The Langley Files: CIA's Podcast
FILE 017
CIA Cyber Safety 101

(music begins)

Walter: At CIA, we work around the clock and across the globe to help keep Americans and others around the world safe. Secrecy is often vital to our work.

Dee: But we're committed to sharing what we can when we can. So let us be your guides around the halls of Langley as we open our files and speak with those who have dedicated themselves to this mission.

Walter: These are their stories.

Walter and Dee: This is The Langley Files.

(music continues)

Dee: So you're listening to the end of the last episode of The Langley Files, on legendary CIA officer George Hocker, and you find yourself mulling the trivia question.

Walter: "Which country is slightly larger than twice the size of California and is the only African country to have both Atlantic and Mediterranean coastlines?"

Dee: And as you rotate your mental map of Africa, you decide to go online and double-check it…

Walter: So you log onto your computer, find a map, and—wow—there's only one country in Africa that borders both the Atlantic and Mediterranean! It's clearly—

Dee: But then something strange happens. A series of pop ups start to fill your screen…

Walter: And then your phone rings…

Dee: And then the lights start to turn on and off… And you ask yourself…

Walter: Am I in Poltergeist?

Dee: Nope…

Walter: Are we overselling this?

Dee: Nope…

Walter: Has every device in my home been hacked?

Dee: And the next question that might come to mind is…

Walter: What would a CIA cyber security specialist do in this situation?

Dee: Bingo. Well on this episode of The Langley Files, you're going to find out.

Walter: We're sitting down with Jennifer Link, CIA's Chief Information Security Officer, to discuss cyber security tips anyone can use to stay safe on the web and—increasingly—in everyday life.

Dee: So whether you're setting up your state-of-the-art smart home…

Walter: Or just streaming a movie during a summer thunderstorm…

Dee: This is an episode chock full of tech news… you can use.

(music ends)

Dee: So welcome back, everybody. I'm Dee.

Walter: And I'm Walter.

Dee: We are fortunate enough to be sitting across the table from Jennifer Link, who is our Chief Information Security Officer here at CIA. Jennifer, thank you so much for taking the time to come in and chat with us today.

Jennifer: Absolutely. And thank you for the invitation.

Walter: It's awesome to have you here.

Dee: So, Jennifer, for folks that don't know what a Chief Information Security Officer, or a CISO is, could you give maybe a snapshot of what that role entails here at the Agency?

Jennifer: Absolutely. So this is not only a role that exists within federal agencies, but it's very common across most commercial companies. And the role can differ slightly from, you know, business to business. Here, at the Agency, though, the Chief Information Security Officer is wholly responsible for the cyber security of the Agency's data and its information systems. The goal is to ensure the resiliency and the survivability of the mission that we're responsible for. And so that means understanding what all of the devices are on every single one of our fabrics. And we have multiple different fabrics. Understanding what the health of those devices are, working to ensure that they are kept up to date. We're also responsible for assessing systems. So when someone has a beautiful idea and they want to put all sorts of different components together to achieve some amazing outcome, then we are responsible for assessing that system to understand what new risks it may bring into the environment. This is often things like cutting edge new emerging technologies that we may not have the kind of telemetry or data collected from it to understand what risk it may be imposing. So we work with really closely with the

system owners to understand that. And then we have a team of folks that work closely with system owners to ensure that they have an understanding of what cyber security policies are in place, understand what cyber security risks there are, and then work to balance that risk to ensure that the Agency is meeting its need while at the same time the system owner has some flexibility in applying a host of different kinds of solutions to their problem set.

Walter: Wow. So, resiliency and survivability are important at any organization, but you can imagine they're especially important with an organization like CIA that's literally tasked with detecting threats to the American people before they occur.

Jennifer: Absolutely.

Dee: It takes a special person to be able to step into that role. So I'm curious what it is that made you want to join the CIA and if you could share a little bit about your career trajectory.

