CYBER SMARTS

FOR STUDENTS

WILLIAM TAN • ABHISHEK ALLAMSETTY • JACK DUVALL
GABRIEL WIMMER • RICHARD LUN • MONICA SARAF

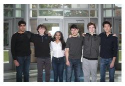
CyberSmart Now

CYBER SMARTS FOR STUDENTS

www.cybersmartnow.org

CyberSmart Now

The authors of this book are students from Thomas Jefferson High School for Science and Technology (TJHSST), and their team was the national finalist in the 2016 National Youth Cyber Defense Competition (CyberPatriot IX) – high school division.



Left to right: Abhishek Allamsetty, Jack Duvall, Monica Saraf, William Tan, Gabriel Wimmer and Richard Lun

ISBN: 978-1-54393-165-5

TABLE OF CONTENTS

hop Safe Online, Even on Black Friday

Chapter Twelve:
Securing New Devices in an IoT World

Chapter One:

Privacy is Our Shared Responsibility

- Abhishek Allamsetty

Recent events focused an intense spotlight on online privacy and security. I thought I'd explore why it's critical we not let this moment pass and just lapse into our normal complacency about these issues once the media thunderstorm passes.

Now more than ever, as our digital footprints grow exponentially, we need to take personal action to preserve our online freedoms. Why? The Internet benefits and belongs to all of us — thus it is our joint responsibility to protect it.

The benefits of the Web have, of course, come at some cost, one of which is a loss of privacy. We are also more vulnerable to data breaches and identity fraud. But there are many things we can do to minimize the risks of both.

The threat from hackers and cybercriminals has expanded in relation to our dependence on the Internet. As our reliance grows, opportunities for them to prey on us increase. Online data breaches are not new. They have been around since the creation of the first networks, but there is a risk that they could reach epidemic proportions — cyber fraud is currently the fastest growing category of crime in the U.S. — and eventually erode our freedom to use the Internet as we desire.

As with past epidemics what is required is a combination of collective and individual action. It is not that much different from how we have managed medical plagues in the past. When enough people stayed indoors, washed their hands or received vaccinations, certain diseases were wiped from the planet. It took some time to convince people to change their ways, but eventually as a society we worked together to inoculate ourselves from many epidemics.

Taking it back to the Web, we should think of our digital identities as susceptible to digital epidemics. Fifteen years ago, led by company IT teams, we started inoculating desktop computers with antivirus software. Now the battle has shifted to the cloud, and we have to start walling off our digital communications, much of which are now mobile. The more people that inoculate themselves from malware, spear phishing attacks or hacker intrusions, the safer we all are.

Think about it, once you establish barriers to unwanted intrusions you wall off the digital ailments that can spread so easily. Your online communications will be one less component in a botnet assault. Your email account or Facebook profile can't be hacked to send a spear phishing request to a friend, colleague or business partner that could lead to a larger data breach.

Although I view the act of taking personal responsibility for online privacy and security as the single most important ingredient in stemming the tide of cybercrime, there is also a role for government and law enforcement. We're in the midst of an interesting time as there aren't comprehensive and functional data collection laws in the U.S. and only some countries have variations of privacy acts, laws, and initiatives.

In the past 50 years, there have been several Supreme Court decisions to guarantee our privacy rights — rights implied but not explicitly guaranteed in our Constitution. But much of the ongoing furor today is in response to certain agencies not abiding by such principles.

The ongoing NSA debate, tech giants advocating for transparency, medical identity theft, and even Google's Street View wire-tapping snafu, however complicated they may be, illustrate one thing — online privacy and security are finally making headlines. So let's leverage the conversation for constructive benefit.

The great struggles — racial equality, gender equality, equal opportunity, and today, universal health care, marriage equality and immigration reform — have all involved crucial dialogue between our government and its citizens. And ultimately a legislative agenda emerges to move society forward.

Of equal or even greater importance is whether or not we, the people, take action. We as individuals need to demonstrate that privacy and security in the digital realm is a top priority — that we are willing to take collective responsibility to protect ourselves from growing threats to our online privacy and freedom.

A Pew Research Institute study from this summer revealed that 86 percent of Americans have taken action to maintain anonymity online — deleting cookies, encrypting email and/or protecting their IP address. Another telling metric from that report states that 50 percent of Internet users say they are worried about the information available about them online, up from 33 percent in 2009.

Additionally, an AnchorFree study from June 2013 that polled 1,200 U.S. and U.K. college students revealed similar sentiments with 82 percent responding that they were concerned about keeping their data private. Those are important developments indicative of a changing tide in attitudes toward online privacy.

But everyone needs to do even more. A recent Verizon study of global law enforcement data found that data breaches have more than doubled since 2009. Cyber fraud perpetrated against individuals is growing at 15 to 20 percent a year, according to the FTC). The only way to build a culture defensible against data breaches, hacks, and identity theft is to contain them within the realm of minor inconvenience and not allow them to be contributors to a mass assault. The more we do to inoculate ourselves against the digital flu, the less likely there will be digital pandemic.

It is no longer enough to install anti-virus software on your PC and dump your cookies once a month. I urge everyone, first and foremost, to actively participate in the debate about privacy and security. Equally important is for everyone to adjust their online habits to help prevent privacy risks and security breaches. Choosing more careful passwords, limiting where, when and with whom you share sensitive data, and using a VPN to encrypt your data every time you go online are simple steps everyone can take.

It is your responsibility to protect the Internet community for tomorrow's users just as much as it is mine.

Chapter Two:
Good Cybercitizens Make Internet a Safer and Better Place

- Monica Saraf

Have you ever been bullied or mistreated online? Have you felt like you weren't safe online? If so, here are some tips on how to feel safe and make the internet a much safer place. First, we'll start with what you should do in order to make others feel safe online and then we'll go to what to do if you don't feel safe online.

No matter where you go or what you do, there will always be people who are out there to hurt people and put them down. This, however, should be the reason that you act the exact opposite. Just as in life there are rules to how you should treat others, there is netiquette – how people should behave online. Have you heard "if you don't have something nice to say don't say it at all?" This also applies to the Internet.

It can be very easy to hide behind a computer screen with a different name or personality, but this should not encourage you to hurt others. Regardless of who you're talking to, it is best to be kind. You might not know what the other person is going through. Compliment photos online or don't say anything at all. It can be really easy to forget that there is a person on the other computer as well who has feelings and emotions. Act the way you would as if you were to speak with them in real life.

Remember that being able to access the internet is a privilege, not a right. Abusing it to hurt others can eventually come back to you. Whether you're playing video games or just talking, it is important to take other people's thoughts and ideas into consideration and when someone makes a mistake, it is good to accept and forgive. You might not always know another player in a video game but when you talk to them, you have to stay polite. People might not understand something the same way that you do. In order to ensure that you are safe and not misunderstood, be very careful with using caps and slang that might not be understood by everyone.

However, just because you help others feel safe online, it doesn't mean that they will do the same to everyone else. If someone decides to be mean or saying mean things online, there is always a reporting option. The following website gives you instructions on how to report a user on many different websites: https://cyberbullying.org/report. You can report the user for saying or doing something mean and if this behavior is repeated, it is best to talk to a trusted adult about it. People say things unintentionally and although once or twice is forgivable, repetitive harassing behavior is not acceptable.

See Something, Say Something

Sometimes you see bullying online or notice that someone is being mean to someone. Just as you should in real life, support the person who is being bullied and help them stand up for themselves. Being there for someone else who is being hurt can never hurt you, unless you hurt the bully. Generally, these are people who are incredibly insecure about themselves and put others down in order to feel better about themselves. They've either been bullied before or use it as a manner to increase self-confidence. Many bullies realize what they are doing it and do it on purpose. Some may not realize and as a friend or a person, you should try to tell them what is happening and to stop bullying. Not only will you gain a friend, but you'll find a way to get rid of a bully.

