Brain Dump of Transcript Data

Section 1: Transcript 1.txt

Transcription Alrighty. Okay. Okay. So, this is going to be an information dump of information for the security book. The main purpose of the security book is essentially to provide a baseline of security knowledge for people um the average everyday person so um i figure the best way to do this is providing a student's um a student's look in or rather uh a tech enthusiast look in who's not a professional but who also isn't dumb about things. Someone that has learned from experience of personal matters and not by the book industry, because people tend to trust people not in uniform opposed to people that are in uniform. So, let's see, what information are we going to cover? So the first things that I would like to cover are generalized what-are questions. So what is a computer? A computer is a mixture of different elements, circuitry. I'm pretty much going to say a computer system has a bunch of ways it can communicate. It has RFC, NFC, Wi-Fi, Bluetooth, and all of these things. I'm going to mention all of the different types, all the way up to... Um, I would say NFC, uh, because that's most, um, that's most, uh, consumer brand computers or consumer grade computers have. But then I'm going to focus primarily on Wi-Fi, Bluetooth, and NFC because that is what is utilized most in the public. So, following this, I'm going to mention, first thing, NFC. What is NFC? NFC is a magnetic signal that is present on most, if not all, cards. So, for example, credit cards or debit cards or even ID badges, NFC can be duplicated easily by a by a NFC reader, or a phone can duplicate these things. Now, what I'm going to say in there is my main goal is not to panic the public, but it is to make everything clear. So I'll say, first off, NFC is pretty much a non-contact slash close-range contact where all you need is a device that can read these magnetic signals, NFC. So if you're living in a big city, you have to watch out for people that are getting a little too close and appear to be holding a black box or some sort of antenna near people's pockets. This is an NFC reader. I also want to point out that if you have any sort of financial information saved on your phone, such as a credit card or notes that are connected to NFC somehow, if you have any personal information that you use for banking or anything in general turn off nfc until you're going to check out or don't use nfc at all. it's also good practice never to actually save your credit cards on phones even though it's convenient it is still not a good idea because there are multiple ways to get it. Um, the second thing, when you're in public, if you do not have a device directly connected to your phone, turn off, uh, Bluetooth. Bluetooth is susceptible to different attacks, such as bluejacking or blue scarfing. This essentially means someone manages to connect to your Bluetooth signal or hijack it, where your device is open and it looks to connect to something, and someone either forces it to connect to something, or you're looking for another device that you want to connect to, such as a headset, and they manage to connect your phone to their device instead. So if you're not directly connected to something before you leave the house, just don't turn on Bluetooth unless it's necessary for some sort of job. Wi-Fi. If you're on your cell phone and you're in public, turn off Wi-Fi. Do not connect to public Wi-Fi. Public Wi-Fi is one of the easiest ways people can get information. You can install a VPN, which is a virtual private network, and that does mask your traffic from local Wi-Fi networks. However, it is not a guaranteed solution for data... security, mainly because when you're connected to a Wi-Fi

