Cybersecurity Informational Guide

Gideon Russ

4/12/2019

Table of Contents

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

-Sun Tzu

Introduction

The march of technology is fast, but almost all technology has inherent flaws in its early stages. But technology doesn't slow down, it doesn't wait for us to solve its problems before it moves on. The internet is certainly humanity’s greatest invention to date. We have access to all of the worlds intelligence with just the stroke of the fingertip on a device small enough to fit in our pockets yet is stronger than the computers used to put a man on the moon. The internet is a blessing to humanity, but every technology has its flaws, and the flaw of the internet is cyber security.

If you think that identity theft is something that happens to other people, then you are wrong. 60 million americans have been the victims of identity theft (Symantec). Cyber attacks cost the global economy 600 billion dollars per year (Financial Observer). In 2018, Japan’s minister of cybersecurity admitted that he had never used a computer (NYtimes). Cyber security illiteracy is rampant as of lately, evidenced by the fact that 95% of data breaches are caused by human error (Cybint). People may believe that only Russia, China, and North Korea are to blame, and they would be mostly correct. However 100 different countries have cyber warfare units (Gale) and many of which commit cybercrimes, albeit Russia, China and North Korea do contribute a disproportionate amount relative to everyone else (CSIS). I could keep blurting out scary numbers and facts, or I could start to teach you how to make sure you’re not one of those poor guys that get hacked by some ethically challenged burnout in his mom’s basement, or a Korean cyber spy.

Trust

Trust is imperative in the realm of cyber security. If you gain someone's trust you can ask them for information that, to the inexperienced eye, seems completely normal. Or you could ask them to download a file that could be any number of malicious programs. If you gain control of someone's trust, you gain control of that person.

Social engineers are people who try to gain trust in order to get personal information, intellectual property, or access to a protected network. They have many tactics and are very clever. A lot of times, social engineers use emails, texts, or phone calls to get confidential information, trick you into downloading malware, or just scamming you out of your money. They pretend to be your boss, the HR or IT (Information Technology) desk, a charity, or even a deposed nigerian prince.

Detecting a social engineer can be tricky, but there are a couple telltale signs of one. Most scammers will demand money in exchange for something else, like a lot of money later on, debt cancellation, or anything that would make you pay attention (SEC). A good rule of thumb is that if it's too good to be true, it probably is. A misspelled email address or website address indicates fraud (i.e. Gooogle.com). Poor grammar and spelling errors are a sign that the threat actor is unfamiliar with the english language, and if they claim that they work for the government, then that's certainly more than a little suspicious (Citizens Advice). Authority and trust is frequently abused by scammers, they claim to be your boss, the FBI, IRS, or CIA when they're actually not (Kaspersky). A fake sense of urgency or a deadline may be used to get you to avoid thinking rationally (Strickland). Also, if they claim that they've tried to reach you before but couldn't, then that's a red flag. If they ask for your password, personal information, company information or anything else that you wouldn't want a stranger to know, then don't reply. If a website or service you use asks you to log into your account to verify your identity and they provide a link to their site, don't click it, log onto the site as you normally would through your search engine. Also if someone claiming to be your bank provides you with a phone number to contact, you should look for the real phone number online and call them (Citizens Advice).

Once you’ve detected a scam, there are many ways to counter them. The most important thing is to not do what they tell you to do. A lot of people like to play with a scammer and waste their time, but that could put you or your company in undue risk. Do not click on any links and do not reply. If the scam was sent to your work email, the first thing to do is to ask the alleged sender in person if they sent the email (If you received an email from someone claiming to be your boss asking for company information). If not, then tell the IT desk and make your coworkers aware of the funny business. If you open an email and a file automatically downloads, you must stop the download as soon as possible (Hold down the power button or pull the plug), then you should contact the IT department (if at work) or contact tech support (if at home). If a suspicious file is able to download before you can stop it then run a virus scan and contact the IT staff or tech support immediately (Jennex). The bottom line is to treat every email, text, or phone call with skepticism, verify the authenticity of every electronic message, and contact someone more qualified in IT when in doubt.

