Recommended Reading List

(and continuing education)

Here are some interesting topics for your review. I have studied this information myself in whole or in part and I have personally utilized these resources to further my own education. Obviously I can't list all of the hundreds of resources I have used over the years but I find each of these topics to be fascinating and hope that you will too! (Please note that video links may change after the date this was published. If the link is broken please use the key words in my description to find the video).

Cyber Security

Cybersecurity and Information security are related–in fact, one can be said to be a subset of the other. The important thing is that we are protecting information and physical access to resources from others who are not authorized to access them.

Best practices apply. Password policies enforcing strong passwords or passphrases which are changed regularly, strong encryption, MFA (multi-factor authentication), layers of security, monitoring, physical and/or time access restrictions, software updates, employee education and other policies are still our best means to minimize criminal activity in a corporate environment. Additional protection may become necessary as AI moves into a dominant position in information technology.

1. Basic cybersecurity principles. This one is an ad for Norton software but lists some valuable points: https://us.norton.com/blog/how-to/cybersecurity-basics
2. Government site: https://www.ready.gov/cybersecurity
3. Utilizing AI for cybersecurity:. Personally, I feel that companies are under-rating security threats posed by AI. Everything a security analyst can produce using AI has a parallel in the hacking world. There really is no way to prevent the same AI "entity" from producing both malware and anti-malware. https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity

Ransomware

Ransomware is not new but it seems to be more prevalent so be proactive and have a plan in place, because we will all open a link in an email or click on a rogue file at some point, if we haven't already done so . Employee education and reminders are important. Make sure all internet-connected devices and firewalls (and especially cell phones and PCs/tablets) are fitted with anti malware that is updated with the latest definitions, and turn on heuristic behavior detection. Utilize VPNs and endpoint protection. Critical infrastructure organizations can use email filters that convert all messages to text and block html emails and images. Regular

backups and data snapshots are essential but make certain you do not restore data from a compromised backup or image.

Here are some very good guidelines from NIST:
https://www.nist.gov/news-events/news/2021/05/nist-releases-tips-and-tactics-dealing-ransomware

Ransomware recovery. This CSO article describes some essentials around backups, offsite storage, and disaster recovery:
https://www.csoonline.com/article/571131/ransomware-recovery-8-steps-to-successfully-restore-from-backup.html

Networks

Cisco CCNA Learning Academy. Free tutorials and tools like "Packet Tracer" which is a network simulator using Cisco routers and switches. https://learningnetwork.cisco.com/s/

Network Chuck CCNA (he also offers a free set of YouTube videos):
https://academy.networkchuck.com/ccna

Operating Systems

I use both Windows and Linux but you may want to take some courses on Udemy and Coursera if you are not familiar with one or the other, especially for the CLI interface for Linux Administration. Linux has "powerful" built-in command line tools for security and system administration but it takes awhile to master them. (The "man pages" and "info" are your friends!). I assume most people have used different versions of Windows but make sure you understand authentication, scripting, and AD.

General background info for OS Administration:
https://www.tutorialspoint.com/operating_system/index.htm

Basic commands for Linux Sys Admin:
https://www.geeksforgeeks.org/beginners-guide-to-linux-system-administration/#

Linux namespaces: https://www.redhat.com/sysadmin/7-linux-namespaces

Infrastructure Security

Our critical infrastructure in North America includes any process, activity, or technology that is essential to maintain our current base level of existence. This includes power production, communication, supply chain, agriculture, transportation, government, and even information

technology. CISA lists at least 16 sectors.
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

You have to understand what you are protecting before you can implement security measures. I recommend that you watch some industry videos on power grids, steel production, wastewater treatment, gas and petrochemical production and fractionation, nuclear power, chemical manufacturing, mineral mining, and the tools used to monitor and control these industries like SCADA and DCS/PLC as well as their vulnerabilities to attack. Once you get some background knowledge it is instructive to look for articles and videos on how to hack these same tools and processes. I especially enjoyed the video on the power grid by Rusty Williams at https://youtu.be/nJ-eBqEnraE . And since I am from Pittsburgh, PA (the home of Andrew Carnegie and US Steel), steel production has always fascinated me. I can remember as a kid watching them pour the hot slag outside at night above the river and how it would glow in the dark. Here are links to a couple of videos to steel production, seamless steel pipes, and steel ball production: https://youtu.be/tlNg4205Tpc , https://youtu.be/Rhc_Kkc-vMY , https://youtu.be/cG5MQTa458s . Did I happen to mention I'm from Pittsburgh?

