Conclusion

Where Do We Go from Here?

Our professional intersection with—and investment in—the material we try to condense and describe in this book goes much deeper than our somewhat removed role as authors. We do hope that here we've been able to offer an easily digestible, essentially linear (entertaining?) framework for both understanding and, even more important, contending with emergent and constantly evolving threats to end users' data security. Broad consumption of even some of the cautions we offer, by sophisticated non-techies trying to function in an environment where the rules of play—and even the game itself—are constantly in flux, has potential to stem some of the truly mind-boggling data and security losses we've all read about and unfortunately even experienced first-hand.

We have a deep professional interest in the emerging questions concerning end user data security. There will always be work…. But like everyone else we are experiencing this "information age" explosion of possibility and vulnerability as spectators in what likely will be viewed by historians as the greatest single moment of evolution in our collective identity as a species. The Borg… perhaps not. But the emergence of virtual community that we're seeing today is simply 21st-century in its proportions—with all that comes along with that period designation. The good and the bad are unfolding simultaneously as we experience what it means to navigate in the virtual world.

As a broad, macro-level societal pattern, what we're seeing not surprisingly is that the vast majority of people just want to be a part of, and enjoy the benefits of, the connectivity that we have come to rely on in so many ways. Open the gates; open the gates! But within this mix, inevitably—with us since the serpent and the apple—is the need for caution and suspicion. There is just no way around the fact that with all of our virtual interactions on the Internet today there is an ever-present danger that requires a thoughtful approach and measured, careful handling.

Intelligent, sophisticated users can contend with these dangers. It starts with watching out for your data—be suspicious. As a basic point of departure, use common sense. Check your credit card and bank statements regularly for any irregularities. Some people do this as a matter of course; others don't. But unless you're regularly checking, small or seemingly inconsequential variations can easily go unnoticed, leading to bigger problems down the line. Report any abuses of your accounts or any suspicious or unauthorized charges that show up. These could be a signal that your accounts have been compromised by digital thieves who've accessed your personal data. Engage the system. Allow the entities you put your financial trust in to intercede at the institutional level on your behalf.

But, you're not on the boat alone. Today, more than ever, these large financial institutions are alert to their own vulnerabilities to virtual attack and exploitation. Size is apparently not a road block to modern virtual thieves, who may be even more likely to see larger banks as an attractive target. For example, on August 28, 2014, Charlie Osborne, writing for *Zero Day*, reported that the FBI was investigating a Russian hack of at least five American banks, including JPMorgan Chase.[1] The banks will, we hope, inform any of their customers made vulnerable through this latest security breach, and perhaps offer them formal guidelines or suggestions for remediating any damage to their personal accounts or online identity. It is critical that private end users affected by these attacks follow the official communications sent by their bank to limit the scope of the damage.

Don't Make It Easy for the Bad Guys

Sometimes, it's up to you to determine whether something is wrong. If you experience any strange behavior or functional slowdowns on your home wireless network, it's time to reboot the system, change your password, or call for help. For most readers, none of these steps is going to be entirely second nature. These maintenance activities are just not part of most people's everyday routine-even sophisticated users—and so likely carry with them some element of uncertainty or trepidation. You are not alone. It can sometimes feel like it in the middle of the night when your Internet stops working or your mobile devices fritz, but there are lines of support you can tap into. The IT staff at your office, online Help resources, even work colleagues who've gone through similar kinds of experiences can help you with these basic maintenance steps.

[1] ZD Net, Charlie Osborne, "FBI Investigates Hack of JPMorgan, Other US Banks," www.zdnet.com/fbi-investigates-hack-of-jpmorgan-other-us-banks-7000033080/, August 28, 2014.

Don’t make it easy for criminals to get access to your data. As we highlight at the beginning of the book, any kinds of clues or hints as to what your password might be are just what thieves are looking for. Don’t write down your passwords in an obvious location—this just invites security failure and loss of control over your property. Another convention worth adopting to help improve the security of your devices on the margins is to avoid spelling your passwords out loud as you enter them! Obvious? Not necessarily, particularly if you have a complex password that requires some concentration to enter. In this digital world, the importance of maintaining physical security just cannot be over emphasized. You never know who might be listening when you’re sounding out “*IspentmyvacationinSt.Louis*”!