network, your phone is now communicating with a router, and if that router is compromised, something could happen. Speaking of networks, the next section is about home networks. Now, how do home networks work? Well, there are two primary pieces of hardware that are used for a home network, those being the modem and and the router. There is something called a combo modem, uh, where it does serve as a relay and a way to connect to your ISP, but that is different, um, uh, from this topic. What is a modem? A modem has only one primary job, and that is to establish a connection between your home and your ISP. Your ISP, Internet Service Provider, is the person that gives you resources, so depending on your plan. For example, if you buy, I don't know, a **gigabit** of service, they're going to allocate a gigabit of service to you. Basically, your modem is your way to connect to their service. um, network and then their network being massive, you connect to everyone else. The router, however, is your actual backbone of your personal network. So the modem takes the resources, and then your router disperses these resources. So when you set up your home network, you're not setting up the modem. The modem is proprietary, meaning it's owned by the ISP. You don't do anything with it other than... other than power it on and wait for connection and register it with your ISP. Whereas your router, you have much more control. Your router is what guides all of the resources to different devices in your home. Now, how do routers connect all of your devices to the internet? How does it disperse the signal? Well, the router uses a bunch of different protocols, a bunch of different things. However, I will go over what different protocols there are. So first off, authentication would be, at least I think it's authentication protocols. You have **WPA2** and **WPA3**. Most routers will act as a hybrid for this because some people have outdated devices that still use WPA2. Now, normally, it would be a good idea to turn off this mixed mode. However, if you do have an older device that is incapable of using WPA3, you need WPA2, WPA3 mode on. Um... and then you have a bunch of other protocols, such as **AES** (Advanced Encryption Standard), and this is, I think that one's authentication, and then I think the communication protocol is AES, no, the communication protocol is WPA. Pretty much for the book, I'm going to say what the protocols are, but I won't go into a lot of detail on what they actually do. I mean, I will, but I won't go into, like, a lot of detail. And then we lead into communication protocol. You have two types of communication protocol that are mainly used. There is one called RADIUS, but not many people use it. Generally, they will utilize... one of two, which is HTTP, hypertext, plain text protocol, and then HTTPS, which is the secure version where it encrypts your traffic. Personally, if I was setting up a network, and I have set up a network for my parents in the past, I would utilize a WPA2-WPA3 communication with HTTPS Traffic and AES, or whatever that protocol is. So how do routers actually manage everything that computers do? Well, routers have a giant... uh list of ports portals or whatever you want to call them their doorways pretty much a port and um these ports there are **over 65,000** ports on a router and what these ports do is they allow computers to communicate using different protocols so The most commonly used protocols for a router are going to be, um, are going to be port **80**, which is HTTP, and port **443**, HTTPS. And port **443**, HTTPS. These two are mainly used for internet connections, and pretty much ports are what allow your computer to communicate with everything by setting up message boxes. So for example, when you set up a web request, have you ever noticed how HTTPS is in front of the URL sometimes? Well, that's because an HTTPS communication is being established. So port 443 on your network is open, and it's waiting for a response from outside. Now there are... like I said, thousands of different

ports that are utilized in modern computing. We are not going to cover them all. However, I wanted to establish how that works. Now, in terms of... that. What are the means of routers managing things? Now, normally, well, back in older times, you would have to set up port forwarding. And port forwarding is essentially, you're telling the computer, hey, if this computer needs to do this type of message, use this port. So, for example, you would grab the **IP address**, which is the internet protocol address. I believe some of them use **MAC address** (the hardware ID, which we'll cover later), but pretty much what you're telling the router is, hey, here's this device. If this device needs to receive a signal of this type, use this type of port. So back when we were starting to do online gaming, you would have to say, hey, if you want to connect to this, this, and that, you'd have to use a UDT port, this, this, and whatever. So for example, Steam, I believe, needs about... Steam, one of the biggest game distributors ever, they use, what, four or five different UDP ports for communication, plus HTTP and HTTPS. And I think they also have a streaming protocol in there too. But yeah, so anyway. Normally, well...

Section 2: Transcript 2 A.txt

Transcription Alrighty. So this will be the, uh, second transcript for my book, um, which I plan to title, um, as an acronym, uh, C S C S or, um, cyber security from a, uh, cyber student. Um, primary, this is the introduction, um, the primary need for this book, the primary purpose of this book is to bridge the gap between a total novice and expert. Uh, in other words, target the most, uh, Target the largest group when it comes to cybersecurity, that being people who set up their own home networks and or use the internet, the average internet user. Most books have too much comprehension. They are specifically made to either train people in the field that already know technology and use different... Well, not different. They use professional terminology. And then there's the other spectrum where it is bare bones, like hardware. What is this type stuff? The four dummies books. And this doesn't help the middle group, which is they know what the stuff is, and they know how it works on a surface level, but they don't understand the risks and how it operates in the background. I also find it interesting that I'm not sure if these numbers are correct, but I believe they are. It is interesting to me that about... Like, almost every child in my generation was exposed to... I'm Generation Z, but almost, if not all children in my generation were exposed to the internet by the age of five or beforehand. Which means we were connected to the internet long before any other generation, and it's only getting younger. Now, who's to say if this is good or bad is up to the reader, but for the context of this book, it mainly means that security is a very big thing that needs to be talked about. Considering the fact that most people in my generation, while they do use the technology, they do not understand how the technology actually operates. And this is very concerning to me. I know I am... I know I am a young individual and I've learned from not only my, uh, college experience, but primarily my own experience in my own research, which I find more value in. Um, but no one's going to take the time to do as much, you know, research. Um, And that's where I want to bridge the gap, because there have been a multitude of things that I've seen, there have been a lot of things that have happened, and there have been a lot of things that I want to prevent happening to people in my generation. So the introduction of this book is pretty much to say this book is for