Artificial Intelligence

There are some fun hands-on examples on YouTube by Radu from the University of Finland. Take a look at the tutorials on creating your own self driving car and one on facial recognition. The first one uses neural networks. https://radufromfinland.com/#about

If you are not familiar with the concepts of AI software, look at machine learning, deep learning, and neural networks. Two good sources I used were Stanford's open courseware on machine learning (MATLAB) by Andrew NG:
https://www.youtube.com/watch?v=jGwO_UgTS7I&list=PLoROMvodv4rMiGQp3WXShtMGgzqpfVfbU&ab_channel=StanfordOnline and the MIT opencourseware course on AI from Patrick Winston:
https://ocw.mit.edu/courses/6-034-artificial-intelligence-fall-2010/resources/lecture-1-introduction-and-scope/

Here is another good article on the new NSA AI Security Center and the Facebook (aka "Meta") interest in AI innovation investment:
https://apnews.com/article/nsa-artificial-intelligence-security-deepfakes-f9b19dd64890884cc2b0700ddf66e666

Programming Languages

Python Mastery from Beginner to Expert (Mosh):
https://codewithmosh.com/p/python-programming-course-beginners

Json and Ajax: easy W3Schools example: https://www.w3schools.com/xml/ajax_intro.asp . Here is a great video tutorial: JSON and AJAX Tutorial With Real Examples LearnWebCode https://www.youtube.com/watch?v=rJesac0_Ftw&ab_channel=LearnWebCode

Secure C++ code. I'm not sure how old this is so you need to look at the current best practices for software coding in C++, and especially C programming. Also be aware of security regarding memory pointers and buffer overflows. https://resources.sei.cmu.edu/asset_files/BookChapter/2005_009_001_52710.pdf

Pen Test and Forensics Tools

Think like a hacker. Be certain to download any security software from a reputable site and then compare the file hash with the online value. Also scan your downloaded file for malware. Free security software would be a great place to install a Trojan horse program.

Wireshark. Wireshark is one of the best known packet sniffer and network analyzer tools. It is used for MITM analysis and is useful for reverse-engineering and forensics of malware and network attacks. https://www.wireshark.org/

Kali Linux and Parrot OS Security. Both Operating Systems are packed full of pentest, forensic, hacking, reverse engineering, and other tools. I've used both but find Kali to be easier to use. In either case, make sure you understand the code and how it works. You don't want to be a script kiddie and you don't want to end up in jail either. It is probably best to play in a virtual machine environment: https://www.kali.org/, https://www.parrotsec.org/

(Legal) Practice sites for discovering and hacking vulnerabilities: https://tryhackme.com, https://dst.com.ng/15-vulnerable-sites-legally-practice-hacking-skills/

Virus Total. Virustotal is both a file and URL scanner and security tool. The options on their site allows you to explore a specific class of malware in more depth as you troubleshoot your system. https://www.virustotal.com

FTK Imager. This software is mostly used by law enforcement and there are similar tools for iOS and mobile devices. There are comparable low cost or free tools for the general cyber analyst in Kali and Parrot OS. https://www.exterro.com/ftk-imager

IoT Security

The IoT ("internet of things") has evolved from simple devices like smart watches and home security cams to local smart homes, vehicles, and cloud-connected applications and devices encompassing wide geographical areas. Simplistically the IoT is a group of networked devices that communicate with each other and/or a master server(s) that analyzes the incoming data,

makes "decisions" and then relays those decisions back to the devices. As an example, your ride home could encompass your GPS location from your car and phone, traffic conditions from online sources, outdoor weather sensors and other sensors, and then unlock your doors, adjust your indoor temperature, and have coffee waiting for you the moment you enter your home after a long day at work!

Many original IoT devices were not built with security in mind. Hopefully the majority of newer devices are more secure but one still needs to guard against side-channel attacks or hopping from one device to another to eventually access information on core servers.