Toward this end, it is good practice, sane practice, to change your passwords often. Consistent with one of the major themes running through the book, the more often you can change your password, the less vulnerable your data are likely to be, but doing so comes at the price of convenience, as you take the time to actually do it. Yin and yang, pro and con, security and convenience—there is always a balancing act that has to be in focus as the virtual threats we face evolve and become more difficult to address in static ways. Similarly, it is important to use different passwords for different services and also for different devices.

Be Suspicious, and Trust Your Instincts

We all live in the real world, with real risks—but also with real time constraint trade-offs and mental load trade-offs. There are only so many passwords that you can keep straight conveniently, and there are only so many that you can keep up with if you’re constantly changing them. This approach has got to become second nature so it consumes less energy and represents a more manageable cognitive load. Once it becomes habit, and some kind of predictable cadence emerges, it becomes easier to adopt a more stringent approach to password security.

With this resource issue in focus, it may be useful to think in terms of levels of security. You might maintain a few “high-level,” very strong passwords for your most critical services, but you don’t necessarily need to retain this kind of stringent gate for less critical accounts. You can probably get away with using “lower level,” less-stringent passwords for what might be thought about as “throwaway” accounts or less important services. This might include a shopping account for a random Internet merchant that you plan to use only once, for example. It just isn’t as critical that you protect this kind of transient connection with a complex key, because if it is compromised nothing of value to you is likely to be lost.

The threats to the security of your data are emerging more and more through various online channels. As we discussed in depth in Chapter 1, it is increasingly important to always verify the authenticity of an e-mail, text message, or web site before providing your password or any other personal data that could be stolen, sold, or used by a pirate looking to get rich. Keep a close watch on all of your devices. Be wary when something feels out of sync or a program or application seems to be functioning differently than it has in the past.[2]

Be cognizant that there really are bad actors out there looking for targets. Things like fake antivirus messages suddenly popping up and asking for money to fix a nonexistent problem should always feel sketchy. Strange software on your computer that you don't recognize, new toolbars in your browser that you didn't mean to install, anything that feels at all out of the ordinary to you should never be taken for granted or ignored. Don't assume that you're just imagining things or misremembering what you installed on your machine.

We are creatures of habit. We pay attention to patterns—our brains function by connecting the dots—and as a consequence we tend to notice when something in our immediate environment changes, feels different or off, or just doesn't smell right. Don't disregard your instincts. Trust them. Here, it is much better to be too suspicious than too forgiving. The potential personal, financial, social, and professional consequences for any kind of nonchalance are just too high. Let hyper-alert become the new normal.

The likelihood is that if it feels like something is wrong, then there is probably something wrong. Don't just close annoying pop ups, which are only going to return again and again. Either investigate the source of the problem yourself, or get someone to help you do so. Or if you can't, then report what's going on directly to the IT department (at work) or qualified repair professional (for personally owned devices) at a convenient big box store like Best Buy or H.H. Gregg. The Geek Squad is there to help you figure out some of the security issues you may not have the experience to handle yourself.

Keep the Home Front Safe

These aren't just work-related threats. Although your home may be your castle, it is not a fortress. People you don't know that well come in and out of it, and you're not always watching them closely while they're there. If someone has been in your home (e.g., baby-sitter, landlord, contract professional) and your computer or other devices seem to be acting differently, check them out. Don't convince yourself you're imagining things when you may not be.

[2] Techworld, Roger A. Grimes, "11 Sure Signs You've Been Hacked," `http://news.techworld.com/security/3500234/11-sure-signs-youve-been-hacked`, February 3, 2014.

Although it can be psychologically difficult to frame security issues in this way, sometimes it is important to take proactive steps to protect yourself and your valuable personal data against intrusions from someone whom you've trusted—but maybe shouldn't have.