Jennifer: So I am a second-generation staff officer. I can probably count on more than one hand how many family members have worked here in the past. Growing up as a child in a family who served the Agency in lots of different ways, public service or serving our country was always sort of top of mind and something that was very much prevalent. It was something that we talked about as an important way of contributing back to the protection of our nation. So I took that very seriously, and it was really part of just us growing up as a family. I saw my mother in particular, who is kind of a hero of mine, single parent taking kids overseas because she knew there was a job to be done. Um, and just really proud of her for all of the sort of the trails that I'm now getting to walk on as a result of her her actions. My road to becoming the CISO, though, is definitely not a straight shot. And I wouldn't even call it a lattice. Uh, so when I joined the Agency as what we call a mid-career hire in 2007, I had well over a decade of IT experience in my background. I had a significant amount of cyber forensic expertise at that time. I had previously worked for DOD in a number of different roles. I really enjoyed cyber forensics, in part because I tend to be a very tactile learner. I love getting my hands on something to learn it. And that is the way that I typically will take in information the easiest. And so I just gravitated towards forensics. But when I onboarded into the Agency, I did not have a degree. And so I was really nervous if the Agency would even accept me because again my parents really emphasized the need for higher education, that sort of thing. So one of the reasons that I joined the Agency, in addition to wanting to serve my country and having that as as a core value, was really in seeking my undergraduate degree. And the Agency was tremendously supportive, through a number of different programs. So I had a very unusual undergraduate program that didn't exist. I had to advocate to the school to allow me to pursue at the time, it didn't exist, Information Security was my, uh, degree program, but I had to take essentially two disciplines, put them together and ask for the school to create this individualized undergraduate program for me. And then further on in my career, was fortunate enough to do a tour at a graduate school. Again, the Agency very supportive of that, uh, for national security studies. Even when I EOD'd, though, or or Entered On Duty at the Agency, it was primarily in identity and access management, counterintelligence roles, and systems engineering roles that I served. This is really my first cyber security role here at the Agency. Which is so ironic considering that my undergraduate degree is in Information Security. But I think it really speaks again to the well roundedness that we need our officers to pursue not just their passions, but different interests, because we have to

draw on so many different perspectives as we are challenged with different problems each day. And so I was first the Deputy CISO and stepped into the CISO role last year and have absolutely been enjoying it. That is not to say that any day has been easier than any other, but cannot say enough great things about the amazing team of people that we have.

Walter: Thank you so much for that perspective. That's, that's an incredible career path. And while we have you here, I mean, you are the resident expert in cyber security here at the Agency. Officers here at CIA of course receive cyber security advice and training of all sorts, but some of those best practices are applicable to anyone. So, if you're game, Jennifer, we propose going through a series of situations that might occur in everyday life - some might apply to folks listening, some might not, some might in the future - and hear how you – the Agency's Chief Information Security Officer, would handle them. Does that work for you?

Jennifer: Absolutely. I'm excited.

Walter: A day in the life of Jennifer Link.

Dee: So it's a regular workday morning. You get up, you use your phone to turn on your house lights, and it's chilly in here. So you're gonna turn on the heat in the house, and you might also have your coffee maker, your TV, or any other home device controlled by your phone. So on your phone you have all of these apps controlling all of these devices. And since you downloaded them from the APP store or a website that you've used before, there's nothing wrong with those apps. They're totally secure, right? No? There's long pause there.

Jennifer: A pause right here. Awkward pause. That's right. So what you're describing is really what we know as the Internet Of Things.

Dee: What we refer to as IOT.

Jennifer: That's right. So when we think about things like home smart devices - sometimes they are referred to as digital assistants. Some of us might have Alexa or Google, Google Home modules at home, uh, light bulbs, plugs, thermostats, absolutely. And I will tell you I have these devices in my house, and it's funny, I can remember as a kid running down to the basement to grab something, turning off the light, and running like someone was about to reach out and grab me. I think we've all had this sort of shared experience.

Walter: They actually train you in this scenario at CIA.

Dee: It's always best just to run really fast.