IoT Full Course (Edureka!): IoT Full Course - Learn IoT In 4 Hours
https://www.youtube.com/watch?v=h0gWfVCSGQQ&ab_channel=edureka%21

Cloud Security

Here are links to security topics from three of the major cloud services providers. Make sure you understand your contract with your cloud service provider–they are usually responsible for their infrastructure, but often you are responsible for any virtual networks, devices, apps, and other services you create or host on their equipment.

1. Microsoft (Azure): https://azure.microsoft.com/en-us/products/category/security/
2. Amazon (AWS): https://aws.amazon.com/security/
3. Google (Google Cloud): https://cloud.google.com/learn/what-is-cloud-security

Cyber Safety for Kids

As a parent myself I am passionate about protecting our children from moral filth and predation by cyber criminals. Remember, if your child is a minor it is *YOUR* responsibility as a parent or caregiver to keep them safe. Just because their friends all have smartphones and tablets with the latest apps and unlimited access to videos and chat doesn't mean it is right, or good. If you are paying for the minutes then it is your phone that they are borrowing. It is a privilege and not a right, so be a good parent. Install safety features, do random unannounced spot checks on their phones, monitor their online activity. "Do the right thing!". Cell phones are not safe babysitters (and children can remove protective software if you are not monitoring it).

Here are a few helpful links:

1. A parent's guide to cyber security: https://connectsafely.org/wp-content/uploads/securityguide.pdf
2. Tips for families with kids. The YouTube kids suggestion is not practical as it does not prevent kids from accessing the other YouTube channels, but the other points are pretty good. https://familieswithgrace.com/15-cyber-safety-tips-for-parents/

3. Protecting kids - online government site: https://consumer.ftc.gov/identity-theft-and-online-security/protecting-kids-online
4. Some moral thoughts on kids and cybersecurity: https://www.geneva.edu/blog/program-spotlight/the-value-of-christian-principles-in-cybersecurity-education
5. Or, here is a thought–keep your kids offline as much as possible. Encourage actual independent thought and real experiences, not fantasy or pretend ones they get online or on TV. Go for walks or camping or play games with your kids. Ask them about their experiences with school and their friends. Make it easy for them to talk to you.

Case Studies

1. Stuxnet: Langner's Stuxnet Deep Dive. https://youtu.be/zBjmm48zwQU . Ralph is a good speaker and subtly humorous. The presentation is technical so if you are a nerd like me with some knowledge about reverse engineering, then you will really enjoy this. I found the details were easier to follow if I listened to the video without watching the visual presentation. The story behind-the-scenes is every bit as intriguing as any crime drama on TV!
2. Solar Winds. This one was interesting because the malware was injected into the software updates. (Perhaps a good reason to first test patches and updates in a virtual environment in lieu of turning on automatic updates on the production servers). Malware was installed as network devices were automatically "patched". https://www.csoonline.com/article/570537/the-solarwinds-hack-timeline-who-knew-what-and-when.html
3. Physical and cyber attacks on critical infrastructure: https://centerforsecuritypolicy.org/recent-critical-infrastructure-attacks-expose-our-vulnerability-and-the-need-for-change/

Security Gurus and Sites that I follow from time-to-time

1. Sans: https://www.sans.org
2. GRC research (Steve Gibson): https://www.grc.com/intro.htm. Steve is one of my favorite podcasters. Look up how he reverse-engineered the bot software to thwart a DDOS attack in progress on his site and even surprised the criminal by "showing up" and warning the attacker to desist in his own secure private chat room on the dark web.
3. Network Chuck: https://learn.networkchuck.com Courses in a wide variety of topics including CCNA, Python Programming, MS Windows, Linux, Cloud Computing, Docker, Kubernetes, Ethical Hacking, etc.
4. Bruce Schneier: Schneier on Security. Bruce Schneier is one of the long time experts in all things security. He writes about a wide variety of relevant topics on his blog and also addresses concerns regards to national security.
5. 'The Art of War' by Sun Tzu. Okay, technically this is not a book on cybersecurity and they probably didn't have digital technology in 500 B.C., but this is a "must read" for anyone

who participates in cyber warfare of any kind. I will leave you with this quote from the book "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."