People say mean things intentionally and unintentionally, make sure that you aren't someone that people want to report. Be careful of what you say and do online because once it is said, it can be retrieved again, even after being deleted. No matter how many times it is said, it cannot be repeated enough, be *extremely* careful of what you say online. If you think you wouldn't want colleges and your future employers seeing what you're about to say, don't say it.

Some things can be the last straw for someone. Even a small joke can be taken in the wrong and hurt someone to an unexpected extent.

Stay Positive

.Compliment people whenever you can. It is better to try to make someone feel good when you truly think it. If you've ever heard about flame wars, you probably know that they can get quite out of hand. Flame wars are when someone starts an argument and others join in creating an uncontrollable, massive argument. Many people will argue for hours at end about something and some people might only be out there in order to start them. No matter how tempting it may seem to argue, it is better not to, *especially* if you do not personally know the other person. You don’t know what they are capable of and what they could possibly do.

Things happen online the way they do when driving. For example, road rage can be incredibly dangerous. Someone might say or do something that enrages another driver, but getting angry and trying to fight, can result in hurting you or another person. On the road, there are many strangers and potentially dangerous people and it’s no different for the Internet. The best to stay safe in both road rage and online situations is to stay calm.

In summary, be careful no matter what situation you are in. The internet is a large area with millions of people on it every day. It is important to know that there are people who are bullied and hurt. A major tip is to not be one of the people who causes others to feel this way and to help those who need help. Stand up for those around you and protect your friends. Stay calm if someone is trying to start a fight and follow the rules and ideals of real life when you are online. You don’t want to be that person who witnessed someone being bullied and stood there watching in real life, and this applies online.

Chapter Three:

How to protect your data and device while travelling with technology

- Gabriel Wimmer

Maintaining a vigilant attitude towards cybersecurity doesn't stop once you leave your house. In fact, it is when you are travelling that your devices and personal information are most at risk. The key to reducing your risk of attack while out and about is to reduce your exposure to unsafe or unfamiliar networks and connections.

The easiest way to protect your technology when travelling is to simply leave it at home, but for many people (myself included) who cannot live without their laptop or smartphone this isn't an option! The second-best option is to reduce the amount of technology you bring with you. While this sounds unthinkable at first, I urge you to take into consideration why you are travelling. If you are travelling for extended periods or school reasons then of course this isn't an option, but if you're on a vacation or visiting relatives then maybe bringing a laptop, xbox, tablet and gaming desktop might not be necessary. You may just need your phone to have a fun and relaxing vacation. Trust me, I have firsthand experience lugging around too much tech when I should have been enjoying my vacation instead.

However, your technology can definitely help you enjoy your vacation, keep you connected with your friends and make you more productive. However, to get the fully benefit of your technology, sometimes you must “connect” to the web. At this point, you have to make an informed decision regarding the risks that you face. Your technology can definitely improve your vacation, but it can also ruin it and a lot more if you’re hacked! For example, let’s say you’re all alone, in an airport with only your phone and laptop to keep you connected to the Web. How will you charge your devices, browse the Web or email your friends all while keeping hackers from stealing your information or damaging your technology?

The first and most simple of threats are the physical ones. When in an unfamiliar area, the safest thing to do is to distrust all connectors, port and charging stations you see. There have been many reports of free airport charging stations being used to hack people’s phones. They do this by providing a port to connect your USB cable into instead of a normal electrical outlet. A USB cable can be used to charge your phone, but it can also be used for other things that may put your device at risk! Your USB cable enables you to connect your phone to computers and other devices, so you can transfer data such as games, photos or videos. Connecting your phone to unknown stations with your USB cable could give hackers access to everything on your phone! A much safer alternative to these charging stations is to use your phone’s wall adapter with an electrical outlet. Another alternative that I strongly recommend is to use a portable battery charger. Portable battery chargers are inexpensive and can usually provide one to three “full charges” to your phone. These are not only safer charging alternatives, but they are extremely convenient when you’re outside. Sometimes, I charge my phone while it’s in my pocket using a small portable charger. If you’re carrying multiple devices, another charging option may be using one device to charge another one. For example, my laptop will charge my connected phone even when the laptop is not plugged into the wall.

Now that you’ve sorted out charging your devices, let’s move on to using them. Your first instinct when trying to set up your computer in the airport might be to search for the first password-free network to join. I strongly urge you to take caution when doing so. Once you are on a network it’s very easy for someone to capture the information going from your computer to the router. If this information is not encrypted, the hacker can piece together the information and view everything you are doing on the internet.

Browsing the internet on unsecure networks can be risky, but there are many different precautions you can take with varying degrees of difficulty and security. The first would be to use websites that support encryption. Encrypted websites use the HTTPS protocol to communicate between your computer and the websites server which encrypts your data and prevents people from piecing the information together and figuring out what you are doing. Not all websites support HTTPS and you can determine if HTTPS is currently enabled by looking for an icon of a lock next to the URL on your browser. Some websites are capable of using HTTPS but default to HTTP. They can be switched to using HTTPS by using web extensions called HTTPS Everywhere which can be added to most web browsers for free. Although adding extensions to your browser is different for each browser that you use, most tend to have the extensions section under the settings tab found in the top right of the browser's screen.

While this is a good first step towards securing your information while traveling, it isn't all encompassing. First, HTTPS is not supported on all websites. Second, HTTPS encrypts the information on websites, but not the actual identity of the websites you visit. A hacker can still follow your trail on the internet. You would be surprised by the amount of information that can be obtained about you by simply seeing the websites you visit. For example, if you go to a specific restaurant's website just before dinner time, then you likely just shared your location with a capable hacker.

A solution to the limitations of HTTPS would be to encrypt everything you send through the network in what is called a virtual private network or VPN. A VPN creates an encrypted tunnel between your device and whatever network the machine running the VPN service is on. Essentially making it appear as if you are currently in that network. Your data is instead sent to the machine running the VPN service which decrypts it and sends it on its way. This means that for a VPN to be secure you must trust the network the VPN service is running on. For most people their home network is secure enough for them and they opt to set up their own device to run a VPN service on their network. This can be done through a wide range of software using devices like the raspberry pi, your home desktop or even your router. Any hacker at the airport attempting to view your internet usage would only see a garbled mess of encrypted data.

Setting up a VPN on your home network is not too hard to do and is definitely worth the effort! There are several websites that provide very good, step-by-step instructions that will walk you through the process. A few of my favorites include: PCWorld.com, lifehacker.com, and howtogeek.com

For those who would like to enjoy even more privacy and security, there is the option to buy a VPN service from a VPN provider. These are companies that specialize in creating a fast and secure network of VPN servers for people to use. Services like these also tend to come with other privacy features such as an anonymous IP address (to prevent you from being tracked), fire walls, and sometimes even ad blockers. This might sound great, but it all goes down the drain if you don’t trust the company providing the service! Before going this route, research the numerous providers first.

If all the hassle around a VPN sounds like too much work, then fear not as there still is another way: cellular. By using your phone’s cellular data, you are avoiding sketchy airport WiFi entirely! While it might be slower (and more expensive?) than traditional WiFi, no one can spy on you or your personal data as long as your phone’s hotspot has a secure password.

Chapter Four:

Spring cleaning - Be green, not blue

- Gabriel Wimmer

Are you tired of your computer running out of disk space every time you try to download a new game? Sick of waiting for the end times just to open your internet browser of choice? Fed up with seeing your CPU usage spike to 100% just by looking at the desktop? If so, then this chapter is for you!