Social Media

There are 3.397 billion active social media users, and the main point of social media is to connect with like minded people (Slideshare). However, it often times serves as the base for some unsavory individuals. Like this book covered earlier, techniques for trust are of utmost importance, and are universally applicable. You have an obligation as an internet citizen to be polite to everyone on social media, no matter how much you hate them. If you are a knob, then you could face the deletion of your account or in extreme cases you could be vulnerable to blackmail. But in some cases you could make enemies, and enemies on the internet can be brutal. Just about every social media network will collect your data, and if you're not ok with that then you're not allowed to use the site. Some mobile apps also track the location of users. This feature can be turned off, but turning it off is only necessary if you have a reason that one or more users shouldn't know where you are. So it's personal preference whether or not to leave it on or turn it off.

If you use social media, odds are you've dealt with an unpleasant encounter with an unsavory person. You may have to deal with stalkers, creeps and sociopaths. The only accurate way to describe these people is to call them social engineers. Social engineers like these always want something; money, personal information, power, or anything really. Social engineers you find on social media are no different then social engineers that use emails or phone calls (SANS). They might show you a picture of your house along with a threat, and they might try blackmail. A fearmongerer can be awful, but if they are demanding something that's rightfully yours, then they are in no position to take it from you. If you find yourself in their crosshairs then the most important thing is to not give in, and notify law enforcement.   Challenges like these on social media are quite common. The challenges and tactics used on social media are applicable to online games and dating sites. However Social engineers will have significantly less leverage on online games but will have much more leverage on dating sites due to the nature of these apps.

Software Optimization

You should regularly update your operating system to keep it running smoothly. For example: The ransomware *WannaCry* made it's first appearance in May 2017 (Cnet). Although Microsoft released an update that removed the vulnerability a day after the attack, the computer still had to update. Many people see windows updates as a nuisance, but they serve a very important purpose in keeping your system running smoothly and secure (UNC).

You should use a Virtual Private Network (VPN). VPNs encrypt your network data so that anybody listening in on your traffic cannot actually read the information, therefore enhancing the security (Symantec). Free VPNs are sufficient but tend to slow down your internet connection. Paid VPNs are faster and more secure than free ones at the cost of a couple dollars a month. Really it's just your personal preference. You should also use antivirus software. Be cautious of free antivirus software, you should use a credible, well reviewed antivirus like Norton or Kaspersky. Keep your Antivirus up to date and regularly scan your computer for viruses. You can also program the antivirus to run a scan at a set interval, be it daily, or weekly. You could also set it to scan at night when you're not using the computer.

End User License Agreement (EULA)

Odds are, you don’t actually read the novel of a contract when you sign up for Facebook or Google when you check the box that says you did. Don’t worry, most EULAs are very similar. Just about every website, manufacturer, social network or cookbook will collect your data and sell it to advertisers. Facebook is one of the most notorious businesses that collect data. They have collected the most personal data compared to any other company, 300 petabytes to be exact (Linkedin). That amount of data is equivalent to about 16 million copies of the game *Fortnite* or about one hundred years worth of 4K movies (Omnicalculator). To help you put that number into perspective, the average computer has a storage capacity of just one terabyte (as of 2019), and a petabyte is equivalent to 1000 terabytes. Their EULA blatantly states that they collect a lot of data (Techcrunch). What they do with this data is sell it to advertisers, making $40 billion a year (Investopedia). Mark Zuckerberg even admitted to the US congress that Facebook collected data and sold it to advertisers (Gale). However the only reason Facebook is free is because the make money from advertisers. This strongly relates to the old saying “There ain’t no such thing as a free lunch” meaning even if you didn’t pay for your lunch, someone paid for you to get the lunch. Or in this case, advertisers paid for you to have Facebook. Don’t worry, because there’s often an option to disable data collection on most apps. If there isn’t, then that means data collection is the price you pay for using their service. There are certain rights that cannot be signed away when you check that box, even if that's just what facebook wants you to think. If a company collects your data, it is expected that they keep that data safe and secure

Passwords

Almost every website you use will be bound to a user account, and every user account has a username and password. You should try to follow some of these practices. Don’t use the same password for everything, because if one account is compromised, the rest are soon to follow. If you can’t remember all the passwords you have, use a password manager, or write them down somewhere no one else can find. If any of the above options aren’t appealing, just use one password for everything that isn’t as important to keep secure (Email, Google, Reddit, etc.) and use different passwords for really important places (Banking, Government secrets, etc.)