Walter: As anyone with a basement knows.
Jennifer: Absolutely. And my kids will never have that experience because when they get upstairs, they can say "Alexa turn off living room light" and the light turns off. And so it's just a very different growing up experience. But certainly all of those devices come with their own sort of set of benefits, but also challenges. And I think this is one area where we really have a responsibility to lean in and understand what technology are they introducing into our

environment? We have to have a conversation, either with ourselves to understand what we are bringing in, or with our families. And so these devices bring a tremendous amount of freedom and, frankly, for people who have accessibility needs, these are just true game changing types of devices. But there is some risk that comes with them. You're installing apps on your phone understanding where that app comes from. So typically you're going to go into the APP store or to wherever your your store is and you're going to go right past the terms of service or you're gonna go right past whatever those long scroll to the bottom and say yes. I would challenge you to pick the last two apps maybe that you've installed and go to the APP store as an example and read the privacy policy. There have been times when my own family members have asked to download apps to control, say, an LED light strip that they want to hang up in their room because all of their friends have them and I want to fall asleep to the red lights while I'm, you know, or the blue lights while I'm going to sleep. And we've said no because of where those apps are created and published, and we say no, they're collecting too much information from your phone. Some of these devices are requiring a download of your contacts, location awareness, your browser history, which don't have anything to do with the use of your thermostat or your devices. So I think really understanding the company and where the information is being stored, how long it's being stored - that's really incumbent upon us. I know it seems like a pain, but trust me, you will have to put in the time when your data is stolen as the result of some nefarious app or something that you didn't bother to check in the beginning.

Dee: Good points.

Walter: Okay, so read the privacy policies for your apps and manage those settings appropriately. And most of your devices are connected to your home network, so as long as you have a Wi-Fi network with basic password and all of your family and friends who regularly visit all have access to that password, there shouldn't be any security concerns, right?

Jennifer: Pause, awkward pause. So, so absolutely not. I think the days of basic passwords are, well, well behind us. The ability for a cyber actor with a relatively low level of knowledge or low level of sophistication to be able to crack passwords now, again, is just way behind us. Very complex passwords need to be established for our Wi-Fi systems. For many of you may have a Wi-Fi router that you got from your telecommunications provider. It probably has a standard password on the back. And I would, I would bet double digit percentage of folks that are listening to this still have that default password on the back of that router. My recommendation is that you change that to something that is very complex. And in the same way that you may have one Wi-Fi network in your home and you use that for everything, imagine, imagine having one room in your entire house and you do everything in that room. You shower in that room, you prepare your meals in that room, you put your holiday decorations up in that room. It might serve a purpose for a brief period of time, but as you have different living experiences, that's no longer sufficient. That's the analogy I use when it comes to having different Wi-Fi networks. In our home, we have almost 10 different Wi-Fi networks as an example, because each network has a different purpose. So all of our IOT devices go on one network and they're only allowed to communicate with that one network. That means when my family comes over and they bring guests with them, we put them on a different network because I only want them interacting with this sort of sandboxed type of a network. And I have restrictions on that about what sites they can go to and what they can download while they're on our Wi-Fi. I use a different Wi-Fi than

my husband uses, than some of my other family members do. Again, just as a way of sort of segmenting our different activities. There's nothing to say that you can't take that one router and, you know, carve it up into different parts and pieces. But I think if you are a listener who has IOT devices, you have guests in your home, and you regularly use Wi-Fi, you're looking at potentially at least three different networks as a means of creating a blast radius around those.

Dee: Wow. So apparently, we're a little behind in the times. I see you taking notes over there, Walter.

Walter: More networks…fewer guests.

Dee: So, complex passwords, including to your router, and creating different Wi-Fi networks for different uses. Got it. Well, back to your day. You get your coffee and your breakfast.

Walter: Light roast?