A decline in your desktop's or laptop's performance is normal as you begin to use it and install programs, In fact, it's pretty hard to keep your computer running as perfectly as you bought it once you begin to use it. These degradations can be a result of malware, background programs, and the overall clutter of data.

The first step towards reclaiming your computer should be to make sure it is malware and virus free. Malware is short for malicious software, which means any software that is intended to do your network, device or data harm. A virus is a very common type of malware. A virus is a hidden program that can spread by copying itself and usually does something evil, such as corrupting your device or destroying data. All the following steps are pointless if your computer has been compromised by malware. To remove any malware on your computer we recommend downloading an anti-malware program such as Malwarebytes (which is free) and scanning your computer. Malwarebytes can be downloaded for free at malewarebytes.com or cnet.com.

Anti-malware programs will scan your computer and remove malware, unwanted registry changes, and even help remove programs that are generally bad news and not to be trusted. Unwanted registry changes are changes to your operating system settings that tell your device to do unwanted things when you boot your device.

Now you have rid your computer of malware you can begin cleaning it up. The next step on your computer cleaning campaign should be to "programs and features." This panel can be reached by going to your control panel, navigating to the programs section and then selecting programs and features. The easiest way to find this page is to search "programs and features" in any of your operating system's search bars.

The programs and features pagewill open a list of all the programs that have been installed on your computer. This is one of the easiest places to weed out the unwanted stuff from your computer because this panel comes with a handy dandy uninstall button. This page provides a wealth of knowledge about what's on your computer and when it was installed! Specifically, this page lists the name of the program, its publisher, install date, size and the version of the software installed. I must caution you that a lot of the programs listed on your computer may not be recognizable but are vital to your computer! A good rule of thumb that I use is that I will not delete any programs installed before the computer was purchased without being absolutely certain what they do and if they're needed! The rest of the programs, installed after I got the computer, are fair game! Another thing that I recommend is to look closely at the install dates. If you are the device’s only user and you don’t recall downloading or installing programs on their install dates, then look really hard at these programs!

Again, the uninstaller typically does a really good job removing unwanted programs. However, in some cases, the uninstaller doesn’t manage to catch every single file left by the removed program. To get everything left by the unwanted folder, you can search for the removed program’s install folder and delete whatever is left. Most of the time, File Explorer is where you’d go to find files on your computer. However, File Explorer does not search all program folders and files. However, this can easily be done by going to your computer’s command prompt and searching your entire computer for the unwanted program’s install folder. To do this, first go to the command prompt by typing “cmd” without the quotations into your operating system’s search bar. Now, simply click on the command prompt option that pops up. Be warned that the command prompt is an all black screen with a flashing cursor that is waiting for you to type in your command. Now, type the command *dir /s /b | find “the name of whatever you’re searching for here.”* In this command, the quotations are needed! When looking for scraps of unwanted programs, I search for the name of the program and also its publisher’s name that’s listed in the program and features page.

For example, let’s assume that you want to remove the DropBox application from your computer. To find the location of its location on your computer, type in the following command in the command prompt:

```
Dir/s/b|find “dropbox”
```

The command prompt lists the precise location of every file and folder with “dropbox” listed. Now, I can use my File

Explorer and easily navigate to the precise location to find and remove the unwanted items.

Now that you have removed all the programs that you no longer need, the next issue to address is background programs. Having an abundance of programs running in the background slows your computer even though it appears as if nothing is currently running. To stop them, open up Task Manager by pressing *CTRL+SHIFT+ESC* at the same time. This will open a list of all tasks running on your computer and how much of your computing resources they are using. These processes can easily be stopped by using the End Task button, but make sure you don't end critical Windows processes that keep your computer running.

To keep these programs from running in the background again you're going to need to stop them from starting themselves automatically. To do this, navigate to live.sysinternals.com in your web browser and click on the autoruns.exe link. After downloading it run the executable file (.exe) and you'll see a window pop up. This window pop-up contains a list of all the programs that are set to run on their own. To stop them from doing so just click the checkbox next to their name. Be very careful though as some of these are necessary for your computer to run normally, a good frame of reference for Windows services and their importance can be found at www.blackviper.com/service-configurations.

While we may have gotten rid of some of the bigger more noticeable slowdowns there are still more things that can be removed to free up more space. Both Windows and the programs running on it create a large amount of temporary files that it saves but sometimes never deletes that are not crucial to the program or Windows. Over time these files can waste huge swaths of space.

Luckily, Windows has a tool built in just for this problem: Disk Cleanup. It can easily be found by typing Disk Cleanup into the search bar. This tool will analyze your hard drive and round up some of the unnecessary files on your machine. Disk Cleanup will also check your recycling bin for files. This is important because every time you delete a file it goes into the recycling bin in case it needs to be recovered. Files in the recycling bin still take up disk space and need to be emptied from the recycling bin to truly be gone. After selecting the locations for Disk Cleanup to check and running the program you should have rid your computer of some of the last bits of clutter but even so there are some things Disk Cleanup doesn't catch.

That's what 3rd party disk cleanup software is for. Programs such as CCleaner have a myriad of different tools to ensure not a single unnecessary file is left on their computer. Popular features for programs like these include duplicate file checking, registry cleanup, and real time file management.

Now that the computer is completely free of clutter and unwanted programs there is one last thing to do to help give it that brand new performance and feel. To achieve this you're going to want to navigate to your Control Panel, then to Administrative Tools and finally to the Defragment and Optimize Drives panel. Or, you can simply type "defrag" into your operating system's search bar.

Defragmentation is the piecing together of files on your hard drive. When a file is placed on your disk the machine cannot always keep it in one piece and sometimes will fragment it to fill empty spaces on your hard drive. What looks like a complete file on your computer screen might instead be a bunch of small fragments of data your computer put together from different regions of your hard drive. As you might expect, piecing the data back together is time consuming and inefficient. Which is what this defragmentation tool is for. It scans your entire drive putting all the files back together for the quickest access to them. There is also an option to set up automatic defragmentation so that after an interval of time your computer will automatically defragment your drives.

Chapter Five:
Use Strong Passwords and Passphrases to lock down your login

- Jack Duvall

In the world of the Internet, passwords are nearly everywhere. From your school accounts to social media to news sites, every application wants a password. But how do you keep all these passwords straight? How should you make secure passwords? And why do we even need passwords in the first place? In this chapter, we will try to answer all of these questions and more.

First of all, why do passwords exist? For starters, passwords are the simplest and most effective way to make sure the person using an application is the person that is supposed to be using that application. You wouldn't want your little brother posting fake news on your social media! Passwords enable email, banking, and other confidential information to be created with the assurance that the creator is who they say they are.

You probably already have made and used plenty of passwords for a multitude of sites. You probably even have you own method of deciding on a password to use. However, what you may not know is whether your passwords are secure or not. A secure password meets ALL (not just some) of the following requirements:

- Don’t use your username as your password. Most websites will enforce this anyway, but you should not do this anyway.
- Don’t use a simple password like “password”, “qwertyuiop”, “111111”, “098765”, or any other variant.
- Don’t use a password that’s on one of the common brute-force lists; a few such lists can be found at https://github.com/danielmiessler/SecLists/tree/ma
- Don’t include easily accessible personal information in your passwords, such as your name, birthday, or address.
- Avoid sharing your password with someone else, even if only for a little bit. If you need to log into someone else’s computer, type in the password yourself.
- Avoid using the same password for multiple sites. This one is more important than you might think; if one site gets hacked, the hackers won’t have access to any other of your accounts.
- Avoid using dictionary words directly in your passwords. You can, however, use shortened or misspelled versions.
- Do insert random punctuation, numbers, uppercase, and lowercase symbols in your password. Be warned, however: some sites block certain punctuation.