people who use the Internet and want to learn how to be safe on the Internet and what exactly happens behind the scenes. All right. So chapter one will be very bare bones. What hardware is involved with networking? What allows you to connect to the Internet? Now, most people, most people, if not all people have Wi-Fi at their home. Now, how does this happen? What exactly connects your devices? What takes this piece of hardware and lets it connect to the World Wide Web? So, there are two main components to every home network. Technically, there's a variation of this, which we will cover later. But for now, The two main things that you need in order to get started on the internet are a modem and a router. Now, these two things have very different roles. A modem is what you get from your ISP. Your ISP is internet service provider, such as Spectrum or Verizon or one of the many internet providers. And then the second piece of hardware you either get from your ISP or you can buy yourself. And that is your router. Now the modem, all it does is it connects to your ISP. It pretty much does this in a nutshell. You set up your modem at home. You give it power. You register it with your ISP. That modem now connects to your ISP's network. Now, depending on the plan you have, that is how many resources you will be given. Now, what I mean by resource is how much service supply you have, how much bandwidth. So for example, if you set up a Spectrum modem and you are paying for one **gigabit** plan, that means you will have one **gigabit** of bandwidth. Now bandwidth is essentially how much information you can send back and forth when using the internet. So, for example, when you download a video game, you are using bandwidth to download that game on your computer. So, if you have a service plan that is 500 **Megabits per second (Mbps)**, a download will take longer than if you have a **Gigabits per second (Gbps)** plan. The higher your bandwidth, the faster the information can go in and out of your network at one time.

So that's what the modem does. It gives you access to this. Now, how do you actually use this bandwidth? What gets the bandwidth? What allows devices to connect? to your modem to use this bandwidth. And that is where the router comes in. Now, the router is... Think of it as a bridge. A router is essentially a bridge between your devices and your modem. When you plug a router into a modem, it now has the ability to disperse all of that bandwidth into your home. So have you ever noticed that newer routers, or if you have an older router, doesn't matter, the router acts as an antenna. The modem acts as the source of bandwidth. So when you...

Section 3: Transcript 2 B.txt

Transcription black box in general they can scan your pocket and steal your credit card now this isn't to scare you this is just to say if someone's walking around and they have an interesting piece of technology just hanging there and they ask you to tap your phone to it don't do it or if they're walking by and they're trying to do the same to people's pockets do not get near them and inform a police officer NFC is, again, a magnetic signature that saves information. So your credit card number becomes a giant mess of magnetic signals and then translated into digital signals to a phone. The second and mostly not talked about method of attacking is Bluetooth.