Dee: Always, always light roast, and you pick up your tablet to read the morning news. You're scrolling. And all of a sudden a pop up comes up from your browser telling you that there's a virus and you need to click on this link right now or all your files on the tablet are gonna be deleted. Now, you're pretty sure that you're up to date on your antivirus on your device. And you're pretty sure that no software updates were shown to you or needed to be taken. Should you be clicking on that pop up link just in case?

Jennifer: No, absolutely not. I think one of the things that we often as users, especially if we feel not very confident in the knowledge of cyber security or just sort of security of the tech that we have, this false sense of urgency really drives quick behavior without thinking, and my ask is that you pause for 3 to 5 seconds and think - do I really need to click this link and does this seem strange to me? Clicking the pop up link is a huge security risk. Even if your device is secure, this is often referred to as phishing attempts. Sometimes we'll get emails, sometimes a pop up like that. This is a pretty typical way that a cybercriminal is going to design a way to essentially scare you into taking action and sort of leaving your critical thinking skills behind. If you choose to click on that link again in a moment of fear, and if you do, you're not going to be the first person. You're not going to be the last person today to have done that. It it is unfortunately, at times a common occurrence. But that link is going to most likely lead to some sort of malicious outcome. That's going to be a redirection to an unsafe website. It might actually result in the encrypting of the data that's on the device through some sort of ransomware, where a cyber actor may ask for payment in in terms of releasing that data back to you, which is why backups are so incredibly important, even today in this digital age, where we feel like we have access to so much data at our fingertips. And it's also important to remember that security doesn't mean impenetrable. They only have to be right once, and we have to be constant in our vigilance in terms of making sure that our devices are protected and up to date. And it's really why ensuring that your system has up to date antivirus. You might assume, well, it's doing those updates automatically, we tell our family, do not rely on automatic updates. And it's not just the device or the tablet that's in your hand, going back to our network conversation earlier, making sure that you understand how to update your router, any other IOT devices, is is just really important. And

again, I think that's impressing upon all of us that we bear the responsibility to ensure the health and safety of the tech that we use.

Walter: So, take a breath and don't automatically click on the links on unusual pop ups, and keep your antivirus up to date, including by manually checking for those updates. Now that that's taken care of, you finish your breakfast. You get ready for your day, and you're about to head out the door when your phone rings. Now, it looks like it's a number from work, but you're not sure. Do you answer that phone call? Or do you let it just go to voicemail and let that do your screening for you like so many people?

Jennifer: More times than not, I'm letting that roll right to voicemail. This is not unlike the pop up question that we were talking about just a little bit earlier. I think, especially with the age of AI that is upon us, where with very small pieces of information audio or video. Again, a low, sophisticated actor using tools that are openly available on either the Internet or the dark web, can take that information and really use it for malicious purposes. I think it's also really important not to say hello first as an example, but to stay silent because if you start speaking then you're giving information away potentially to that actor who's on the other end of the phone who may be using that recording for nefarious purposes later. Don't answer yes or no questions. It sounds legitimate. This sounds like the person I've talked to before, but again in this age of AI with small pieces of information being able to easily generate those things, it's really important to understand that impersonation is is on the rise for sure, not just the person who's calling you, but using your information to potentially impersonate you later on.

Walter: Wow. That sounds like something out of Mission Impossible or something.

Dee: Or like Inspector Gadget?

Walter: Inspector Gadget would never do that.

Jennifer: And it's very easy now to block numbers. So if you're getting phone calls from numbers that you don't recognize, or you look at that voicemail later and it doesn't make any, you know, it doesn't resonate with you as a legitimate call, you can choose to block that number, and then not sort of have to entertain that moving forward.

Dee: Okay, so consider letting calls from unknown numbers roll to voicemail, and be wary of speaking first or answering yes or no questions if you do pick up, and consider blocking suspicious numbers. So back to your day. You are heading out to work at this point and on your way you hit some construction, and while you're trying to think of, like, possible alternative routes, you call out to your phone's virtual assistant. The digital assistant in a phone has been around for quite some time now, but what we're hearing more about with phones, and the apps that we use on those phones, are starting to use new technology like Artificial Intelligence. So what are you conscientious about with this new tech and how our mobile devices are continually adapting?