- Do make your password easy to remember for you, yet hard to guess. A simple phrase like “I wish I had some ice cream right now” can be turned into the password “1wIh@d5umICrn!”, and “Wow this is such a great EBook” can be turned into “!W0W!ti54gr8[3BUK]” for example.
- Do make your passwords long. Every character you add makes randomly guessing your password around 8x harder even for the best hackers.

Contrary to what some say, if an organization does not enforce it, you do not need to change your password every month or every year. Doing so just encourages you to make weaker passwords because you are more likely to forget which password you use. One strong password is better than a bunch of weak passwords. There is one exception: If you suspect your account has been hacked, or have seen in the news that a site you visit has had its passwords leaked, CHANGE YOUR PASSWORD! It really doesn’t take that long.

Eventually, unless you have a superhuman memory, you will start to forget passwords for all the different sites you sign up for. Your browser will probably save your passwords for you, but it’s better to have a specialized password manager do that for you instead. Software suites like KeePass, LastPass, and 1Password are designed to do one thing very well: keep your passwords safe and encrypted so you only have to remember the decryption password.

Of course, there are many other ways of verifying the identity of a user. You may have heard of fingerprint and facial recognition sensors on iPhones and various one-time passcode generator apps such as Google Authenticator. These make up the other 2 parts of the “identity triad”: Who you are (fingerprints), What you have (your phone), and What you know (passwords). The more “authentication factors” you supply to an application, the more secure it is. Until recently, it was hard to have anything more than a text password, so that is what has become the standard. Still, many sites nowadays do support at least 2 factor authentication (password + code generator usually), and it is highly recommended you use that whenever possible. The extra inconvenience logging in the first time is worth it to practically guarantee you will never get hacked.

To summarize, make your passwords long and hard to guess with plenty of randomness, but easy for you to remember. Use a good password manager, and also use multi factor authentication whenever possible. Finally, never share your password. Remember, passwords are close to the last line of security, and need to be the strongest.

Chapter Six:
Beef up your physical security

- Jack Duvall

There’s a common saying in computer security: physical access is game over. Once a hacker can touch and modify your device for as long as they want, they can potentially do anything with it. Fortunately, since you have control over your device most of the time, there are plenty of things you can do to slow thieves and would-be hackers down. Physical Security is your first or last line of defense depending on the attack, and it needs to be secure either way.

The first and most obvious thing you can do to prevent these sorts of hacks is not let your device out of your view. If possible, always keep your computer, tablet, or phone within sight. That way, you can prevent any obvious stealing or tampering. If you do really need to leave your computer somewhere unattended, first ask a trusted friend to keep watch while you are gone. If there are no friends in the vicinity, inconspicuously hide your device somewhere relatively safer than out in the open.

Another party you have to rely on for your device’s physical security is the manufacturer. Apple iPhones and many other big-name smartphone manufacturers are notorious for making their devices hard to get into with regular hand tools. Many laptops nowadays are going the same way, using tiny proprietary screws instead of regular philips head or hex nut, and are cramming all the components into a small a space as possible. While this is bad from a hobbyist perspective (it isn't easy to modify your own device), this is great from a security perspective (it isn't easy for others to modify your own device). Any hardware additions, unless crazy sneaky, will be immediately noticeable from a loose case or bulge.

There are also some non-physical modifications you can make to your device that will improve its physical security. The most easily done and most heavily recommended is to secure your laptop and/or smartphone with a passcode. By far, this has the highest ratio of security payoff to simplicity. All major operating systems highly recommend, if not require, securing user accounts with a password. Usually they also make it very easy to do so too. If a random passerby can just access a computer as if they were you, imagine all they destruction they could do to your account! The same principle goes for leaving your account logged in on public computers. I can't count the number of times I've found someone's account logged in on a library computer with their personal files out in the open. If an unwanted person can get access to your account that easily, you are just welcoming low-effort attacks that can be both annoying and extremely damaging. An easy solution is to, as mentioned in the chapter on Password Security, use a dedicated password manager with password-encrypted passwords to store all your passwords.

While the previous bit of advice is universal, the next is a bit out of the norm. To prepare for the extreme case that your device is stolen, you should disable your browser's password saving feature. I know, I know, that's absolutely crazy and there's no way you'd ever do that because it's simply too much effort to remember all your passwords. Besides, aren't hackers more interested on the files on your computer than your agar.io login? That's only partially true: While sensitive files on a computer are good targets, account information is an even better one. If you have your browser configured to remember your login sessions and your passwords, people can post unsolicited material to your social media accounts in your name, sign up for services with your email, and worst of all, access your banking info. You might not care too much about the risks to your accounts right now, but the effects can be devastating.

The following paragraphs apply only to those who are interested in server security. If you'd like, you can skip to the next chapter instead.

When doing server security, there are many more factors to consider than for physical security of personal devices. For instance, you are often not going to be carrying around a server wherever you go, so you don't have constant surveillance of it. Also, for higher end servers, the environment needs to be much more controlled than for a laptop. Because of all these different factors, server security is hard to get right.

For starters, you definitely want to keep your server in a specially-equipped room. For something like a desktop, a room with good standard home air conditioning and a network drop will be fine. For something more heavy duty like multiple rack-mounted servers, special temperature control units, uninterruptible power supplies, and high-speed network connections are necessities.

Now that you have so much expensive equipment in one room, of course you are going to want to secure it. For the small desktop case, a simple padlock or bike lock on a locking case combined with a door locked with a key should suffice. A normal case probably does not come with a locking mechanism, so you will need to buy one that does. For a larger server setup, you should use a pin code lock or a badge scanner lock combined with heavy-duty doors. In both cases, you should also make sure the wires going to the room, such as the power and network lines, cannot be easily tampered with. If you want to avoid excessive damage in case of a fire, you should also install electronics-safe flame retardant dispensers to replace sprinklers in the server room. Finally, get security cameras to monitor the comings and goings of anyone accessing the server room, in addition to adopting the policy of notifying the person in charge of the server room any time it needs to be accessed.

Chapter Seven:

Secure remote access - Easy as A, B, C

- William Tan

It's easy and convenient to access your personal computer and files while away and unable to haul what might be a twenty-pound machine with you. Being able to access everything on your computer when you're halfway around the world isn't something to sneeze at. Remote access, after all, can be made safe. It just requires some additional thought.

However, remote access to a regular home and/or personal computer is often negative in that it exposes your system to additional vulnerabilities, such as malware or scammers. For the best interests of security, a personal computer shouldn't be allowed to be accessed in any form other than physically, which means actually touching the computer and using the keyboard to enter a username and password.

Many sorts of malware can exploit the openness of your computer and gain access to files it shouldn't be allowed to access in the first place. With a bad password, remote access can be taken advantage of to do lots of damage to the computer or steal personal information in order to buy items in your name with your computer. Accidental remote access is one of the more frequent ways malware uses to enter your computer.

Remote access is also often the goal of many scammers, who pose as tech support from Microsoft, Intel, or some other large company. Their objective is to gain access to your computer by abusing your trust and then either stealing files or injecting malware that could do a myriad of nasty things to all your personal files. There are plenty of articles and YouTube videos online that detail scammers and how they were dealt with. Though hearing a scammer from 'Microsoft' getting scammed in return is pretty hilarious, scammers are no laughing matter, for they hold authority (if only in name) and know to use that authority to get you to panic and make bad decisions, such as letting them into your devices.

