Phishing, Vishing and Smishing

00:00:01 - 00:05:01

Announcer:

You're listening to the Harris Beach PODCAST, a show that explores evolving issues in the law and how they shape organizations the way business is conducted and how we live and work. The information provided in this episode does not and is not intended to constitute legal advice instead all information content and materials are for general informational purposes only. Thanks for listening. Here's Today's host.

Host
Melissa Pheterson:

Hello my name is Melissa Pheterson from Harris speech and I'm your host for today's episode which will explore the problem of fraud in its various forms and how companies can protect themselves. I'm joined here in Rochester by Dawn Russell, our director of Compliance and Risk management and Ross Hoffer attorney on our Cybersecurity and Financial institutions teams is joining our studio from Harris Beach’s New York City office. Welcome to Dawn and Ross.

So let's start with exploring whether cybercriminals or finding new ways or a better ways to perpetrate scams and fraud.

Dawn Russel:

When you say scams we should talk about the three categories: fishing, vishing and smishing. So scams are often perpetrated through email and we all know that as fishing, but we also get phone calls or vishing and sometimes we even get text and we would call that shmishing. So all of those types of media we need to be aware of that we can receive scams.

Host
Melissa Pheterson:

Ross- how about you? Ross. How about you?

Ross Hoffer:

I would say that the trend right now in any of these scams is really the level of sophistication that the cyber criminals are coming with. And by that I mean if it was five, ten years ago the most common scams were very far-fetched Situation that that most people recognize as a scam. The Nigerian prince scams are the ones that come to mind immediately. But, nowadays cyber criminals are scouring the Internet looking through social media looking, through company's website and really personalizing the attack or hopefully the attempted. When did we see this? When it comes to law firms cybercriminal is posing as a new client and horrid shooting law firms business development groups or you know attorneys who were looking for new matters of but when it comes to a business it can be targeting a sales team, it can be targeting an accounting group, can be targeting just about anyone and these days a lot of that information is easier to find on the Internet. So you can look up a particular business and no not only One it is that they that they sell the product auto service but also know the mortgage they're operating in and cybercriminal can deduce from that who’s going to be the juiciest potential customer for that company? And who would you know who the company most likely respond to so. It's really a level of sophistication indication these days that fool a lot of people.

Host Melissa Pheterson: So are there any red flags or other clues that something that seems plausible and legitimate really is not?

Dawn Russell: One thing you want to look at is the domain name. So many times Caesar impersonation emails and they wall display the name of someone who is familiar to you in your organization. But if you take a closer look at the domain name you'll see that it's often- it's not something that will that matches the organization. But I do think you need to be careful with that because if a bad actor does get access to somebody's mailbox, the domain name can be correct because it is actually being sent out of the mailbox of the person.

Ross Hoffer: I think that people who receive emails in particular, also phone calls or text messages need to be aware of the context. Just yesterday or two days I got an email from somebody who was posing as a as a perspective client asking if Harris Beach as a law firm does litigation work. Well of course we do litigation work. If anyone who's spent any time on our website they would know that we did litigation work. Similarly most law firms have a litigation practice so it was one of those was things that was just a question that had such a readily available answer to it that raised the red flag to me because I knew that the next step would have been okay.

* 00:05:01 - 00:10:34*

Great now that you do ______ here's a link where you can access some documents About my litigation matter and so you know it was one of those things that that did raise a red flag for me and so I would recommend that people look at the context. Verify wherever possible using a second method. So if you get an email from a correct domain name maybe then find the phone number for them. If you may get an email from chase bank about your credit card and you do have a credit card with chase bank. Well call the number on your card and confirm that this is the right that they're calling you for a proper purpose that they're emailing you for proper purpose they're text messaging you for proper for this. If there's fraud then these companies will be reaching out to you, but you know it is very common for companies to be reaching out to you saying that they're following up on a fraud investigation when there's nothing.

Host Melissa Pheterson: Can you share an example you might have come across that might illustration some of these things either something actual or hypothetical?

Dawn Russell: Scams have become somewhat sophisticated. But there's also the unsophisticated scams. Every year between January and April people are getting calls from accountants posing you know to have to be calling them about tax issues calls from the IRS. I've known people who've gotten calls from Border agents saying that they're calling on behalf of somebody who is stuck at the border. There are all sorts of scans that come up and we've seen a lot of them but they really range in and these days the scams are more and more specific to the recipient. They're really becoming coming tailored in a way that they never were before.