Everyone knows what Bluetooth is. Bluetooth allows you to connect your phone to your computer or your phone to a speaker or headphones or anything else. Well, Bluetooth can also be susceptible to hijacking and a few other things. Which is why I personally recommend you turn off Bluetooth and NFC when you're out in public and you don't need it. Now, Bluetooth hijacking is essentially where a hacker... pretends to be a device you're trying to connect to. So if you tell your phone to scan for a new device and it's looking for a specific device, a hacker can make their device look like the Bluetooth device you're trying to connect to. And obviously, most people have auto-connect by default. So if the hacker is duplicating a Bluetooth signal, this means you can, well, connect. Your phone will connect to the hacker's device, and then information going through Bluetooth will go to them instead. There's also another technical term that I don't really want to use because, again, this book is made for the general public, but blue snarfing, which is data stealing, and then blue jacking, which is sending unwanted messages, all going through the Bluetooth hijack. Now, the most... This advice is... I say this with a sigh because not many people like this advice, but I'm sorry, it is true. If a place is providing public Wi-Fi, please do not connect to it. Now, I understand you're going to say, but it's for the public. And yes, there isn't anything inherently wrong with connecting to public Wi-Fi as long as you don't do anything sensitive or you don't have credit cards or anything stored that you don't want stolen. In general, my rule is do not connect to a public network. Always connect to your data. This is because their routers are mostly configured to be very convenient for the public, which also makes it very convenient for criminals. Criminals can connect to the router, and like I said, if the router isn't configured to be secure, they can pretty much see all the traffic that is going on on a... on a router. Now, you can use a VPN, which is a virtual private network, and this essentially means the router cannot see your traffic. It only sees an encrypted signal. Now, router... Now, if you do need to connect to a public Wi-Fi network because you don't have data, here are some very crucial things you should never do on a Wi-Fi network. Number one, never open any financial bank, any financial application ever when you are connected to a public Wi-Fi network. This includes your bank's app, any financial apps, including Cash App, or any service involving payment of any kind. So, for example, Amazon. Anything that has your credit card, just don't open it. Again, don't store your credit card on your phone. Even though it's convenient, it's not a good idea, personally. Now I know, as I said before, convenience versus security is a very big thing. So, if you are going to store a credit card on your phone, please do not connect to the public Wi-Fi. It's bad. So, anyway. Next, we should talk about securing credentials. Well, maybe. Maybe. No, let's talk about... Let's talk about... I suppose we should talk about the tools that hackers use. Yeah, tools. Okay, so this mainly goes into your general internet usage. So when you're online... Number one, if someone you don't know sends you an email and it has an attachment, please do not open it. Now, this is going to be a little bit confusing and maybe somewhat off topic for this book, but I feel it's very important to mention this to the public. An image sent by someone online can still have bad stuff in it. where you see a picture of an image, they see a program that has been placed in the back of the image. Now, I'm not going to go into detail on how this actually works, but pretty much what they do is they utilize a file masking tool where the data becomes an image, and then when you load that image, program that they put in to the image is loaded onto your computer. Not going to go into detail with it, but pretty much the rule is, if someone sends you an image or a file and you don't know them, do not download it and do not open it. That is priority one. Don't do it. Alright, so with that out of the way, what are

the different types of things that hackers can use to steal information? Well, number one, there is image things, mainly called Trojan horses, or a myriad of different other things. But pretty much what it is, is it's a thing that looks like something, but it is not that thing. So when the Trojans attacked that one king, pretty much everyone knows the Trojan horse. Giant horse put out in the gates of Troy. They opened it and well, then everyone was attacked because the thing inside of it was a bunch of soldiers. Same thing with programs. If someone offers you a quote-unquote free version of a paid game, do not download it. It's not good. It's never good. Even though it might work the first time, in the background, stuff is still happening. Many people in my generation don't understand just how much things happen in the background when they are running computers. Some good, some bad, and some are meh in between. We'll get to that later so what are the general rules of security for yourself online number one password is key now yes everyone hates it but it's true you need a long password and it needs to be more than just a single word now My personal rule is **16 characters long minimum (or a pass-phrase of similar length and complexity)**. It has to be that long. Unfortunately, most computers are very good at distinguishing patterns. This includes passwords. So if you use a singular word, and it's below 16 characters, your password is significantly more vulnerable to brute force attacks. A brute force attack is what it... ... (rest of Transcript 2 B.txt content) ... your device and won't be sent over Wi-Fi. However, if someone gets into your computer and downloads these pictures, well, then they know pretty much everything that you did, including whatever you're typing on screen. Okay. But this is mainly reserved for UPU, not CPU, UPU computers. We talked about advertising. We talked about a bunch of other stuff. Oh, I should note, never store anything sensitive in an email because emails are pretty much open. If someone gets into your account, they can read it. So there's that.