Jennifer: Insert tense music here.

Dee: You heard her, Grif.

(music plays)

(laughter)

Jennifer: So one of the things that concerns me is also one of the things that I greatly appreciate about my device, and that is just the mass amount of storage. One of the things that worries me is the fact that your information is no longer just local to that phone. It is being stored in the cloud, wherever that might be, and so that now means that your information is in places where you may not understand where that information is being stored. So again, understanding the privacy policy of the applications that you download, to understand where that data is being stored, who has access to it? Uh, who maintains persistent access even to information that's on your phone is incredibly important. Things like traffic apps, you know, they're trained to learn your habits. They're trained so that when you get in, would you like to go to work now? Would you like to go to, you know, your happy hour of choice? It's Thursday. Would you like to do that? Again, which is one of the benefits of that. It makes our lives easier. But stopping and remembering that insight does not solely reside on that phone. That that insight is being used potentially by someone else or host of someone else for some for some other purpose. I heard a phrase many years ago that if the service is free, then you are the product. If you download a free app to use that free app, then you are the product. They are selling you. They are selling your habits. They are selling your data. And so again, being mindful of when we use that. I, I tend not to take a never shall we ever. I think it's being more prescriptive of when does it make sense to use this kind of technology? And when is the risk simply too great? And I think there's a balance to be met, and each person is responsible for sort of deciding that on their own. But it all goes back to cyber security practices, keeping your software updated, reviewing and managing data sharing settings. I don't know that that's something that people often do.

Walter: Okay, so be mindful of what information your apps have access to, consider changing those settings as appropriate, and understand that information might be stored outside your device.

Dee: Talking about your phone, is there ever a situation where you might be concerned that something suspicious is happening with it? Are there signs that you look out for or steps that you take when something just doesn't seem right?

Jennifer: Yeah, absolutely. I think some of the more suspicious things that jump out at me if folks should be concerned, are things like sudden or drastic changes in your battery drain. If you tend to only have to charge your phone, you know, at the end of an average day, and then all of a sudden a drastic shift where it's lunchtime and now I'm having to plug my phone in. But all of my apps are closed, so nothing is running that I'm aware of. That could be a sign that your battery is actually being used or drawn from apps that you may not be aware of, because maybe there was a malicious link that was clicked without again uh, intending to do so. And so there may be apps or malware that are consuming those resources. You might have unexpected data spikes. Frequent apps that crash or freeze on you. I used to be able to click, click, click, and it did just fine, and now it's pausing, and it's freezing up on me. Deleting that app and reinstalling it,

rebooting your phone are great options. Unexpected pop up ads or redirects. That's another sort of sign that there might be an actor that's trying to push you to click on or to go to a particular site. Sometimes strange noises and vibrations - we've seen reports that this has happened. Certainly if your phone or device is making a strange noise or vibrating for no apparent reason it could be a piece of malicious code that just is not well made. And so there are certainly some things to be concerned about. I mean, I've given you sort of a laundry list of things…

Dee: Yeah sure. Of course. Yeah.

Jennifer: ...that might cause people to say, oh my goodness, what can I do about that? I think the age old just rebooting your phone in some cases because some malware malicious code does not persist or does not survive a reboot. And so when asking yourself, when was the last time I really rebooted this device? If it's been weeks, I would recommend that that be sort of part of your regular cyber security routine moving forward.

Walter: That's all really helpful—so watch out for abnormal behavior from your phone and when in doubt, reboot. So, to continue on with the day here, Jennifer, you get to work and later in the day you are asked to purchase some items for that upcoming company party. So, you head to your favorite internet browser, you search for the item – party hats, and you click on the link of a site that looks like it carries just that. This page looks legit, but you notice that the URL, or web address, seems a little different than what you would have expected. Now, you shake it off, this is probably just some update done to the official site, right? And you can continue with your purchase. Right?