Password security, physical security, and a good degree of common sense is needed to make and keep a remote connection secure. After all, you open many, many vulnerabilities once TeamViewer, LogMeIn, or any other remote desktop utility is installed.

When you log in to your computer remotely, you begin something that's called a session. Always end the session when you're finished (by logging off) or when you're going to leave the accessing computer unattended (also by logging off). You never know if someone might take advantage of you leaving it open to do nefarious things on your home computer. It might be tedious to type your password in over and over and over, but it's well worth it, considering the risk of someone sensing an opportunity and going for it by putting nasty stuff onto the computer while you are in the bathroom. Ensure that your password is secure, as well. If, somehow, someone gets the unique identifier to remotely access your computer or the account that the remote-access program uses, it would be much better if they didn’t get in simply by typing in ‘password,’ ‘12345,’ or other insecure key-phrases.

Also, if you are not accessing it from another device you own, ensure that the device you do access it from is not tampered or rigged with malware that can trace exactly what you put in to access your own device. In addition, that malware can also trace the activity you do on your own computer and might sweep up details you might not have wanted it to know, like credit card details, a home address, a phone number, and other personal information that can be sold and used by crooks. In accordance with the prior chapters, evaluate the devices you are accessing are secure as well as the devices you are using to access them. If one end is compromised, both of them are vulnerable to maliciousness.

Though most utilities encrypt the usernames/identifiers and passwords for remote access, there are some that simply send it along without any attempt to obscure the authenticating data. Ensure that the network you are connected to is secure and communications cannot be intercepted, which should be fairly intuitive based on the wi-fi symbols on your taskbar or screen, which will display alarm images and throw messages that indicate that the network you are on is not secure. Otherwise, the security of the username and password matters not to someone who might be monitoring network traffic like a shark, waiting for the right moment and the right morsel of information to pass through.

A remote connection to your computer at home through some utility or service is like a vital blood vessel linking the device that accesses your computer to your computer. It is an extremely vulnerable direct line of access that can easily be taken advantage of. That’s one of the main reasons why, when most businesses allow remotely accessing, multiple layers of authentication are required, with programs that can strongly encrypt any sort of communication sent, rendering it invisible to anyone watching from the outside.

Even when you’re using a more insecure utility for your home use, this vulnerability can be shored up and defended. All it requires are, as stated before, password and physical security, along with a sense of when to use or not use it.

Setting up remote access is fairly simple: download, click, and install. Some programs would require a free registration; feel free to supply a rarely-used or newly-created email address to avoid any potential spam. Then, register your computer with the program and ensure that your password and everything else is secure.

Remote access can also be set up without having to download anything. Remote Desktop, for example, can be used with Windows without any additional installations. However, Remote Desktop is very vulnerable to being exploited as well as being used as the primary entryway for any potential hacker. It would be better if an alternative was installed and used.

If you’re worried that your remote-access username and password have been found out by someone else, immediately change the password and (if possible) the username.

Once you have your device ready to be accessed, always remember: keep the device you’re using to remotely access safe; always log out when leaving the computer unattended; and ensure that, if you don’t own the device you’re using to remotely access, then make sure it is not tainted by any viruses or malware.

Chapter Eight:
Are you ready for ransomware?

- Richard Lun

Ransomware. For cyber criminals, it's an almost-perfect crime. For organizations and individuals, it's an absolute nightmare, and it's just getting started. This chapter will look at the epidemic of ransomware: what is it, how does it get into your systems, and what you can do about it.

The Hostage Crisis

Since the medieval times, criminals have used blackmail to hold hostage the safety and property of others. Ransomware, the latest generation in that long criminal tradition, gains access to a computer system and makes either the system or the data inaccessible, then attempts to extort payment from the owner in return for returning access. Often there is a limited time to pay, after which the data will be permanently lost, and the payment is typically in some kind of untraceable cyber currency such as Bitcoin.

Like other protection rackets, ransomware is a high-profit strategy for criminals. There are multiple steps to monetizing personal data, intellectual property, or other sensitive information that is stolen outright. It is often “fenced” on the Dark Web, a part of the web not accessible through big search engines such as Google, then the buyer has to turn it into a false identity that can be used to fraudulently obtain goods or services. With ransomware, on the other hand, the victim has to pay the criminal directly, the payment happens within hours or days in untraceable currency, and there is no chain of custody to point to the criminals because the data stays on the victim’s system the whole time. It’s simple, anonymous, and fast.

The Inner Workings: In a Nutshell

Most ransomware either locks the interface or encrypts files on a computer or network, sends users a ransom message, and, ideally, releases the interface or decrypts the data after the ransom is paid. However, companies can even have a 20 percent chance of not getting their data back after the ransom is paid. The details of ransomware can and do vary widely, partly to keep attackers ahead of security experts and partly to keep victims off balance and paying.

At this point, there are two major types of ransomware: locker and crypto. Locker ransomware restricts user access to infected systems by locking up the interface or computing resources within the system. It puts up a display page telling victims to pay through credit vouchers purchased from local stores or money transfer services. These days attackers have moved away from locker ransomware because the disabled interface prevents victims from paying in crypto currencies such as Bitcoin, which are faster and less traceable, so better for the recipients. However, experts expect that locker ransomware may regain popularity with attackers because it can affect mobile devices and devices on the "Internet of Things" (IoT). We'll discuss more about IoT in Chapter X.

Crypto ransomware encrypts files on the target system so that the computer is still usable, but users can't access their data. It typically uses strong industry-standard encryption schemes, often with encryption keys that time out, adding urgency to the ransom payment deadline. Crypto ransomware leaves the user interface functioning, so that users can get to the Internet to make ransom payments in cryptocurrency.

Fighting the Fear

The technology behind ransomware is formidable, as developers employ stronger encryption and more tactics to elude detection. Eventually, security technology will catch up, but in the meantime, organizations and individuals need to avoid giving in to fear because that is the ransomware criminal's greatest weapon. Just as the earliest forms of ransomware extorted users with non-existent threats, much of today's ransomware is not as invincible as it seems, which is why attackers keep coming up with scarier tactics for their malware. One of the most brutal is the Petya virus. Not only does the malware attempt to lock the whole hard drive at once rather than slowly encrypting individual files, its user interface is a grinning skull and crossbones made mostly of dollar symbols. Later on in the chapter we will examine preventions, some possible ransomware cures, and steps you should take after the crisis has passed.

Defense

Until the security and privacy community figures out how to stop it, ransomware infections may be inevitable. But the better you handle them when they happen, the less chance you will be plagued by them over and over again. Here are some things you can do to lower the likelihood of a malware attack, and how to handle one if it happens, both during the attack and after.

Building your defenses

Obviously there is no perfect defense against ransomware. If there were, attacks wouldn't have increased by orders of magnitude in the last couple of years. That said, there are steps you can take to reduce the risk. Prevention is great, and it will fend off some percentage of ransomware attacks, but your most important defense against ransomware is mitigation — planning ahead to limit the damage and to help recover quickly from an attack. The key to recovery is to have backups that are complete, up-to-date, disconnected from your systems (either physically or in the cloud), and tested regularly to be sure that you can successfully restore from them. More on backups in Chapter X.

Game Plan

1. Don't panic!
2. Don't turn off systems (that can make things worse), but do isolate them from the network and the internet.

3. Do get online and do your research. At least you can find out what kind of malware you're dealing with, and you may find decryption and other tools available to help restore your systems.
4. Don't let scare tactics push you into paying the ransom before you've explored other options.
5. The ransom decision can be a tough one. Paying ransom encourages this kind of criminal activity. Take the time to find out what you're dealing with and to assess the your options and risks before making the ransom decision. If you have good backups and can recover quickly, you may not need to pay at all.
6. Be an unequal opportunity target with good firewalls, anti-virus, and anti-malware software running.