The virtual and the physical dimensions of the security questions we examine are beginning to overlap in strange and unpredictable ways. In our discussion of physical security threats, we reflected on the emergence of apps that can allow criminals to get the key to your home printed at a hardware store by simply taking a picture of it. In August 2014, two researchers took this approach somewhat further. They demonstrated proof-of-concept through which they were able to create a "bump" key (a type of master or skeleton key) merely by obtaining a photo of the keyhole![3] These universal bump keys can potentially be printed by even a poorly funded, small-time thief at home, thanks to the prevalence and falling cost of "3-D printers," which facilitate the production of physical objects from digital blueprints.

We truly are living in a brave new world where technology is in many ways surpassing our current understanding of conventionally recognized boundaries associated with identity, property, security, and community. When someone can walk up to our front doors, take a picture of the lock, and half an hour later let himself in with a key he printed in the basement, what is clear is that rules of engagement have changed in fundamental—even unrecognizable—ways.

We have tried to stay away from conventional analogies to physical homes and neighborhoods in our treatment of the security issues and the virtual setting that defines the boundaries of the questions we address. However, when these worlds intersect in such an unconventional, and so 21st-century, way, it is hard to avoid drawing attention to the convergence of the old and the new worlds in which we're living and trying to operate safely, effectively, and productively.

Don't leave your machines (or your front doors!) unprotected. Take advantage of new data protection services offered by your employer, your telecom provider, or your e-mail or cloud storage company. If your employer offers antivirus, encryption, or other security software for use on personally owned devices, make use of these measures. They are often provided to employees free of charge and can ultimately save users a lot of time, money, effort, and other resources otherwise spent on retrieving data, dealing with identity theft and outright financial losses, and generally trying to get themselves back to par after a loss.

[3] *Wired*, Andy Greenberg, " These 3-D Printed Skeleton Keys Can Pick High-Security Locks in Seconds," www.wired.com/2014/08/3d-printed-bump-keys/?mbid=social_fb, August 26, 2014.

Watch for New Technologies

Become a more informed consumer as it relates to the digital devices you use and the virtual services you consume. Watch for announcements from telecoms and cloud or e-mail providers about new services that they're offering. Often, they're optional when they first come out. But take advantage of the opt-in as soon as it becomes available so you can preempt the vulnerabilities these new services are designed to address.

For example, Yahoo! will offer end-to-end encryption to their e-mail users by 2015.[4] This service will provide a significantly heightened level of security because data in transit are no longer "visible" to criminals in readable form. If you're a Yahoo! Mail user, opt in when you have the choice, because the sooner your data are protected, the fewer opportunities thieves will have to get their hands on your e-mail.

Another example is the cloud storage provider Dropbox, which made some changes to its service offerings in late summer of 2014. Most of the media attention these developments drew focused on Dropbox's lowering of its per-gigabyte price to compete with Microsoft and Google. However, Dropbox also made some important security enhancements to its Dropbox Pro service. These included the ability for end users to share files and folders with someone on a time-limited basis, setting access to expire after a certain point. Dropbox also added the ability to remotely wipe files from a lost or stolen device.[5]

Some of these more muscular services, while enhancing security, inevitably require you to think again in terms both of security and convenience. For example, as we discuss early on, Google currently offers an optional two-factor authentication for its Gmail service. Although this may seem like a hassle—particularly if you check your e-mail as frequently during the day (and night!) as most users with smartphones typically do—consider opting in and adopting two-factor authentication, particularly if Gmail is your primary e-mail provider. It could save you unnecessary heartache and pain.

The advances in security you can take advantage of today aren't limited to software and cloud services. Watch for other new features from hardware manufacturers, telecoms, or third parties that can also allow you to better protect your devices and data: new biometrics, new password managers, new ways to

[4] *PCWorld*, Ian Paul, "Yahoo Mail to Support End-to-End PGP Encryption by 2015," `www.pcworld.com/article/2462852/yahoo-mail-to-support-end-to-end-pgp-encryption-by-2015.html`, August 8, 2014.

