Ep. 74: Is it 'Fishing' or 'Phishing?'

Welcome to Sword and Shield, the official podcast of the 960th Cyberspace Wing. Join us for insight, knowledge, mentorship and some fun, as we discuss relevant topics in and around our wing. Please understand that the views expressed in this podcast are not necessarily the views of the U. S. Air Force, nor the Air Force Reserve, and no endorsement of any particular person or business is ever intended.

Welcome to another episode of the Sword and Shield. I'm Chief Master Sergeant Christopher Howard. 960th COG senior enlisted leader. And today I have... I'm Samantha Mathison, the 433rd public affairs specialist. But I also function as 960th PA. Awesome, Sam. Once again we're going to talk about you know some cyber stuff. Um and we use the quotation marks of stuff. It's always with the bunny ears, you know when it comes to uh these terms and phrases in the cyber world. So some of them can be kind of misleading, especially if you don't really know what it is or what it's referring to exactly. So chief, if you don't mind, we'll go ahead and segue a little bit into today's subject matter. So Chief really wanted to geek out bunny ears on phishing and whaling. So are we taking a trip on a boat into the ocean? So I want you to think of jobs, right? So you have that boat and you just kind of floating down the down on the gulf since we're here in Texas. Um and we've got our poles in the water, you know, that's what we think about fishing right in general? So we're fishing and then, you know, we're gonna go after uh after sharks or whatever, and when we talk about cyber and we talk about fishing um a little bit different, but kind of the same, right? So um what they're doing is they're casting out of line cyber wise right through e-mails through text messages and the other formats with the idea that they're laying the bait out, right? Um And there the idea is that they're going to be able to get something to bite on it, they're going to click on something and that's going to open up a vulnerability for them to kind of get after and then um exploit that information or exploit uh the systems that they now have access. Um I don't know if you remember the last time you took the cyber awareness challenge, Actually, it's part of the cyber awareness challenge is fishing and understanding what fishing is and you know, but we're going to dig into it a little bit more today, I think awesome. Sounds fun. So what is phishing? Right, what is phishing? What is it? Is it, I mean it's spelled differently too, right? It's a it's a ph, right? Instead of an f just to be clear, right? You get the grammatical pieces out. Um but it's actually a criminal act more often than not, right? So what they're trying to do, you know, the whole point of fishing is predominantly email. It's a cyber crime that you know it's really about deception. They're going to send you an email saying hey you need to update this information. I think that a lot of people have seeing those e mails like hey or even phone calls or text messages like one of my favorite phone calls I've gotten recently is um the I. R. S. Has found that you have uh you know oh the money they're going to shut down all your accounts and if you don't call us for right now with this information then you will be in big trouble. And then there's been a like and I guess a warrant put out for your arrest right? I've gotten those two. So the first time I heard that I mean I'll be honest the pucker factor went high right? Right? And after I

took it to a couple of seconds to listen to it breathe through it like nah not so much right? But typically the cybercriminals are looking for things like your date of birth, right? Um your social security number, your phone number, credit card details, home address, password information like that's another common one right? Hey your passwords out of date, go ahead and click here to update your password or hey um you know your credit card has been is in default click here to look at these things and they want you to punch in all this stuff. Right? The whole idea is that they're trying to gather that information in leverage it for nefarious actions. Right? So yeah. Yeah. So chief I actually do have a question because I received a phone call recently and um uh this is a new one on me but I'm pretty sure this was a phishing attempt. So recently I got a phone call from uh this company, it's an investigations company, I'm not gonna call out the actual name, but they called me out of the blue basically saying that there is about $12,000 in a state claim out on my name and they're searching for me so that I can get money right? So of course you know the only reason I answered honestly Chief was because I was expecting a phone call from someone else um and I thought it was this other person but it wasn't. But anyway basically they were wanting to confirm my home address in my email, that's what they were wanting and I was like now not going to do that, I'll call you back you know And so later on I ran a Google search on them and um there were some positive reviews for them but there was also a lot of like this is a scam. And so because it was so suspicious, you know I fully intend to not take the bait and answer that but that is a new thing um that I heard recently usually um people are wanting through email uh like a prince from another country in Africa infamous one, right? Yeah. And if you help them, but you know, temporarily, you know donating about $6000 or however whatever amount to them, you know, you'll be made rich and famous, right? Yeah. But no, I mean these things are effective right? According to the FBI about $57 million just in the past year was lost um to phishing schemes, right? You know, and I think that, you know, your example brings up some key points there, right? So what is the it's always a tagline think of it from a marketing perspective, almost I'm going to give you an offer that you just can't refuse. Right, okay, you've got money coming. Oh, so you're excited, right? So the whole idea is let's see if we can get you to drop your guard for a second or inactive since an emotional moment, like fear, excitement or something like that, right? Because um you know, the primal brain kicks in. Yeah. And you know, like, oh in the excitement, adrenaline comes up and some of the cognitive reasoning and logic pieces start to kind of come down, right? So then you want to act fast, you want to get after this thing? Okay, so I got money coming. All right? So, okay let's go ahead and send this information off, right? And then you end up; well we need your bank account so we can get this money to you right away? Oh here's my bank account, right. Yeah. I'm going to make 12; I'm going to make $12,000. Next thing you know the five grand did you have in your account gone? And you're like, what the heck, what the heck. Right. And then there's the buyer's remorse, right? I can't believe it fell into it, right? But they're predators, right? And they're out there trying to find that stuff. Um and you know, the thing is that a lot of times we'll even use letterheads that looks similar, right? Um some of the key things to look out for theirs are this offer too good to be true. If it's too good to be true. Take a take a pause. Right, okay. If this is