Jennifer: I think you have to always trust your gut with things like this. Especially if something seems off. You know something that's counterfeit, a malicious actor, or a cyber actor, a scammer - whatever your sort of term of choice is, they want to be as close to the real thing as possible. They want you not using your critical thinking skills, not pausing. They want you click, click, click. We've actually seen a rise in quote unquote sponsored links actually being malicious links. So if you go to search for something, party planning activity of your choice, and at the top you'll often see, say, three or four links at the top of a search engine page, you may notice the word sponsored above them. I tend to skip past all of those and go down to what are the quote unquote legitimate sites. Skipping the search engine, going directly to the store's website is certainly an option. We see some really interesting misspellings in URLs often. So there might be an extra period. There might be an extra dash. There might be an extra odd character. And again, if you're just moving super quickly through your day as we all are and we click on something because it looks so close to the original, that's oftentimes how we sort of make those those errors. Even if you are on a legit site and you feel comfortable about it, I think you always have to be mindful that your banking information is valuable for that third party. So that that web front questioning well how likely is it that they have done their due diligence from a cyber security perspective. So being mindful about what form of payment that you use, not using things like debit cards as an as an example, um, not using things like routing and accounting number. I think there's certainly always an opportunity to use things like Apple Pay or Google Pay, which really provides some level of anonymity. There are a couple of other services out there, is something that has increased certainly my comfort when I'm making purchases like that. It also makes it easier sometimes to dispute charges later if it turns out to be a scam.

Dee: Those are all helpful insights. So, be careful about sharing financial information, go straight to the official link, rather than those sponsored ones, and be wary of those misspellings that might redirect you to a malicious site. Back to the task at hand - party planning. You've used, let's say, Apple Pay to finish up ordering the items from a legitimate site that you feel is the correct site, and you wrap up your work day and you're heading home. You get home, you and your significant other are making dinner for the family. One of your younger kiddos comes over and grabs your tablet, wants to play on the tablet until dinner is ready and you are quickly OK with this premise, you know, peace and quiet time is always welcome. Since you regularly let the kids play with the tablet, there aren't any other precautions to take with that particular device right? I mean, they're on it all the time. Likelihood they're just gonna watch a movie or cartoons or something like that. No other precautions necessary, right?

Jennifer: I think, if anything, I'm probably a little more suspicious because whatever critical thinking skills and energy I have to apply to it, they just don't have, oftentimes. That's just not where they mind space is. And in some cases I love them for that. They just have a very, you know, open opinion of the world. And so I think we have to be especially mindful when our family members, especially those both that are younger and may not have a lot of experience, or especially in my case, where I have older family members who just are not as cyber aware but have a very just a very open impression of the world. There's a couple of options there. One, I know parental control software has become really popular in the last few years. I've mentioned before, I have two young daughters. When the oldest of the two, we decided to give her a device, we had long conversations about what she was allowed to do and not to do on it. And while I absolutely want to believe that she's gonna make the right choice 100% of the time, we didn't rely on that. And we did our due diligence in terms of what settings were available on that tablet, that we could help her make good decisions by not asking her to have to sort of be as vigilant as we know that she just isn't capable of at a particular age. And so many of the operating systems have taken, I think, some significant steps in terms of limiting what content is available, whether that's age restrictions, whether that's keyword content, whether that's not loading certain websites, whether it's a gambling website or inappropriate content, high levels of violence, things like that. And that that gives me a level of comfort as a parent, but also as an Agency officer, that we are instilling in them a deeper understanding and appreciation for what is out there and how they need to take responsibility for that on their own. So we would sit down and go through the settings with them and say, this is why we're choosing these particular things, even on things like digital assistants. When we think about Alexa devices, or Google, or others, there are often quote unquote kid settings. And I think when you look at things like parental control software, I think you also have to remember that brings a different level of complexity. Are you prepared to sort of troubleshoot on your own when the app fails? Have you looked at the privacy setting for that? Because oftentimes you're giving a pretty fair amount of data access to companies like that because they need to monitor on your behalf. Um, I will say too, a lot of telecommunication providers in their own apps often have controls, such as how fast was your child driving? How many times did they pick up their phone while the automobile was moving? That's a tremendous amount of insight that comes right out of the box with the device. We just need to sort of investigate that and and take that into consideration.