Section 4: Transcript 3.txt

This is going to be. Another umm, not quick, but well, maybe quick, I don't know. But this is going to be another transcript for my book. I wanted to cover some of the basics again. Again, this is what this book is for. It is for. It is for the general public. So umm, one thing that I would like to cover because my mother brought it up last night actually when she was trying to get onto the Internet and she almost clicked a link that was clearly a scam so. Figured I would talk about the dangers of AI generation as well as scams in general. I know I covered it a little bit in my notes previous but I want to cover more. So yeah. So one of the primary things that mainly gets your system compromised and your information stolen. Umm is uh, scams. Now I'm going to talk about specifically phishing scams because what people don't actually know is most of the time hackers and scammers do not quote UNquote steal your information. You give it to them. And what I mean by that is you click on a link that goes to a website. That website prompts you for information. Now not looking, you may not notice that the domain name of the website is different or. That the umm. That the page looks slightly off and you will be prompted to login and you would be prompted to give information to the website. Now normally this would work out just fine, but because this is a false website. Then you've essentially given whoever owns the website your information. It's the same with. Phishing emails. They claim to be someone else

and you give them your information. Now, one of the most important things I'm going to say in this book is, well, I believe I said it before in the other transcript, but one of the most important things I'm going to say about this topic is. A company will never e-mail you that they forgot your credentials or e-mail you and ask you to log in with the quote UN quote dear user. Tagline. Companies will always give you a direct link to their website with some sort of some sort of reason for contacting you. So for example if you haven't touched. Your account in two or three years, a company might e-mail you and say, hey, we're going to disable your account after this date because you haven't touched it for two to three years. So that's that's normal. Another example of normal is they will inform you that your password was changed. Now most companies won't even give you a link to go to the website. You have to go to the website by yourself. Scammers will always give you a link. Hackers will always give you a link. They want you to click on something that's bad. Umm plus they'll also use blunt language and try and make it seem urgent. So for example they'll say something like we forgot your banking details or someone made a deposit in your account. You have to log in right now using this link. To fix it. Now this is a scare tactic. Their whole entire goal with this is prompt, a sense of urgency. Urgency is the favored weapon of the scammer, and it's effective in many. Many, many ways. Umm, because no one thinks about it so. Bottom line is if you're getting an e-mail from someone and you're not 100% sure it is the business, you can call the business now. Or leading into calls and such. There are things that sometimes pop up on screen that say you have to call someone because they found a virus. This is mostly fake. A computer will never do this. The only time it would do this is if you install software to show you that there's a malicious. Website that's active, or a virus, or your computer shuts down and gives you an error code. Never when you're in the browser. Are those virus things real, Or rather the ones that say call now are real? Now there's other types of sophisticated attacks. There's something called frequent reload pages, which are essentially pages that are programmed to reload themselves when you try and back out of them. Now these are less common as most of the. Countries that do scams are less sophisticated and they do the bare minimum. Uh, that's the difference between a hacker and a scammer. A scammer does not know what they're doing on a machine. They may know the basics, they may know how to use a remote access program that people download, but they do not know how to do. Actual damage to a machine. They just want you to give information. Whereas someone that is technically versed and can do damage and can steal things without your input, that is a hacker, or at least someone that knows how to write a script to get stuff is a hacker. Umm, now hackers are common on the Internet, yes, but as long as you stay on the clear web you should be fine. And as long as you don't click links you should be fine. Clicking links as in add links adds are it said to say. What most ads do lead to some form of scam, which is terrible. I don't know why this is legal, I don't know why it's not investigated, but it's true. Speaking of scams and links, let's... Social media is one of the biggest things in our world. It allows everyone to connect with one another directly, unlike video games where you have a. Objective and no one's really paying attention to one another and just playing the game. Social media is the exact opposite. Social media is a platform designed for attention. It is designed for likes. It is designed for shares. It is designed for social interaction in general. Now, unlike video games in which I personally think. Uh, children are fine playing as long as it's in the age range. Social media is a different story. Social media by its nature is designed for, well, socializing, and it can lead to some interesting things. It is much more easier to communicate with someone. It is

much more easier to see something that your child. He's not supposed to see. Granted, there are security measures in place for many and many. Umm, companies do offer child protective uh systems. However, if the parent does not do their duty to manage and ensure the child is on these specific platforms or settings, it can lead to some bad things. For example. Even if you were on social media, for example, it could end very badly and you could have not trauma but have seen something that was not supposed to be seen. End of Transcript 3.