really true. If I don't get to it this second, it's probably still going to be there, right? Um you know, it's like I get all these text messages, you've won $100 gift card for this. You $100. All we need is your account information or we need your address or something like that click this link, right? So you know, again they're trying to get that to you. Um But ultimately takes a step back, look at it, look at the letterhead. Is it, is it look legit? Sometimes it does. Sometimes I don't you're not an expert right? All the things to look at, right? Um does this seem logical, right? Um are there misspellings? MS feelings? One of the key indicators there? Right. Um and then when I read it is that I feel like a real letter right? Because you'll notice especially in the initial read write the brain will pick up on little things and just make corrections. Especially as you're getting that emotional sense like okay wow I just want and then you go back and you find out okay. Um they spelled 1000 wrong. Right? So I'm getting 12 you know Susan's right? We all want $12,000 or um you know the length isn't doesn't coincide with the company name. Like little things that go in there and then. Okay. The other pieces is a what kind of information are they asking? How do they want me to contact them? Why are they not contacting me directly if they found my email address? Right. If I really resonate estate and it's my money, how did they find my email address? And not necessarily send me a certified letter. Right or why didn't I get a I mean even with the phone call you got to be weary but there'd be a couple of different ways that would probably try to contact you. Right. Um and again that whole thing about is this too good to be true? Right? You have to definitely check that out? Right. So it's always good to go into any kind of phone call or notification of any kind with a little bit of cynicism and suspicion because yeah, you definitely don't want to lose your identity, you know, or money specifically right now. And you know, going to some of those key indicators, right? You'll see things like amazon customer support, um your bank or a bank. Right? PayPal are used quite often. Your cars extended warranty cars, extended warranty. Right. And those little details are in the U. R. L. Right? Which is that the link like I talked about before or the way the attachment sits and little things like that? And there are multiple types of fishing uh examples. Right? So there's regular phishing email than their spear phishing? Right? Spear fishing is a much more targeted phishing email attack. Um and it's you know, collected by the victim or the victim's employer. So they're looking for specific information um and specific targets, right? Uh and they're relying on these emails to really trick you to get you into that um or take you to a popular site or try to draw you in that way and collect that data. Yeah. So what exactly does that look like? So spear phishing versus just regular fishing? You said it's more targeted. So um what does that mean exactly? Spear fishing is usually using spoofing, right? So it looks very legit. Um and it it's that it just depends on what the end goal is. Right? More often than not. It’s always about money, right? Because I think we've talked about it during our previous podcast about the cyber domain and the cost of entry, right? Cost entry is really low. Um, so that allows for more criminals to be in the domain and hence why there are a lot more active. And that's why you end up having statistically higher number of criminal acts. Then let's say, you know, foreign actors and session, it doesn't eliminate them from that, that that uh, example, but it is predominantly meant to get information about you so that they can leverage your identity. They can leverage your bank account; they can leverage something about