Dee: What about the the older kiddos? The teens? What kind of conversations are you having with them about social media?

Jennifer: Yeah, absolutely. This was really interesting, especially when Covid kicked off, because it was, in a lot of ways, the only place where friends and friend groups were getting together. Mom, I need to have this app because all my friends are on here and I'm missing out on all the good chats. We have impressed upon them rules like never sharing your true name in a social media platform. Never sharing personal information like the name of the school you go to, the grade that you're in, what your gender is, um, what your school mascot is. We don't take photos of any person and upload that to the web. So, like a hand or the shadow of something - all good, but never anything that shows us as people - that is not something that we are permitted to share as a family. As I mentioned uh, I have two girls, and so it's been interesting. Now one of them has more leeway than the other, because now she's older and seeing how she is taking on that role, and it was rocky at first. She's trying to be mindful about what she's posting. I still have oversight of that. So having to go back to her and say, so I saw you having this conversation, and she was forgetting oh, wait, you were aware of all of this. And now I have that insight. And so it forced some conversations. But again, I want her to be mindful of what her responsibility is as she grows to be an adult, that this is another sort of way that her behavior is visible and she needs to take responsibility for them.

Walter: So consider using the parental controls for kid of all ages, and be very careful about what information anyone, really, posts online—particularly things like photos or clues to where specifically you live or work.

Dee: So Jennifer, anything else in the space of social media that that you might want to share regarding safety?

Jennifer: Yeah, something that I have found really helpful - going back to this idea of that we are our own best advocate when it comes to what information we want to share and what we what technology we choose to use. There are several, sort of, influencers or channels that are out there both on YouTube as well as other social media platforms that come to mind, who really have built a base around helping users understand the settings in particular applications. What data is released or not as a result of certain configurations. And so if you're intimidated or feeling a little hesitant about sort of diving into the settings of your phone, I would seek out some YouTube channels or some social media accounts to help you understand how to navigate a particular app or just want to know more about how do I set my privacy settings to be more in line with what I want to choose to share? There's also say, on an Apple phone, things like lockdown mode that immediately lock your phone into, say, a minimal set of functions that don't allow links to be clickable, for example. So I think there's a whole host of options available that don't require people to be highly sophisticated from a technical or cyber security perspective. It just takes time. It just takes time and sort of a sense of curiosity to sort of dig into those.

Dee: Those are great tips, and I feel like that's universal against any age group too.

Jennifer: Absolutely.

Walter: Ok, so the day is winding down, and you are getting ready to wind down by watching your favorite show on your favorite streaming service. First though, in the meantime, you decide to check out some of your social media. You know, we've heard that there are these audio video scams that have been occurring these past couple years where people might receive audio or video via social media, or even DM – direct message, of what sounds or looks like a loved one asking for help or needing assistance. Jennifer, what are your thoughts on these?

Jennifer: Yeah, audio and video scams are definitely on the rise, and this is one of the ways that we see AI being misused in some cases, and it goes back to the importance of keeping your social media private, for sure. Understanding what the settings are on your social media accounts. Understanding who can gain access to that information is one way to help minimize the likelihood of something like this happening. Recently there was a Facebook video scam that was going around where it seems like a friend is contacting you via a video call asking for help. As it turns out, it's really just a video that's been pre-recorded based on some publicly available information through social media accounts. And so I think it's a reminder that our social media privacy settings, and what we choose to share through those outlets, really can become input for malicious actors who are looking to either get us to click on something or to take an action, whether it's to give our money away, whether it's to share more personal information than really we would otherwise, just remembering that that is a possibility. I think if you get messages, too, from friends or family saying, hey, I need to text you this code, I'm trying to recover my email account. That's another way that we've seen cyber actors try to gain access into people's data. Don't agree ever to receive codes or share codes or click on a link again, going back to sort of where we started a lot of this conversation. In order for the scammers to gain access, they needed to trick you into sharing that code with them so that they could essentially take over your account.