You should use strong passwords. 1234, admin, password are all easy to crack. Dictionary words are better, but not best. A long sentence with special characters, intentionally misspelled words, mixed with numbers is extremely secure but makes it far harder to remember, so you’ll definitely need to write it down somewhere. However, probably the best password practice is to make a long sentence (Nist). A long sentence, also known as a passphrase, is sufficient as most hackers trying to access your accounts that don’t know your password will use brute force software. Brute force software attempts to learn a password by just entering every possible combination of characters until it gets it right (Kaspersky). The more characters you use, the longer it takes a hacker to crack your password. The other benefit of using a passphrase is that it's a lot easier to remember.

The Hidden Web

The Deep Web is everywhere on the internet that cannot be accessed with a traditional search engine (Symantec). It’s a common buzzword thrown around by news outlets that is meant to be synonymous with hacking and cybercrime and they typically have no idea what they’re talking about. A lot of things are found on the deep web such as password protected websites, and websites that are not available to the public because they are incomplete.

All of the illegal and potentially dangerous stuff that everybody talks about is found on the dark web and is intentionally hidden. Such as social networks used by citizens living under a repressive regime, as well as illegal goods, illegal services, and illicit software. For your own safety and the safety of those you love, do not attempt to access the dark web unless you have made precautions to keep yourself safe. You would need Tor (the search engine) and Tails (an operating system). Although Tor is extremely private and secure, it is not impenetrable. I do not condone unethical or illegal activities. Access the Dark web at your own risk.

Be Aware

Be aware of anomalies in your phones and computers such as unauthorized downloads on your phone or computer (A file starts to download even though you never intentionally commenced the download). Unauthorized background services (Press ctrl+Alt+Delete to open task manager, then click on services and look around at the services and their descriptions). Texts from unknown sources that have bad grammar, misspelling, and non latin characters. These are signs that someone’s trying to scam you. Do not respond, and do not click on any links they send you. If its a text something along the lines of “New phone, who’s this” then they should be fine.

You should also know how to counter certain types of cyber attacks. If your computer is acting abnormally you should run a virus scan. Windows has a pre-installed virus scanner and most antivirus software comes with a better version of virus scanners. Look out for emails that you don’t remember sending, emails from an unknown source, or suspicious links, PDFs, or executables. If your email account is sending emails on its own, then that's fairly good evidence that the account has been compromised. If an email comes from an unknown source and manages to make it through the spam filter, then don’t open it. If an email from an unknown source contains a link, do not click on it.

Security of your bank account is definitely very important. If there are any anomalies in your bank account, you should call your bank immediately to get it sorted out. Be aware of unauthorized access to your account, unauthorized money transfer of any kind, or alerts from your bank. But if you get an email of phone call from your bank, make sure they are actually from your bank before giving them any information.

Many new credit cards have an RFID (Radio-Frequency Identification) chip on them. RFID is the same technology used on metrocards and microchips for your pets. RFID can be detected at a range of about 4 feet and can be read through clothing. This means that anybody with an $80 RFID wand can walk past you and get your credit card information (NPR). This can be countered by getting a wallet with an RFID blocker, or just a regular wallet with steel implants. Many new wallets have RFID blockers and they typically cost no more than a regular wallet.

Following your work’s security policy is of utmost importance as depending on where you work you could compromise intellectual property, personal data of you, your coworkers or clients, work time, company finances, and in extreme cases you could put your own safety at risk. Lock or log off of your computer when you leave it. Report anything suspicious to your superiors. Never plug an unfamiliar usb into a work computer. For example the Stuxnet worm that is believed to be written by intelligence agencies of Israel and the United states was deployed on a usb thumb drive on an unknown date and was discovered in august of 2010 (CSOonline). Stuxnet was a program that did no harm to regular computers or networks but targeted very specific systems used in the production of enriched uranium. Stuxnet sabotaged Iranian nuclear plants and although nobody knows how it first spread to Iran’s Natanz nuclear plant, but it is speculated that it was transferred from an unauthorized usb thumb drive was plugged into a company computer by an employee.