There are so many yet-to-be-answered questions about ransomware: What tactics will hackers try next? How can we stop it? Is it a breach? When to pay and when not to pay? The only certainty is that criminals will continue to have motive and means to attack for the foreseeable future. The best we can do is to limit their opportunities through user awareness, choosing the best cyber-security we can afford, and through preparation that enables us to respond and recover as efficiently as we can. The more we can keep ransomware from being a fast track to riches, the less criminals will invest in its future.

Chapter Nine:
Do you have a Personal backup plan?

- William Tan

Imagine that one day you wake up and suddenly find your computer blinking a grainy, obscure error message signaling the worst possible event has occurred: drive failure. Everything that you had stored on that device is now in the annals of history. Your pictures, music, videos, financial documents and data are now gone and inaccessible. Data loss.

It can be the consequence of malware, whether by utterly bricking your computer or by destroying the files on the machine. As covered in Chapter X, ransomware has your data as its actual target. Aiming to render each and every bit or byte on the drive into inaccessible, unintelligible computer vomit, ransomware is the malware most people dread to be attacked by.

People are not infallible. A mistaken click on the wrong “download” button, a particularly enticing advertisement, or an “official” email can spell out the infection of the user’s system by malware.

The loss of data can also be caused by software problems or particularly nasty bugs in the software’s code. While bugs are found and patched quickly by major software companies, sometimes the mistakes are left to fester. During this time, the bug can affect plenty of unlucky individuals that satisfy the conditions for the bug to occur.

Yes, company media releases and comments often say that “a small amount of people” were affected. However, out of the large number of users in the world, a “small amount” can still be a lot of people.

Bug effects can simply be annoying, but they can also be gravely serious, putting the entire computer at risk either directly or opening the way for malware to do so. On January 2015, Steam’s Linux variant had a horrible issue that would delete the entire file system if the installation files were moved somewhere else, including the files of everything attached to the computer. Even more recently, Apple’s OS X High Sierra was seen to have a fatal flaw, where anyone and anything could gain administrative access to the computer by simply typing in ‘root’ as a username and not entering a password, which put the affected users (basically anyone that used a Mac) at immediate risk of losing their data to malware.

Of course, that’s just half of it. On the physical side, there’s always the possibility that your device might just get stolen. Pickpockets. Burglars. Robbers. If you leave a device unattended and unsecured, there’s always the remote possibility that it might get lifted. Some criminals might even get the hots for a particularly flashy laptop and break in to retrieve it. While passcodes and encryption do keep the data safe, there’s no stopping the crooks from pawning it off for scrap in the case of phones, tablets, and other mobile devices or simply changing out the drives and tossing out the ones that you had every single thing on into the garbage. Either way, the device (and all the data that was on it) can be considered completely gone.

Then there's the simple accident. A phone or laptop can be lost by pure negligence. A dropped laptop here or there can mean a drive failure and extremely costly data recovery efforts. A spilled glass or mug can result in the loss of the system, as well. Plain old misfortune—something unlucky happens, and the data can be considered as good as lost. Devices can also be destroyed by disaster, like a flood or a fire. Though a lot of people carry their mobile devices out with them when evacuating, larger, bulkier machines, like desktops, sometimes have to stay behind, silently betting on the slim hope that the computer manages to survive. That slim hope is relied upon even when a device is misplaced or forgotten somewhere, not to return until some arduous searching, with everything on it now disappeared.

For too many people, data survives with the help of luck, luck that is fickle and liable to disappear in the blink of an eye. Luck isn't enough.

To ensure that data is safe and secure, you need to back up your data.

The principles backing up is built on is simple: you make a copy of your files somewhere else that's not liable to the problems that might plague your devices, which allows an easy restoration of everything that might be lost. The only thing needed is a method of storage, which can be easily fulfilled by a USB stick, an external hard drive, or even an internal hard drive with special connectors. These smaller storage devices can be carried from place to place and stored in a safe location, making it easy, when something bad does happen, for it to be accessed and plugged back in.

The basic backup is, in essence, selecting everything that's important to you and copying it to your storage device of choice.

It’s very simple, and it saves exactly what you want for later use. If critical files are all that’s important to you, then backing up should be the simplest business in the world.

However, if there are more items that might prove tedious to download it might be more convenient to back those up, too. The problem is that those things might be in the multiple gigabyte range, proving hard to move back and forth due to their immense size. At this point, you might just consider backing up the entire computer system. It covers the entire range of what you might’ve stored on your computer, even things that might have been forgotten or might be important later on.

That’s not as easy as the method mentioned before, but thankfully most operating systems have built-in programs to do the work for you. They back up the computer’s operating system to a drive of sufficient space.

For Windows, there are two options. The first one is more modern but only backups a certain user’s files, requiring possibly time-wasting manual selection of other files for backing up. This is implemented in Windows 10. The second is an older variant, introduced on Windows 7, which essentially takes every file known to the operating system and backs it up, compressing it to save a bit of space.

For Mac OS X, there’s a utility called Time Machine, which automates the backing up procedure. Activating it is as simple as entering the Preferences menu and turning it on with an external or remote drive attached.

For Linux, a more complex utility is used—rsync. This utility is used to synchronize one drive’s contents with another. It’s more complex than Mac OS X’s Time Machine or Windows’

Backup and Restore, but it serves as an excellent tool to backup an entire drive.

Once a backup has been made, care must be taken to store the backup drive in a safe and secure location. While the average enterprising criminal probably wouldn't consider stealing a simple drive due to the possibility of it being encrypted and unintelligible, the drive might still fall victim to a fire, a flood, or simply being mishandled, dropped, or having liquids spilled upon it. That would make every effort already undertaken moot and would cost you a potentially expensive piece of equipment.

Lastly, backups need to be made whenever a significant change is made to the device or when something important is added to it. Significance and importance are at the judgment of the user, but it will maximize the safety of the files on the device, allowing those things to be recovered in the event of an emergency.

When something goes wrong, it's always a relief to have a copy of everything important on hand. Having only a single copy of everything makes it massively liable you'll suffer lots of anguish when everything disappears due to misfortune. Don't take a chance. Back up.

Chapter Ten:
Don’t let a phishing scam reel you in

- Richard Lun

Phishing is one of the easiest forms of cyber-attack for a criminal to carry out. A basic phishing attack attempts to trick the target into doing what the scammer wants. That might be handing over passwords to make it easier to hack your system? or altering bank details so that payments go to criminals instead of the correct account.

That data can be as simple as an email address and password, to financial data such as credit card details or online banking credentials or even personal data such as date of birth, address and a social security number.

How Does a Phishing Attack Work?

A basic phishing attack attempts to trick a user into entering personal details or other confidential information, and email is the most common method of performing these attacks.

Scams vary in their targets - some are aiming at unwary consumers. Here, their email subject line will be designed to catch your eye - common phishing campaign techniques include offers of prizes won in fake competitions such as lotteries or contests by retailers offering a ‘winning voucher’.

In this example, in order to ‘win’ the prize, you are asked to enter details such as name, date of birth, address and bank details in order to claim. Obviously, there’s no prize and all you’ve done is put their personal details into the hands of hackers.

Why is it Called Phishing?

The overall term for these scams, phishing, is a modified version of ‘fishing’ except in this instance the fisherman is the cyber attacker and they’re trying to catch you and reel you in with their sneaky email lure.

Types of Phishing

The least sophisticated type of phishing attack is one where generic messages are mass-mailed to millions of users. These are the ‘URGENT message from your bank’ and ‘you’ve won the lottery’ messages which look to panic victims into making an error or blind them with greed.