Dee: Best to just to call the person directly?

Jennifer: Directly. That's right.

Dee: Yeah.

Jennifer: Even if you think it might be the right person say, hey, let me give you a ring back and immediately call that person. Very typical advice, too, when we saw earlier where a lot of people were getting calls from banks, financial institutions saying your account's been broken into or hacked into hanging up that phone and calling your bank directly back and realizing that that was not the case. Always a safe bet.

Dee: Great.

Walter: This is also probably a good time to note that CIA will never attempt to contact you to elicit money or personal information or to attempt to do so as part of some kind of vetting for a date or something like that.

Dee: Absolutely.

Walter: No one claiming to be from The Langley Files will ever contact you.

Dee: I mean, as much as we'd love to.

Walter: Yeah, indeed.

Dee: Ok, so you finally made it to the end of the day. You're sitting down to watch tv, but is the tv watching you?

Jennifer: Probably in some way. It's definitely interested in your watching habits. Again, one of the benefits that I think we all derive is you turn on that TV and boy, you've got a really personalized experience and your experience doesn't look like my experience. Or maybe it does. I don't know. We could have some similar interests, but remembering that that is data that is collected about your habits. I think also it's a reminder, too, that your devices like TVs, like smart speakers, and things like that, also have to be updated.

Dee: Walter I don't know about you, but I definitely learned a few things sitting here across from Jennifer.

Walter: Oh yeah. We did a previous episode on CIA travel safety tips—

Dee: Which was Episode 10…

Walter: That's right. And this goes to show, though, that you don't need to leave home to benefit from CIA-like situational awareness when it comes to cyber safety.

Dee: Absolutely. So thanks again, Jennifer, for agreeing to come in and chat with us. We appreciate you being on the show, so thank you very much.

Walter: This has been super helpful. Thank you, Jennifer.

Jennifer: Thanks so much.

Dee: You're going to share your notes with me, right?

Walter: Absolutely. Just a heads-up that the first three pages are mostly about avoiding basements.

Dee: One day, I will come up with a good segue to trivia.

Walter: They're all good.

Dee: Ok, so we're just going to jump right in.

(*music plays*)

Dee: So let's get back to that trivia question that we reminded you all of at the beginning of the episode. So, at the conclusion of our two-part episode featuring the legendary Black CIA officer, George Hocker, we asked the following trivia question, brought to us by our friends over at CIA's World Factbook. As we talked about on the episode with George, he spent a good majority of his career on the African continent. So as we focus in on Africa, the question is - which country is slightly larger than twice the size of California and is the only African nation to have both Atlantic and Mediterranean coastlines?

Walter: The answer is Morocco. Strategically located along the Strait of Gibraltar, Morocco's population is found mostly along its 3000 km of coastline, and the Atlantic coast specifically, proves to be a particularly rich environment for fishing.

Dee: And now you know.

Walter: And now for our next trivia question. This year marks the 50th anniversary of an extraordinary feat of CIA ingenuity and a mission with an incredible yet believable cover story, which included a well-known billionaire and the supposed "depths" to which he would go for some minerals. Our question to you is – what was the code-name of this now publicly-known mission? Hint – this one was mentioned on Episode 5 of The Langley Files.

Dee: So stay tuned to the next episode for the answer, unless you want to take a peek over at CIA.gov and read all about it right now.

Walter: That's it for this episode, everyone.

Dee: Thanks to our audio pals, Corey and Grif, and thanks to all of you for listening…until next time…

(*music begins*)

Walter: We'll be seeing you.

(*music continues*)
Walter: Have you ever been fishing?

Dee: I have, but definitely not in the context of cyber security. I mean, it's old-fashioned rod, reel kind of thing.

Walter: (laughter) Right. Worms.

(*music ends*)