealing information), sabotage (i.e., damaging systems).

Phishing: An email attack designed to confuse the recipient into doing something they shouldn't do, like reveal a password. Phishing could also be a vector to introduce malware for various purposes.

Ransomware: A recent trend for attackers who manage to get malware into your computer is to encrypt your hard drive, then display a message saying, "pay up or never see the contents of your hard drive again." The early attackers who did this were sloppy, allowing for workarounds to recover your data. More recently, they seem to have improved their tooling--bad news for you if you're a victim. This is yet another reason why it's essential to run up-to-date software (and thus have fewer vulnerabilities for

attackers to exploit) and to have a good backup strategy (and thus be able to recover your data from backups after an attack).

Sabotage: One of the two broad classes of attacks that any organization might face, sabotage refers to attempts by an attacker to damage an organization's data or systems. This could include overwriting and deleting data. It could also refer to physical infrastructure being damaged or destroyed. One example of a sabotage attack is "ransomware", where an attacker manages to encrypt your files and requires you to pay them in order to get the decryption key.

Shoulder surfing: Literally, somebody looking over your shoulder as a way to either observe you typing your password, or simply read a sensitive document off your screen.

Social engineering: Phishing and spear phishing are a specific example of a general purpose mode of attack, wherein the attacker pretends to be something he or she isn't. This can occur over the phone, in person, or electronically. As an example, hospitals have strict privacy rules for revealing information about a patient, but somebody who knows the lingo (i.e., a trained nurse or doctor), can almost certainly learn things over the phone that would violate the rules. As with phishing attacks, a social engineering attack may have a variety of goals, whether learning secrets or installing malware.

Spear phishing: A phishing attack, but targeted at a specific individual. What's the difference between phishing and spear phishing? The former targets everybody. "Hey, your account got locked! Click here." The latter takes advantage of things that a specific individual might know or believe. As an example, an "email prankster" created fake accounts with names like "Jared Kushner" and "Reince Preibus" and used those to email real White House advisors. If it's this easy for a prankster, imagine what a skilled professional can accomplish.

Two-factor authentication (2FA): Traditional usernames and passwords have proven too easily hacked. Users tend to pick their passwords poorly and reuse them across many different web sites. By adding something electronic (maybe an app on a phone or an electronic "key fob" that goes on your keychain), you can have potentially much better security (e.g., the equivalent of a different password for each web site, all hard to guess) with good ease of use. Alternately, you can add biometrics. The current consensus it that it's better to use a combination of passwords, biometrics, and/or key fob devices.

Two step verification (2SV): Often used synonymously with 2FA. The first step is your password. The second step is a key fob or otherwise.