[5] Ars Technica, Jon Brodkin, "Dropbox Matches Google and Microsoft Pricing for a Terabyte," `http://arstechnica.com/information-technology/2014/08/dropbox-matches-google-and-microsoft-pricing-for-a-terabyte/`, August 27, 2014.

track your lost or stolen devices. For example, in August 2014, researchers at the Georgia Institute of Technology demonstrated prototype software on the Android operating system that can encrypt any and all communications to and from a device, regardless of the particular app used.[6]

This represents an entirely new phase of in-transit data security for end users that isn't even on the market yet, but don't let too much time pass when it becomes available before adopting. One of the inevitable realities of the virtual landscape we all must navigate today is that as soon as a new level of security is developed, criminals immediately begin the process of unraveling its secrets and chipping away at the protections it offers. Certainly, particularly in light of the tremendous rate of change we've seen in programming sophistication, the benefits of even the newest protective screens can be assumed to be relatively short-lived at best. No matter the size of the swatter, a bigger, badder bug is always just around the corner.

Keep Your Hands off Old Machines

Given the increasingly serious threat posed by virtual crime, although we are creatures of habit, we can no longer afford to be sentimental when it comes to the devices and programs we use to store and manipulate our data. We like our ratty T-shirts and it's hard to get rid of old things, but this shouldn't apply to computing devices, no matter how battered and familiar, which it is absolutely critical to regularly keep updated. Discontinue use of all "dinosaurs" or other obsolete devices, as these simply carry with them too many liabilities to be of any kind of consistent viability. It's not just hardware that becomes obsolete. You must also keep all of your devices up-to-date with software patches from operating system manufacturers and application manufacturers.

It can be annoying to restart your computer and integrate these patches, particularly if you procrastinate and wait until you have 15 to 20 minutes worth of updating to do, but, it is essential that you don't allow any of your machines to get behind, even by a few weeks. The nature of the threats to which they're exposed today is constantly evolving, so continuing to regularly take small steps forward is the best approach currently available.

If your employer seems to be stuck in the proverbial "stone age" when it comes to hardware and software upgrades (which some of the tragic tales we've related here, such as T.J. Maxx, among others, illustrate in an all-too-immediate way), speak up. Say something to someone in a position to do something. Forward current articles about the dangers of out-of-date devices

[6] *Wired*, Andy Greenberg, "This Android Shield Could Encrypt Apps So Invisibly You Forget It's There," www.wired.com/2014/08/m-aegis-android-encryption/?mbid=social_fb, August 19, 2014.

and software to your supervisor, or even your supervisor's supervisor…carefully! Smart money would even go as far as to leave a copy or two of *10 Don'ts* behind in the executive conference room, with pages strategically flagged! There are a lot of misconceptions about what modern computing hardware/software looks like, particularly among employers who are loath to spend money on new devices and upgrades when "We just bought you all new computers/phones three years ago!" But today, with the rate of change that we're seeing across all spectrums of the virtual computing landscape, three years is positively Jurassic.

Dangerous, outdated devices aren't just relics lying around your own office or garage; sometimes you get stuck somewhere without your devices—lost in transit, left behind, dropped, stolen, etc. If you are forced, temporarily, to use an antiquated device or operating system, never transmit any of your sensitive data on it. Wait. It is always better to avoid this kind of exposure whenever it's possible to do so. It's not that a thief is necessarily lurking or that malware is poised to infect at the moment you log on to a machine with an unsupported operating system. But, a thief could be doing precisely that. The probability that you get snared or infected or identified increases every time that you take chances with old equipment or outdated software.

Maintain Your Privacy

One of the biggest issues that technology users face today is the loss of privacy and anonymity as it relates to online activities. Do some research on your own. Find and use a secure or non-traceable browser, as discussed in Chapter 6, to help keep your online activities as private as possible. Get some help from an IT professional if you aren't entirely fluent in the process of adopting new software. There is, of course, no perfect solution to the problem of snoops interested in your business. If they really want to look over your shoulder—if they're committed to doing so—the options start to get pretty scarce. But, you can make it more difficult for snoops to initiate or sustain unwanted intrusions into your personal business. We deserve to be able to operate autonomously online. Sometimes, we have to fight for that privacy and sometimes we need help to achieve it.

