Appendix

Everything's Connected, Everyone's Vulnerable: Here's What You Can Do About It

Throughout this book we have investigated the looming technological threats that society faces and explored a variety of ways to systemically reduce these risks. The "UPDATE" protocol, described below, provides some practical every day tips you can use to protect yourself, your business and your loved ones from today's most common technological dangers. Follow these simple steps (the digital equivalent of locking the front doors to your home and not leaving your car keys in the ignition) and you can avoid more than 85% of the digital threats that pervade our lives daily.[i]

Update Frequently

Modern software programs are riddled with bugs. Hackers and others use these vulnerabilities to break into your computer and other devices, steal your money and cause general havoc. Avoid these problems by automatically updating your operating system software, computer programs and apps. Pay particularly close attention to browsers, plugins, media players, Flash and Adobe Acrobat—favorite targets of bad guys trying to rip you off. Failing to update automatically leaves your devices wide open to attack via problems that can be avoided if you simply update your software.

PASSWORDS

Passwords should be long (think 20 digits or more), contain upper and lower case letters, as well as symbols and spaces. Though we've all heard it a million times, the strength of a password is one of the key factors in protecting your accounts. You should absolutely not use the same password for several different sites. Doing so means once hackers get access to your login credentials, they can use them across multiple domains, from your social media network to your bank account. Memorizing long unique passwords for every account and website in your life, however, is of course more than the human mind can manage. Fortunately there are a bevy of password "wallets" or managers that can make this process relatively painless. Criminals have been known to create their own password wallets in an effort to trick you into giving up your digital crown jewels. Thus use only use well-known and established companies such as 1Password, LastPass, KeePass and Dashlane, most of which work across your computer, smartphone or tablet. In addition, many services, such as Google, iCloud, Dropbox, Evernote, PayPal, Facebook, LinkedIn and Twitter offer two-factor authentication, which involves sending you a separate one-time password every time you log on, usually via an SMS message or app directly to your mobile phone. Using two-factor authentication means that even if your password is compromised, it cannot be used without the second authentication factor (physical access to your mobile device itself).

DOWNLOAD

Download software only from official sites (such as Apple's App Store or directly from the company's own verified website). Be highly skeptical of unofficial app stores and third-party sites hosting "free" software. In addition, avoid pirated media and software widely available on peer-to-peer networks which frequently contain malware and viruses. Settings in both the Windows and Mac operating system can help you "whitelist," so that only approved software from identified vendors is allowed to run on your machine. While doing so will not guarantee software safety, it can greatly reduce the risk of infection. Pay particularly close attention to apps and their permissions. They are "free" for a reason and you're paying with your privacy. If a flashlight app tells you it needs access to your location and contacts, run the other way.

ADMINISTRATOR

Administrator accounts should be used with care. Both Windows and Apple allow users to set account privileges, with administrators having highest privileges. While you will need an administrator account on your computer, it should not be your default account for every day work and online browsing. Instead, create a standard 'user' account to do the majority of your work and for day-to-day use. When you are logged in under administrative privileges and accidentally click on an infected file or download a virus, the malware has full privileges to execute and infect your machine. If you are logged in as a general user and the same happens, often the virus, Trojan or worm will require your specific permission to execute, giving you a warning sign that there is a problem. Always run your computer as a non-admin users unless absolutely necessary to carry-out a particular task, such as a known update from a trusted source you are conscientiously installing.

TURN-OFF

Turn-off your computer when you aren't using it. The simple act of turning off your computer while you sleep will automatically reduce your threat profile by 1/3 because thieves cannot reach out and touch your machine when it's not in use and connected to the Internet. In addition, turn off services and connections on your smartphone when you aren't using them. Keeping Bluetooth, WiFi, NFC and cellular hotspots on at all times, provide additional avenues for attack, which thieves can use to hack your phone, spread malware and steal data. Also, keeping WiFi on allows retailers and advertisers to persistently track you through your physical world, further encroaching on your privacy. Only turn these services on when you need them.

ENCRYPT

Encrypt your digital life, both locally and as your data is in transit across the Web. Both Windows and Mac include free programs for full hard disk encryption, (Bitlocker and Filevault respectively). Encrypting your hard drive means others cannot read its contents if lost or stolen. You should also encrypt your Internet traffic by using a Virtual Private Network (VPN), particularly when using a public WiFi network such as those at airports, universities and coffee shops—frequent targets for hackers and thieves. Your phone, too, should be encrypted, since today's mobile devices can have as much, if not more, personal information as our laptops. Always use a password on your mobile phone and consider enabling biometric security, such as Apple's iTouch fingerprint technology. Using a password in the latest version of iOS and Android not only ensures nobody else can access your phone and its data in your absence, but it also provides full encryption on the device adding another layer of privacy and security.

Additional Safety Tips

If you faithfuly follow the UPDATE Protocol above, you can avoid more than 85% of threats. To further secure yourself, follow these additional tips.

1. Use common sense with all your email. As a general rule of thumb, be wary of any request to click on a link or open an attachment sent to you–even when it looks as though it comes from somebody you know. Criminals are expert at tricking the general public with irresistible headlines, such as "click here" to see the shocking photos of this naked movie star or another. Phishing attacks only work because unsuspecting individuals click on files and links that look realistic or enticing, but contain a malicious payload which will infect your machine. When in doubt, check with the individual who purportedly sent you the email to verify it came from them (don't reply to the email itself!) And no, there isn't Prince of Nigeria who is reaching out to you personally with a viable way to get rich quick.

2. USB drives are one of the most common ways to spread malware and other computer viruses (the Department of Defense has even banned their use). Generally speaking do not accept the thumb drive from a stranger (or even a person you know well) or plug one into your machine without first scanning for viruses. Disable "auto run" on your computer to ensure that any viruses do not automatically execute thereby infecting your computer. The same advice applies

to external USB hard drives and even smartphones that do not belong to you.

3. Back-up your data frequently. You can back it up onto an external hard drive using built-in operating system tools such as Mac's Time Machine of Windows Backup. You can also use cloud providers such as Carbonite, Backblaze and SpiderOak. When utilizing cloud providers it is wise to encrypt the data before uploading it for an extra measure of protection. In addition, you should always have multiple back-ups of your data. Keep one or more physical drives for back-up and ensure that at least one of them is stored off-site so that in time of disaster, fire or break-in, a back-up of your data will be stored in a safe and secure location.

4. Cover-Up. Unfortunately it is easy for hackers, criminals and spies to get access to all the Internet-connected the cameras in your life, whether on your computer, smartphone or tablet. When not in use, cover the camera lens up. A simple PostIt note or piece of tape will do and will provide cheap protection from unwanted prying eyes.

5. Sensitive browsing, such as banking or shopping, should only be done on a device that belongs to you and on a network that you trust. Whether it's a friend's phone, a public computer, or a cafe's free WiFi—your data could be copied or stolen. Be particularly wary of computers in common or high-trafficked areas such as airport lounges, favorite targets of criminals who have planted malware and keystroke loggers in areas where business people congregate.

6. Think before you share on social networks. Criminals, ranging from stalkers to burglars, routinely monitor social media for information. Posting travel itineraries can let burglars know that you will be away from home for two weeks on vacation–an invitation for trouble.

7. Use your operating system's built in software firewall, available in both Windows and Mac, to block unwanted incoming connections to your machine and enable "stealth mode," to make it more difficult for hackers and automated crime bots to find you online.

Note: Both the threats and tools to protect yourself online change frequently. For additional guidance, visit www.futurecrimes.com

[i] http://www.asd.gov.au/publications/Catch_Patch_Match.pdf