Although cybercrime is rampant and extremely damaging, nobody but you can keep you safe. The FBI has limited resources and must allocate such resources accordingly. That means that while the FBI will protect businesses, they will normally not protect regular people, and even then, due to the lack of universal law, the FBI often has to rely on local governments for jurisdiction to enforce the anti-hacking laws of that country. There is no UN legislation regarding cybercrime, therefore making it completely legal in some countries and allowing the operation of state sponsored hackers.

Fancy Bear

Fancy Bear is a hacking group sponsored by the Russian government. They've done their fair share of infamous cyber attacks including hacking the DNC in 2016 (Arstechnica), hacking Ukrainian field artillery (Interfax), and hacking the German and French elections in 2016-2017 (London South East)(CBSnews).

Bureau 121 (The Guardians of Peace)

Bureau 121 is a north Korean hacking group responsible for the attack on Sony Pictures following the release of *The Interview* that intimidated sony to downplay its release and sony employees also had personal information leaked to the public (CNN). Bureau 121 also calls themselves the Guardians of peace.

The Shadow Brokers

A group of hackers that hacked the NSA and made off with several different classified cyber weapons including the aforementioned Stuxnet worm. Then they sold copies of the weapons on Twitter. There are unconfirmed theories that they are linked to Russia (BBC).

Syrian Electronic Army (SEA)

The SEA is a hacker group run by the Syrian government to investigate and remove web content that is critical to the Assad regime, they also work to find the locations of Syrian rebels (BBC).

Equation Group

The equation group is believed to be the offensive branch of the NSA. They were involved in the creation of Stuxnet. They take great care to remain undetected, evidenced by their reliance on powerful encryption and self-terminating malware (Arstechnica).

Conclusion

This document was meant to help common people improve their knowledge of cyber security tactics and challenges. This is by no means a substitute for a training course in cyber security, but rather is meant to create interest in the topic and a small summary of cyber security. If you want to learn more about cyber security, you should check out the courses I used to learn about it. At the time of writing, I am enrolled in Cisco's networking academy which offers several courses in IT including networking, programing, and of course cyber security. The courses can be found at https://www.netacad.com/ . Please note that most of these courses are not free, and most of them also require classroom instruction.

I entered Cisco networking academy my junior year because I wanted a class that wasn't based in lectures and homework, but learning through experience. What I got was a class based on even more lectures, and even more homework with some learning through experience. Although this was not exactly what I hoped, I enjoyed the program, and decided that I wanted to dedicate my life to networking, but my teacher had a different idea. He proceeded to tell us about the huge lack of cyber security professionals and the massive vulnerability to attacks. The job security, combined with a large median salary and an interesting career path is what inspired me to pursue cyber security. All of this decision making happened during my junior year, which can only be described as hellish. Waking up at five in the morning for JAGS model UN and getting home from work at eleven at night only to have loads of homework to work on was extremely stressful. My tense life was further exacerbated by the suicide of a close friend and a school shooting at the middle school. Although junior year was difficult, I gained resilience, and an improved work ethic from the hard work.

In addition to taking Cisco networking and cyber security, I am also in the Jackson Academy for Global Studies (JAGS). The focus of JAGS is to make students globally minded through a rigorous curriculum dedicated to globalism and service. In order to complete JAGS and receive a JAGS endorsement on my diploma I must accumulate a total of 80 service hours, complete the JAGS 4 year plan of courses which includes 4 years of a world language, and I must complete a capstone project. The capstone project is meant to be the culmination of all of my JAGS career. Its supposed to reflect everything I've learned throughout high school and JAGS. Cybercrime is a global problem, and I'm going to study cyber security in college with ambitions of becoming a security architect. I wanted to combine my passion for cyber security with the globalist mindset I found in JAGS, So I decided to make a simple guide for common people to keep their data secure, which is manifested in this very document. I personally thank you for taking the time to read through this document, as I've put so much hard work into it. Everything I learned in high school has been reflected in this document. From my time in cisco teaching me the meat and bones of networking and cybersecurity, to my time in english and model UN teaching me how to write a meaningful paper. But most of all this paper was sculpted by the mindset I got from JAGS, a mindset of compassion, globalism, and the drive to fight in my own way to improve the world.