Schemes of this sort are so basic that there’s often not even a fake webpage involved - victims are often just told to respond to the attacker via email. Sometimes emails might play on the pure curiosity of the victim, simply appearing as blank message with a malicious attachment to download.

Spear phishing is more advanced than a regular phishing message and aims at specific groups or even particular individuals. Instead of vague messages being sent, criminals design them to target anything from a specific organization, to a department within that organization or even an individual in order to ensure the greatest chance that the email is read and the scam is fallen for.

With billions of people around the world using social media services such as Facebook, LinkedIn and Twitter, attackers are no longer restricted to use one means of sending messages to victims. Some social media phishing attacks are simple and easy to spot: a Twitter bot might send you a private message containing a link which leads to something bad such as malware or maybe even a fake request for payment details.

Spotting Phishing

The whole point of attackers carrying out phishing attacks is to use deception in order to trick victims into compromising themselves. While at its heart phishing remains one of the most basic forms of cyber attack, the simple fact of the matter is that it works.

However, there are some key giveaways in less advanced phishers which can make it obvious to spot an attack.

Poor Spelling and Grammar

Many of the less professional phishing operators still make basic errors in their messages - notably when it comes to spelling and grammar.

It’s common for attackers to use a service like Google Translate to translate the text from their own first language, but despite the popularity of these service they still struggles to make messages sound natural.

A Strange Sender Address

Always keep an eye on the sender address to ensure that the message is legitimately from who it says it is, even if it may seem legitimate.

The Message is Too Good to be True

Congratulations! You've just won the lottery - now just provide us with all of your personal information including your bank details to claim the prize.

If it seems too good to be true, it probably is.

The future of phishing

For some people, it might seem strange that there are people out there who can easily fall for a 'You've won the lottery' or 'We're your bank, please enter your details here'.But there are billions of people in the world who don't regularly use the internet. Unfortunately, criminals are there looking to scam and deceive people and it's easiest to do it to people who are naive or overly trusting. And the low cost of phishing campaigns and the extremely low chances of scammers getting caught means it remains a very attractive option for fraudsters.Because of this, phishing will continue as cyber criminals profit from dropping malware in the laziest way possible. But it can and hopefully will be stopped simply by knowing what to look for.

Chapter Eleven:
Shop Safe Online, Even on Black Friday

- Monica Saraf

No matter who you are or what you're buying, you might find it very convenient being able to sit at home and shop off the internet. But this fun and easy way to get what you need can also be problematic. It is not only addicting, but also can be dangerous if you do not shop on secure sites.

Most websites and companies have highly secure and updated websites in order to ensure that their users' accounts and information are all safe. Usually, if it is safe, it will use the HTTPS Protocol mentioned earlier. On a normal, insecure website, it will only be http:// meaning that it is not a secure website. These are not trustworthy and it is far better *not* to use them, especially for shopping purposes.

Some unsecured websites use a keylogger meaning that they can log every key stroke that you make. These usually end up saving passwords or credit card information and this can lead to fraud. Many people also get fake emails and ads that lead them to give up their personal information. If you're using a website that is already trust worthy, these issues usually don't happen.

There are times when there are security breaches of big companies such as Target. In 2013, there was a major breach that affected over 41 million customers according to USA Today. Since then, multiple other companies have been attacked. There are many ways to stay safe but keep in mind that it does not mean that you will always be safe. In addition to that, it doesn't mean you should never shop. One way to be safe is this: Instead of entering you entire card number at once, jump around in between numbers and fill out other sections of the checkout form. This way, the keylogger will collect random numbers instead of capturing all of your information in order.

Many people have accounts with companies that they frequently shop from. These accounts however might not have very secure passwords. This is one of the major reasons people get hacked, the lack of a strong password. As stated in the chapter about passwords, it is important that a password contains some upper-case and lower-case letters, at least one symbol or character, and at least one or more numbers. This makes it much harder to crack. However, it must *also* be longer than 8 characters. Some of the most common passwords are just "password" or "password123." Remember to never use your name in your password. A great tip is to also create a passphrase. For example, "I like pie!" can become "1Lik3Pi3!" It is easy to remember and strong.

Many companies will ask you to save your credit card number to your account. Although this may seem convenient, it is best to pull your card out each time that you pay online. Saving your card number makes it more vulnerable to being used for fraud.

It is common for browsers to track search data so it can fill different websites with ads and because of places you sign up or enter an email. You might get phishing emails. This is where a person uses your search history or information they know in order to lure you to a website. This link can lead you to eventually give any personal information that can lead to identity theft or you credit card information being stolen. This doesn't only mean emails, it can include phone calls, apps, and other means of shopping.

One more important thing to beware of is shopping on free Wi-Fi that you do not own. When in coffee shops or other places with free Wi-Fi, it is best not to use them for online shopping. Anyone can connect to the network and if you do not have a secure computer, they can take some personal information, too. It is better to use your own personal hotspot on your phone. Using gift cards are a great way of not having to enter credit card and other sensitive information.

On top of all of this, it is highly important that you protect your laptop with an antivirus to ensure that people cannot hack *your* computer. Even if you have a secure password and make sure you do not give out too much information, you also need to make sure that you do not leave your computer exposed to hackers and the outside world. Protect your internet and your devices, as well, with strong passwords.

Shopping is a pastime that many people do throughout the year. This does not mean that you should disregard these tips and advice to staying safe online and keeping your credentials safe all the time. Black Friday and Cyber Monday is the time of the year when websites and online shopping sites are most targeted by hackers because people try to buy so much stuff and do not realize that they are not shopping safely.

Do not forget to follow these tips and ensure that you and your money is safe. Just the way you wouldn't give a stranger on the street your address, make sure you do the same for hackers and people online. Check for secure sites and try to use websites of known companies. Use strong passwords and a variety of them for your websites, make sure to write them down or find a way to remember them. Pay attention to whether calls and emails are valid or are phishing scams. Do not use free Wi-Fi wherever you are because sometimes there can be hackers on the network, trying to steal your information. Instead, use your own hotspot or Wi-Fi network. Use gift cards! They're a great and convenient way to keep your information safe. Last, but definitely not least, make sure that you protect your computer itself. These tips may seem simple but they can go a long way. Make sure to keep your information safe and away from hackers, especially while shopping online.

Chapter Twelve:
Securing New Devices in an IoT World

- Abhishek Allamsetty

In recent years, the dramatic growth of Internet-connected devices has transformed how people, households, and businesses interact with each other and the physical world. Connected devices as diverse as security cameras, digital video recorders, printers, wearable devices, smart light bulbs, and Internet connected-appliances have come to be collectively known as the Internet of Things (IoT). IoT devices represent a growing constellation of gadgets and tools designed to collect, exchange, and process information over the Internet to furnish their users with convenient access to an array of services and information.

Unfortunately, IoT devices have also become an increasingly attractive target for criminals. To attack IoT devices, cyber criminals often probe the devices for security vulnerabilities and then install malicious software (malware) to surreptitiously control the device, damage the device, gain unauthorized access to the data on the device, and/or otherwise affect the device's operation without permission. Installed malware may not only compromise the operation and information security of the infected IoT device, but can also provide hackers a conduit for penetrating other electronic devices on the same network. Unless appropriate precautions are taken, malware can quickly spread across networks of IoT devices without a user opening a file, clicking on a link, or doing anything other than turning on an Internet-connected device.