you to make money off of you. So you are usually the target or another effort is to have access to something you have access to, right? Um, as an employee then they're looking at making money from that company. Right? So you mentioned most of time it's money like what is another goal that these hackers are bad people could have. So, another way of doing this is fake websites. Right? So, again, it's just collecting more information. Um, uh, the idea is to leverage that information or that access again for nefarious actions, right? So, um, corporate espionage is a very big industry as well on top of the money, but again, always comes down to the dollars, right about that money. So let's just say that we were working at a pharmaceutical company at the beginning of Covid, right? And we're just we happen to be a couple of admin um working in this company and there's rumors that we're making progress on something. So maybe we have access to information that shows. Okay, well whom do they just hire? Um where, what supplies, what supplies are getting? Right? So we're making those compounds. What are some of the things? I might be a law G. But I have access to all the orders. Right? So now they know what chemicals were buying two then produce this product or maybe they know what kind of engineers were hiring to make a product. Maybe all of this information can then can be co located and leveraged against us, right? Or an organization from a military perspective, that's the same way. Right? So if we get hooked in a spear fishing or fishing expedition and they can get information um in our roles, right? They might know that we're changing our posture. It's Opsec, right? So being able to co locates that information and then uses it against another organization or profit from it. So would you say the tactics are slightly different when they're fishing for information versus just money? Um I think when we talk about it comes down to the actor. Right. So the one that's actually perpetrating the fishing event or any of these other events, it's um the level of sophistication will improve, right? So when we're doing a fishing expedition at the lower level we're talking probably um Not always more often less sophisticated criminals. Right? Um we're casting a wide net. They're pushing out a lot of things. Right? So how some of this work? Right? So how did they get my information? I think we've talked into other podcasts or we will definitely in the future um discuss how does our information get co located and then it gets sold. Um I don't know that a lot of people know this, but all this information that's gathered from you. When you enter contests. When you enter websites, when you sign up for newsletters, all this stuff goes into information with a bucket that together and they sell it. Um there's actually companies out there that sells what they call universes or sub universes or portions of a global list based on certain details. So when you put in for information in there I as a person as a company, I can actually buy a list of X. Number of people that are interested in. Uh let's just say um deep-sea fishing. Right? And then I get all the information. I'll get their phone number, I'll get their email address, I'll get their name and um I'll get some details that they're like fishing. So now I have a list of individuals that I can send out a text to an email to or a letter to saying, hey I heard you like deep sea fishing and I have a great deal on a fishing expedition for you today, Click here Today and save $150 and catch the biggest marlin of your life. Right? Uh, and then now I've got them right now with that said maybe I get them to sign up for something else or maybe I get them to click on something over. Hey, you were on one of our company partner’s boats recently and

you left something behind, click on here to get your information, your credit card validate your credit card information. Now I can click that now. I have the credit card. I can use it. They already know they have disposable income. Right? These are things I can use. So I'm kind of sending out a very wide net based on this and you can do that with anything. You can do that for veterans. You can do kitten lovers. You can do, you know, you know anybody that likes to do crow chain, whatever it may be, any subject of information. You can buy that and then leverage it for these types of attacks and it's not all that expensive, especially if you get a couple of wins on this thing. Yeah. So not only do we have to be wary of phishing attempts, but we also have to be wary about what we're signing up for online and the internet in general is what I'm hearing and that's, that's pretty sneaky, especially the part about Yeah, you love something behind, you know? And so that kind of leaves a person potential big time an evil human being. So I think you know that you just act like it. Yeah, Yeah. But yeah, I mean that is pretty sneaky, you know, so maybe you are actually missing something, you know? And so you're thinking, oh, you know, maybe that's where I left it because this email text, what a phone call person is saying that you left something and it just so happens to be this thing you've been missing for a while. So unfortunate confluence of events can potentially lead you down a bad path where you lose your identity, you lose all your money and next thing, you know, you're suffering right with you, you know, and kind of digging deeper into that, you know, what other reasons why we do it other than just making money installing malware, right? Um then they can do a couple different things, right? Um and then there's also a slave body, right? Basically what they do is like if you click on this, you give them access, they have access, and they have a back door to your machine. And then what they can do through some coding and some malware is actually they can slave your machine and leverage your Internet connection and your computing power to get after other problems. And then even leverage it as a part of a larger network for computing purposes and for routing purposes. So to hide things inside of a bigger network? That's pretty crazy. So how would a person know if they're machine has become a slave as you put it to, to be honest with you, you got to run for the common individual. It's really about keeping your antivirus up to date. Right? So every time one of these things happens, our, uh, there's a large database that gets shared amongst companies, um, that share what's going on to a certain degree. Um, and anytime there's a known threat that's identified, that gets updated. So those software updates, that antivirus update is then scrubbing, looking for the keywords, the signatures there, um, to find out if that's information on your, on your, your computer or your device and then being able to isolate and remove it, right? Or then also to prevent it. Right? So your antivirus, everything comes through that and it's kind of a net to catch all the comes through. Uh, we'll call it the filter for the filter. So what I'm hearing is make sure your filter is up to date up today, right? It's not going to catch everything. And then even based on the fact that there are opportunities for you to bypass that through some of these, uh, these skill sets, but ultimately you must do what you need to do. Right? You need to be cautious about what you share. You need to be cautious about your passwords need to be cautious what you download, right, understand who's sending it to you. Did you ask for this information or not? Right being just yeah, you know, one of the examples I have in