Cybercrime is detrimental to the global community, with technological superpowers committing acts of espionage on other countries. Hacker groups are stealing intellectual property and financial assets. Some state sponsored hackers even sabotage democracy itself. Countries are waging cyber warfare against each other with no end in sight, and it's raising tensions, damaging relationships and making the world a more dangerous place. With this document I plan on removing vulnerable links from networks therefore making hacking more difficult and less logical. The hope of this project is to make 1 less person the victim of cybercrime, therefore reducing the rate of cybercrime, reducing the financial cost of cyber attacks, and reducing cyber crime overall. Cybercrime can be greatly diminished through stronger security technology, more security literacy, international treaties and more comprehensive policies. But the benefits would be huge. We'd see improved foreign relations as a result of greater trust between nations, international business would flourish, and we'd also get faster, cheaper internet. Overall, less cybercrime will make the world a better place, and by reading this guide and following these guidelines, you will contribute to this secure utopia.

Works Cited

Usa.kaspersky.com, usa.kaspersky.com/resource-center/definitions/spear-phishing.

The Internet Classics Archive | The Art of War by Sun Tzu, classics.mit.edu/Tzu/artwar.html.

Kaspersky.com, www.kaspersky.com/resource-center/definitions/brute-force-attack.

"'NSA Malware' Released by Shadow Brokers Hacker Group." *BBC News*, BBC, 10 Apr. 2017, www.bbc.com/news/technology-39553241.

"10 Cyber Security Facts and Statistics for 2018." *Official Site*, us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html.

"The 7 Most Data-Rich Companies In The World?" *LinkedIn*, www.linkedin.com/pulse/7-most-data-rich-companies-world-bernard-marr.

"Advance Fee Fraud." *Investor.gov*, www.investor.gov/protect-your-investments/fraud/types-fraud/advance-fee-fraud.

Cbs/ap. "Russia-Linked Hackers Targeting French Election, Security Firm Says." *CBS News*, CBS Interactive, 25 Apr. 2017, www.cbsnews.com/news/russia-hacked-french-election-trend-micro-report-fancy-bear-pawn-storm/.

Constine, Josh, and Josh Constine. "Facebook Rewrites Terms of Service, Clarifying Device Data Collection." *TechCrunch*, TechCrunch, 4 Apr. 2018, techcrunch.com/2018/04/04/facebook-terms-of-service/.

DataReportal

Follow. “Digital 2018 Q4 Global Digital Statshot (October 2018) (v2).” *LinkedIn SlideShare*, 26 Oct. 2018, www.slideshare.net/DataReportal/digital-2018-q4-global-digital-statshot-october-2018-v2.

Esser, Mark. “Easy Ways to Build a Better P@$5w0rd.” *NIST*, 7 June 2018, www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd.

Fowler, Sarah. “Who Is the Syrian Electronic Army?” *BBC News*, BBC, 25 Apr. 2013, www.bbc.com/news/world-middle-east-22287326.

Fruhlinger, Josh. “What Is Stuxnet, Who Created It and How Does It Work?” *CSO Online*, CSO, 22 Aug. 2017, www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

Gallagher, Sean. “Windows Zero-Day Exploited by Same Group behind DNC Hack.” *Ars Technica*, 2 Nov. 2016, arstechnica.com/information-technology/2016/11/windows-zero-day-exploited-by-same-group-behind-dnc-hack/.

Goodin, Dan. “New Smoking Gun Further Ties NSA to Omnipotent ‘Equation Group’ Hackers.” *Ars Technica*, 11 Mar. 2015, arstechnica.com/information-technology/2015/03/new-smoking-gun-further-ties-nsa-to-omnipotent-equation-group-hackers/.

Haponiuk, Bogna. “Video File Size Calculator (by Format).” *Omni*, Omni Calculator, 24 Oct. 2018, www.omnicalculator.com/other/video-size.