Although malware has existed for many years, the burgeoning popularity of IoT devices has significantly increased the number of Internet-accessible targets that may be exploited; the advent of a new generation of malware dedicated to exploiting IoT devices is largely to blame. For instance, Dyn, a company that monitors and routes Internet traffic, was a victim of a distributed denial of service (DDoS) attack in October 2016 that was launched from thousands of IoT devices infected with the Mirai malware. Unlike more conventional forms of malware, the Mirai code was written specifically to allow a remote user to infect IoT devices and use them as an army of machines capable of transmitting internet traffic without the device owners' knowledge. On October 21, 2016, thousands of Mirai-infected IoT devices were directed to unleash a torrent of traffic that overwhelmed Dyn's systems. Many high-traffic websites that used Dyn's Internet services (for example, Paypal, Twitter, Netflix, and CNN) were rendered wholly or sporadically inaccessible for substantial periods of the day.

The interruption of Internet service associated with the Dyn disruption underscores the significant, systemic harm that may be caused by malware dedicated to exploiting the security vulnerabilities of IoT devices. To help prevent and/or mitigate the impact of future crimes involving IoT devices, the Criminal Division's Cybersecurity Unit and the Consumer Technology Association are providing the following suggestions to owners of IoT devices. While these measures are intended specifically for IoT devices, many are more generally applicable and are also sound practices to institute when using most Internet-connected devices.

There are a number of precautions you may take to shield your IoT devices from cyber intrusions and prevent them from being commandeered to launch cyber attacks. The following measures will allow you to enjoy your IoT devices while also better securing your IoT devices against malware and safeguarding your data and privacy.

Research: If you decide to purchase an IoT device, do your research to ensure that the manufacturer takes cybersecurity seriously. For instance, if the device uses a password, make sure the IoT device allows you to change its password. (Some devices come with default passwords that cannot be changed.) Also, consider whether you are confident that the manufacturer will deliver timely security updates to combat new malware and security threats. Having a device that is configured to easily download security updates increases the chance that the device will be using the latest protections. To keep cyber criminals out of your home, business, car, or anywhere else you may choose to use an IoT device, it is important to make security features part of the considerations you weigh when buying an IoT device.

Immediately secure your device: An IoT device that is not properly secured may be exploited within minutes of being connected to the Internet. With this in mind, do not let the excitement of acquiring a new IoT device distract you from securing it before putting it to use. Before installing your new device, visit the manufacturer’s website and download any new security patches for known vulnerabilities. Also, without exception, immediately reset any default passwords with secure passwords.

Safe passwords: Proper password security is critical to information security, regardless of whether that password protects an IoT device, desktop computer, router, Wi-Fi connection, or online account. Passwords should be difficult to guess, avoid incorporating information about you that is readily available on the Internet (for example, through social media), and be unique to each secured device or router. To make passwords complex enough to thwart password-cracking software, use a combination of upper- and lower-case letters, numbers, and symbols. To help keep track of multiple passwords, consider using a password-management program that can maintain and safeguard your passwords.

Software updates: Your IoT device has software embedded on it called firmware that may be susceptible to exploitation if not regularly updated and patched. To keep your IoT devices secure, you should register each of your devices for any automated firmware updates that are offered by the manufacturer. If automatic updates are not available, it is well worth the effort to periodically check the manufacturer website for firmware updates and device patches to ensure your IoT devices are current and running the latest and most secure firmware updates. Only install updates from known, reputable sites.

Disconnect insecure IoT devices: Even some relatively new IoT devices may have outdated security and may not allow you to change administrator passwords or update the device’s firmware. If your IoT devices cannot, at a minimum, be updated with strong passwords or receive security patches, they may be vulnerable to malware infection. You should consider disconnecting such devices and replacing them with newer, secure models.

Turn off IoT devices when they aren't in use: The malware used in some recent cyber attacks is stored in memory and can often be erased with a power cycle, that is by turning the device off then back on. Accordingly, as a rule of thumb, you should always turn off any smart devices when they are not in use, such as video cameras and devices with microphones that can be compromised and used to invade your privacy. IoT devices that are in regular use (for example, thermostats) should be restarted periodically.

Protect your routers and Wi-Fi networks: To keep your IoT devices secure, it is also important to secure the home routers and Wi-Fi networks to which they regularly connect. Use your home wireless router's built-in firewall (that is, log in to the router per the manufacturer's instructions and confirm that the firewall feature is enabled; ports 25, 80, and 443 are sufficient for most needs). Also, use secure password practices for managing your router (described above) and consider using media access control (MAC) address filtering to limit the devices able to access your network. Disabling the Universal Plug and Play (UPnP) on your router can also enhance the security of your network, though it may cause problems for some applications, such as media servers and players. You should only enable UPnP if necessary.

Avoid a single point of failure: One vulnerable IoT device may allow an intruder to penetrate your entire network and access other devices on your network. To minimize the potential harm caused by a single compromised device, keep passwords complex and unique for each device and router. Further, most routers allow you to segment your home network so that IoT devices do not have access to the entire network. For instance, you may set up one network for your computers, printers, and other computing devices, a second network for Internet connected-appliances, and a third network for mobile devices. To keep your visitors from infecting your network with malware, many routers also offer guest networking that shields your devices from those of your guests. Consult your router's manual for further direction. The more you segment your networks, the harder it will be for hackers to access your devices and information.

Keep up with mobile security: When remotely checking your IoT devices from a smartphone or tablet, it is generally good practice to avoid using public Wi-Fi networks that are not password protected. Insecure connections can make your IoT device vulnerable to hacking. However, if you must use an unsecured, public Wi-Fi network (for example, at an airport, café, or hotel), you should consider using your smartphone or tablet to initiate a virtual private network (VPN) connection to your local network before opening your IoT-connected applications. Some newer smartphones or tablets have preloaded VPN software, while many others support downloadable VPN applications. Although not foolproof, a VPN connection creates a secure tunnel to your local network that will make it difficult for anyone to eavesdrop on such sessions and acquire login credentials for your IoT devices.

Try using anti-virus programs: These products are capable of protecting IoT devices in much the same manner as antivirus software can protect laptop and desktop computers. They can detect abnormal behavior on any device communicating on your network, including a tablet, digital video recorder, or Internet-connected refrigerator. These relatively new products are typically hardware devices that connect to your home network, but software-only versions of this capability are also available. As IoT devices proliferate, so too will software and hardware security products that may help secure IoT devices. Keep abreast of such developments and consider adopting them.

Get some help when you need it: You may not feel comfortable installing, configuring and maintaining the security of your IoT devices, routers, and Wi-Fi networks by yourself. Turning off features like UPnP, configuring a firewall, or segmenting your network, may seem daunting. If you feel uncomfortable, consider asking more technology-proficient friends or family to provide help, or paying to have your IoT devices and routers properly installed and secured. Investing the time and effort at the outset can prevent difficulties later.

How do you know if you've already been infected: It can be difficult to determine whether your IoT device is infected by the Mirai malware or some other IoT-targeting malware. An infected IoT device may still function correctly but suffer occasionally from sluggish performance as a result of surreptitiously engaging in botnet activity while performing its regular functions. Some free online resources can help you determine whether your IoT devices are susceptible to being accessed from outside your network by Mirai or similar malware. However, exercise due caution when using such resources to ensure they are not malware disguised as security software. Be particularly careful if they are not provided by well-known, reputable sources and require you to download and install programs on your computer. If you determine that your IoT device has been compromised by Mirai or similar malware, turn it off and then on again after several seconds to purge the device's memory, as instructed above. Malware, such as Mirai, often resides in an IoT device memory, so purging the memory will remove the malware. If your device was compromised because of poor password management, change your password and follow good password management practices as described above before reconnecting it to the Internet.

CyberSmart Now

Students helping students to become smarter online.