my notes is a funny cat. Video could hide malware, right? So you download this right gifts, pdfs, e-books. All these different things that we normally consume are also potential threats to your digital environment. Yeah, one of the things I often see at least in Facebook land, because I'm always on there is what we call Click bait, you know, and it's basically like these highly, either controversial or just engaging titles, topics, but you have to click a link, you have to click on a video, you have to click on something in order to open it up and usually it is chock full of ads and it takes forever for these articles to get to the point, you know? And so a lot of times I'll see comments on these Click bait articles, you know, of people basically saying like, yeah, it takes a million years to get to the bottom because, you know, I'm over exaggerating, it doesn't take years, but you know, it takes a good, good second or two to get to the point and they do this on purpose because they want to waste your time. They want you to click on these links, you know, and they want you to look at all these ads. I mean that's ultimately the point is to make money for, for these ads and articles. So, um, yeah, people will often comment on them. You know, and I call them the Facebook heroes because they'll just basically say, hey, this is ultimately the point or the screen shot at, you know, and put what the point is, you know, just to save the rest of us normies from, you know, having to dig through to get to the point of these things. And it's, it's, yeah, so that's something else to keep an eye out on at least on Facebook in general is, uh, these Click bait articles, they're usually, and I'm not gonna lie, I've been sucked into him to chief on occasion. I'm like, you know, what happened to this poor little girl who may have been abducted and stuff like that or, you know, it's amazing what happened to this cat, you know, and how that, how did they survive? And you know, it's often these very engaging, uh, topics, you know, and it sucks you in, you know, and it's very easy because again, it's that knee jerk reaction you were talking about chief. You know, you just want to click on it and find out because we're all naturally curious, We want to know, you know, so that's something else to keep an eye out for when it comes to fishing because that's also a way to draw people. And part of that is, uh, is called mass advertising, right? That's a technique that uses online advertisements and pop ups to compel people to click on them. Right. And then that's what allows malware to get installed or collect additional uh, information about you. Another one we haven't talked about is the man in the middle attacks. So what that is, is it's a sophisticated email attack where they actually have two different persons in the same organization or they're connected somehow, um, email and they start emailing them as the other person to collect information. So now you have a trusted in person and another person and I think they're sharing information between the two. So, um, that one is very sophisticated. It's a high-end type of version, but things to look at. So you know, what that said is, how do I, how do I get around that one? Right. Some of this is a trusted person. Why are they asking for information that would normally ask for? Right. So if you, you sent me an email and said, Hey chief, I need your social finding my social, Yeah, that's a good question. Why would I need you or hey, I know that we haven't talked about this in the past. What's going on with operation uh, you know, Snuffy McGee? Well what do you know about Snuffy McGee? You know, did you even know about that little things, right? Or um, hey, I was wondering if you could tell me about what's going on with the, you know, the latest troop movements or whatever