Most Important—Be an Educated and Informed Digital Consumer!

Another theme we've returned to throughout the book is that the exposures we have to contend with are emergent. They are like viruses, mutating and evolving in response to the prophylactic interventions security professionals devise. In light of this dynamic landscape, it is crucial to remain current. Be on the lookout for new threats. Read computer magazines, web sites, or blogs. *Wired, MacRumors, CNet, PC Magazine*, and others of the genre are all aimed toward nontechnical to moderately technical users. These resources can help you to keep aware of current hacks or Advanced Persistent Threats that are making the rounds on the Internet. Staying current is increasingly important as the cycle of offense and defense becomes more and more abbreviated.

Remember, this isn't necessarily a process that you have to engage in on your own. Your company's or organization's IT department may circulate warnings or advisories of recently discovered attacks, and what you need to do to steer clear of the threat they represent. Although it can feel like this doesn't pertain to you, because there are a lot of potential targets out there, and it is very seductive to think that "It won't happen to me…," don't ignore these cautions. Read them. If they call for a particular action (e.g., change your password) or non-action (e.g., don't open an attachment from `XXX.com`), the likelihood is that if you follow these instructions your machine won't be exposed to a threat that could otherwise lead to the loss of your data or other broad vulnerability with costly systemic consequences.

We're also in the game. Keep an eye on *10donts.com* and our Facebook and Twitter pages for up-to-date information on current security threats as well. The bottom line here is that because the nature of the threats to the security of your data will continue to mutate and evolve, you can't become complacent and assume that because you were safe yesterday, you're safe today. This is something that needs to be on your mind.

Although the game is changing, some of the old, proven cons and snares are still out there. Ransomware, drive-by downloads, social engineering tricks, etc.—criminals will continue to use many of these same old scams as long as they continue to work. Variants of phishing scams, attacks on cloud providers, and wireless networking attacks will continue to emerge. Governmental agencies and for-profit firms focused on your money will continue to find new ways to "snoop" on private users. Variants totally unrelated to those threats we currently know about, employing methods we can't predict, will be developed and spread and be addressed and continue to evolve in response.

An old adage is relevant here: follow the money. That is exactly what criminals on the Internet will continue to do. As long as there is money, there will be criminals focused on getting their hands on it.These threats will never disappear. They will most certainly continue to mutate, and while there may be intermittent, temporary reprieves from some of the most virulent, these threats are a definitional companion of the virtual infrastructure in which we and all of our collective data are now embedded. These threats will never disappear.

Where there are valuable resources, crime is an inevitable consequence, which is a predictable, regrettable aspect of human nature. Yet, there also are probabilistic realities that bear on the calculus used to weigh risk versus return.

Criminals will always look for targets that carry with them the lowest probability of getting caught in the end, with the easiest escape routes, the most concealed entrances, or other security weaknesses. Twenty-first-century digital thieves are no different from the bank robbers of the 20th century—they will look for the easiest targets and attack those first. Don't make yourself one of the easy targets.

A Christopher McDougall quote is relevant here, albeit with a slightly different indication. As McDougall famously wrote in *Born to Run: A Hidden Tribe, Superathletes, and the Greatest Race the World Has Never Seen*:

> *Every morning in Africa, a gazelle wakes up, it knows it must outrun the fastest lion or it will be killed. Every morning in Africa, a lion wakes up. It knows it must run faster than the slowest gazelle, or it will starve. It doesn't matter whether you're the lion or a gazelle—when the sun comes up, you'd better be running.*

Here, it may not be necessary to outrun the fastest lion; it may be enough simply to not be the slowest gazelle. As the Internet more and more becomes a vehicle for digital commerce, what is clear is that it will become even more inextricably connected to dollars—massive dollars. Digital data are big money, on a truly epic scale, and getting bigger all the time. As some of the recent corporate data-security breaches have highlighted—T.J. Maxx and Target among others—these numbers are big enough to attract the most sophisticated criminals. Don't make it easier than it needs to be for the bad guys, the government, or corporations to get their hands on your data. Always try to keep at least some of the other gazelles in your rear-view mirror.