“Help &amp; Support.” *Help Support*, help.unc.edu/help/what-is-windows-update-and-why-should-i-run-it/.

“How to Safely Access the Deep and Dark Webs.” *Official Site*, us.norton.com/internetsecurity-how-to-how-can-i-access-the-deep-web.html.

Interfax-Ukraine. “Defense Ministry Denies Reports of Alleged Artillery Losses Because of Russian Hackers' Break into Software.” *Interfax*, Interfax-Ukraine, 6 Jan. 2017, en.interfax.com.ua/news/general/395186.html.

Milkovich, Devon. “13 Alarming Cyber Security Facts and Stats | Cybint.” *Cybint Solutions*, Devon Milkovich Https://Www.cybintsolutions.com/Wp-Content/Uploads/2019/01/1500px_cybint_logo_CYMK_-e1548863169367.Png, 17 Jan. 2019, www.cybintsolutions.com/cyber-security-facts-stats/.

“Russian Hackers Suspected In Cyberattack On German Parliament.” *Russian Hackers Suspected In Cyberattack On German Parliament - Finance News - London South East*, 19 June 2015, www.lse.co.uk/AllNews.asp?code=kwdwehme&headline=Russian_Hackers_Suspected_In_Cyberattack_On_German_Parliament.

Sharma, Rakesh. “How Does Facebook Make Money?” *Investopedia*, Investopedia, 12 Mar. 2019, www.investopedia.com/ask/answers/120114/how-does-facebook-fb-make-money.asp.

Sherr, Ian. “WannaCry Ransomware: Everything You Need to Know.” *CNET*, CNET, 19 May 2017, www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/.

“Significant Cyber Incidents.” *Significant Cyber Incidents | Center for Strategic and International Studies*, www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

Silverman, Lauren. “There Are Plenty Of RFID-Blocking Products, But Do You Need Them?” *NPR*, NPR, 4 July 2017, www.npr.org/sections/alltechconsidered/2017/07/04/535518514/there-are-plenty-of-rfid-blocking-products-but-do-you-need-them.

“Spotting a Scam.” *Citizens Advice*, www.citizensadvice.org.uk/consumer/scams/spotting-a-scam/.

Strickland, Jonathan. “How to Detect Online Scams.” *HowStuffWorks*, HowStuffWorks, 20 Mar. 2009, electronics.howstuffworks.com/how-to-tech/how-to-detect-online-scams.htm.

Tapper, Jake. “Panel: Were North Korean ‘Cyber Soldiers’ behind Sony Hack?” *CNN*, Cable News Network, 18 Dec. 2014, thelead.blogs.cnn.com/2014/12/18/panel-is-north-korea-waging-a-cyberwar/.

Victor, Daniel. “Minister in Charge of Japan's Cybersecurity Says He Has Never Used a Computer.” *The New York Times*, The New York Times, 15 Nov. 2018, www.nytimes.com/2018/11/15/world/asia/japan-cybersecurity-yoshitaka-sakurada.html.

“What Is a VPN?” *Official Site*, us.norton.com/internetsecurity-privacy-what-is-a-vpn.html.

Świderek, Tomasz. “Central European Financial Observer.” *Financial Observer*, financialobserver.eu/poland/cyber-attacks-cost-the-world-economy-usd600bn-each-year/.

“Cyber Security Literacy” Murray E. Jennex

"China's hacking attacks are more than just a nuisance." *Sydney Morning Herald* [Sydney, Australia], 8 Dec. 2015, p. 16. *Global Issues in Context*, https://link.galegroup.com/apps/doc/A436708567/GIC?u=mass12242&sid=GIC&xid=261fbfb3. Accessed 19 Mar. 2019.

"Transcript of Zuckerberg's appearance before House committee." *Washingtonpost.com*, 11 Apr. 2018. *Global Issues in Context*, https://link.galegroup.com/apps/doc/A534461397/GIC?u=mass12242&sid=GIC&xid=bc6a031e. Accessed 19 Mar. 2019.

Alexander, M. (2019). *SANS Institute: Reading Room - Critical Controls*. [online] Sans.org. Available at: https://www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972 [Accessed 20 Mar. 2019].