our level, right? But if we're going to, again, going back to, you know, we're going to pharmaceutical company. Hey, do you, do you have the codes for or the access to the database for all of this for all of the ordering? Well, you don't do orders, you do something else. So yeah. Little things. Right. Yeah. It depends on the job function. So that's something else. I think you bring up a good point chief that you got to keep an eye out for insider threats to you as well. And that's something that you can keep an eye out on when it comes to your co workers and people you actually know, like it's always good to have that healthy cynicism and think about why are they asking these questions? You know, and it doesn't hurt to ask the questions. Well, what do you need to know this for? You know, right. It's always good to ask why is that person downloading that disk and walking out of the stick with it. Right. We won't name any names. Yeah. Right. Or, you know, you see that mysterious unlabeled disc laying around somewhere, right? Let's put it in my computer. Let's hit it, see what this is. But you know, there's a lot of resources out there of how social engineering that kind of works and how they're looking at this and then what they're doing to your accounts and your information and actually the Federal Trade Commission, um, if you go to uh, you know, consumer FTC dot go, they actually have a list of things to, to use, to protect yourself from fishing. Um, and what they identify as, uh, you know, protect your computer by using soft security software. Again, your filter, right? You get an anti virus, right? Or the security settings. Um, you know, and then protect your mobile phone by setting software to update automatically, making sure that you're up to date because every time you update your apple phone isn't just because they want to, you know, Jack, your phone do other things sometimes now it feels like that, right? But those updates are how they update the software to look for those signatures and prevent you from getting Jack. Yeah. And the timing may be bad. Like I've dealt with that frustration myself honestly, you know, it's like always first thing in the morning, it takes forever for my computer to finally get to the point where I can use it. However objectively I do know what's happening is software being updated, the patches are coming through. You know, it's doing that scrub that supposedly it's supposed to happen overnight, you know, whenever you leave for the day, but let's face it, it doesn't always happen that way. Usually it's when you try to log in and the computers like, let me do all these scrubs right now and security checks and you're just sitting there waiting what feels like a million years, but really in reality it's only, you know, 5, 10 On a really bad day. 20 minutes. Yeah, that's why they do tend like I have a lot of apple products, I know badly um well. You know where you sit on the fence, right? Um, and the updates happened at night when you're asleep, when you're not normally using it. So you don't necessarily see it. And it keeps you a little bit safer. But another way to protect your accounts is by using multi factor authentication. So what is that? Right? So that's usually uh, you see a lot of your banking applications now require you to sign in, log in and then they're going to send you an activation code or one time use code, which gets into another device that you didn't bring in uh, and plug it in. Right? So use a plug in them by any means. It just happens. They send that stuff to me all the time. I mean I have it for a number of different other websites that I leveraged and use it to get the multi authentication. So it's another sense of security rate. It's another way to, to prove you are the trusted member of that account, right? Yeah. And it can be frustrating,

especially when every account you're trying to get into, does that? And you have to move quickly. You know it does take time and you're like oh man I gotta do this again like come on however it's to protect your information and your stuff so then you know are safe because we all like our money we all like our identities. I'm not Scrooge McDuck but I love my yeah we all got bills to pay, you know we got kids to take care of pets; you know vehicles, all that fun stuff. So yeah I mean in the short term it is frustrating but in the long term it's good it's healthy and just got to keep that what's the environment? Right? So nobody's really happy that the environment changed the point where um in a digital environment that we have um that trust is so thin right? Um There is a natural tendency for us to want to trust information that's given to us um or trust that you know everything's on the up and up and people prey on that and these systems are meant to help prevent that and then protect you from yourself right? Because you're being manipulated uh you know one other way to protect yourself too is uh you know back up your data. So like if you have anything that's uh um important to you especially on your computer or your phone constantly backed that up on a regular basis. Um In case you do get hit and if you lose part of it you don't lose all of it um and then also password protect files, password protect your information, um keep it safe wherever you can type of stuff, you know, just b um safety aware and security minded to kind of get out there, you know? So if again going if things seem too legit, obviously you've got to be, be weary of it, yep. Yeah, chief, well we're running short on time, so I know we didn't get to everything you wanted to talk about, so we'll have to just save it for a future podcasts okay, definitely plenty of things to talk about in the cyber world, of course, especially for Lehman's, people like me, you know, and then of course for our cyber experts that are out there. So chief, I will let you say you have the last minute words on this episode. No, I appreciate that Sam, thank you, thank you for giving me the opportunity to talk about this. Obviously I'm not an expert, I just have a little bit of knowledge and this is really meant to share a little bit of it and make people aware of what the intent here is to share a little bit about what to look for, Be weary of it and then challenge everybody to critically think, so you think these things through um and take a deep breath when looking through these things don't get caught up because your information is vital, your digital environments vital. Um and then from an organization perspective, we also don't want to make you vulnerable to other attacks or make the organization vulnerable to attacks. Um I am confident that most of uh individuals listening are well aware of these things um but it's always good to refresh the conversation and then keep up to date what was going on. So um to all of the our gladiators out there, you know be vigilant, be again safety minded insecurity aware and then go ahead and uh get after it right? So with that said I have to close it out with all right gladiators get out there and stab your enemies in the face through cyberspace.