And I think one of the big differences between scams that we were seeing tend and even five years ago many times it was just take a shot. There was nothing specific in the scams. Today we're seeing more and more often that they're totally plausible. So Ross mentioned the email that he received asking whether or not we do litigation services- these people are going out there doing being research and then targeting not necessarily a specific person or even a specific organization, but in industry. So they're still using the buckshot method, but they're focusing on a particular industry or something that makes that group unique.

Host
Melissa Pheterson: So we mentioned some measures companies can take to avoid being victims. Should they have formal policies adopted, maybe tailored to different levels of information or just general kind of proactive training or procedures in place?

Dawn Russell: I think every organization in is going to be different. You really need to do a risk assessment and understand where the gaps are or where your organization might be most vulnerable and then tailor that information security and let's not forget privacy as well. Tailor i those programs to the needs of the organization There's always of course the traditional technical controls that we all know about firewalls smell hygiene products web filters encryption of course and of course physical protections- we're all very familiar and understand those. One of the areas that I think people don't think about often is it ministry of controls and one specifically is the education of employees so the weakest link and we're talking about fishing and the way a bad actor gets in through phishing is by fooling someone. They're very good at it but if we can provide more education to the individuals within our organizations have a formal policy procedure and training program. That's going to help cut down on the risk related to phishing scams that were seeing.

Ross Hoffer: I agree I think that education is extremely important on this. I think that when we do trainings for our client they are very effective and I know that the training that we do internally that that's mostly led by Dawn is extremely impactive. I mean it's one of those things that people need to be constantly reminded but beyond the training I think that that there are Proper Protocols and policies that can be put in place. As Dawn has mentioned, you know it's very specific to each business and the business’ risk and what they're facing here. For instance an accounting department should generally have some threshold for a second layer of approval before for writing a check or sending out a wire transfer or something like that because the actors can come in and personally somebody with authority to be saying.

00:10:34 - 00:15:04

Well send a payment to this bank account and you know send the wire transfer particularly early to this bank account, well an accounting department should either have protocols in place for all transactions depending on their risk or for certain dollar threshold to escalate that to a supervisor to require that before initiating a wire transfer; a phone call needs to be made to verify or some other control and again I mean these are going to be very specific to each business, but just some general measures that that people can put in place.

One thing that that we've found to be very effective is having the capability for someone in IT be able to open documents, click on links- really the Do any of these things that that have a red flag associated with them on a computer that is not connected to the organization's innovations network. And this way if there is a virus if there is some sort of hacking attempt, it is not going to get past that individual machine. It’s never going to make its way onto the larger network the way that an individual that is on the network clicking on a link would give a bad actor access.

Dawn Russell: Ross brings up a good point. There are more products on the market that aren't the traditional technical, safety protections that we put in place and one really good example of that is the newer antivirus malware products that are out there. Most of them are heuristic and so they learn the habits of the person in the organization and really all organization should be looking at those. The newer products that are out there those types of methods where we can protect ourselves.

Host
Melissa Pheterson: So is there anything thing that I missed or didn't bring up that you'd like to explore?

Dawn Russell: I think one thing that people should remember going back to the scams and dealing with those- always trust but verify. If something doesn't feel right you should stop. I always say to people in the training class. If it's too good to be true or it's too bad to be true, you should really stop and take a closer look.

Ross Hoffer: I agree with that and I think it's about ensuring that employees or our vigilant and looking out for these scams and knowing that there are these bad actors out there so you know that that's why the training is important but it also needs to be reinforced and so people can be expected to just know it as a matter of common sense that that there are these bad actors out there needs needs to be told to them in informal training and then followed up and then it could be followed up with monthly reminders minders from IT to stay vigilant and keep an eye out for scams or it could be followed up when there's a specific Incident or something that comes up that reported in the news about- Hey guys just so you know. Keep an eye out for these types of emails. They you know they could pose a threat to our organization.

Dawn Russell: And I do think it's important for organizations since to constantly be doing risk assessments so these threats are evolving and emerging so quickly that it's almost impossible to react to them. So if we're constantly doing risk assessments as Ross said. What's going on in the news? Make sure that the folks in your company we are aware of that. Are there new risks to your organization? Is there some sort of new virus that that's out there that's effecting organizations but it's really about constantly doing risk assessments understanding what the risk to the company is and then addressing that risk appropriately.

Host
Melissa Pheterson: Thank you Ross and Dawn for joining us today. And to our listeners and subscribers.

00:15:05 - 00:15:27

Thank you for tuning in. You can learn more about our capabilities related to cybersecurity by visiting our website HarrisBeach.Com.

Announcer: Thanks for listening to the Harris. Beat podcast be sure to visit harrisbeah.com to join the conversation and access show notes. Please rate, subscribe, and leave a review wherever you listen to your podcast.