- You're listening to the HR Mixtape. Your podcast with the perfect mix of practical advice, thought-provoking interviews, and stories that just hit different so that work doesn't have to feel, well, like work. Now, your host, Shari Simpson.

- Joining me today is Nate Peacher. He has been a dedicated risk investigator at Paylocity for the past eight years. He's actively involved in the Association of Certified Fraud Examiners and various industry fraud prevention groups, showcasing his passion for helping people safeguard against fraud. When he's not tackling financial crimes, Nate enjoys spending quality time with his family and embracing the great outdoors. Nate, thank you so much for jumping on the podcast with me today.

- Thanks for the invite. I really appreciate it and excited to be here.

- So this is a topic that I feel like we have seen bubbled up more and more over the last several months, especially the last several years coming out of the pandemic. So I'd love if you could start by maybe walking us through some of the most common types of phishing schemes that you're currently seeing.

- Well, I've seen quite a few. They generally are all the same, meaning that they all want money. And so, it's either money or information to get money. And so, one that I've been seeing for years and years was emails that would go to someone in an organization trying to get a change for direct deposit. It's kind of obvious in that scenario. They want to change your employee's direct deposit and have those funds, instead of going to the employee, goes to a fraudulent account that the fraudster controls. So, on the payday, an employee realizes they haven't been paid. They reach out to the company admin or HR person, and they realize, "Oh, well, that was actually something I changed." And then they end up trying to get those funds back, which is quite a bit of a challenge sometimes. So, that's one that I've seen for years. The FBI had an alert back in 2018 about that. And so a few others that I see pretty common. There's lots of CEO impersonation, trying to get someone to send funds, often gift cards. Sometimes that comes via email or text and even phone. So that's been coming more and more popular. One thing that I've seen more recently is related to fake login sites. And so these sites have, the scam's been around for a while, but the goal is to basically steal the credentials of whoever gets on these sites. And so unwittingly, the users are providing the bad actors everything they need. So they can go in, they give the username, password. If there's like multi-factor authentication, the user gives them that and so provides the bad actor everything they need. And once they're in, they do what they can to try and take money and information. In the example of an HCM platform, they wanna change direct deposits, they wanna change it to the accounts that they control, and they possibly wanna go in and look

at information or even run payrolls. And so that's, I think, the biggest one right now, and definitely the one that we're trying to get the word out.

– How do we as HR practitioners, one, educate ourselves on potentially false login screens, and two, educate our employees on how to know when they're logging into their HCM that these are legit, these are the actual applications they should be using?

– Well, it is a big challenge 'cause you can look at these sites and compare them side by side to a legitimate site, and they look the same. So, visually, the user may not be able to pick up on it. The trick is usually it's in the URL. So, you know, for example, paylocity.com, if it was misspelled, that could potentially be a bad website. And so, they may get to that bad website through an email or a text with a link. They might get to that website through a search engine. And so being trusting, these users click on that, see what looks familiar, and provide the bad actors everything they need.

– Wow. How can companies protect ourselves? You know, I feel like, you know, as an individual, right, I'm always looking at emails, I'm always trying to evaluate, "Hey, is this a real email? Is it not?" You know, you get an email from AT&T that's like, "Hey, you need to log in and look at your bill," right? You might have said that to Shari 10 years ago, and she'd be like, "Oh, click on the email, it's great." Now I know better, right? You go into AT&T's website and you log in the way you would log in normally, right? You don't click on the link in the email. But these cyber criminals aren't just targeting individuals anymore, they're targeting businesses. So how are... What's the difference that you're seeing there between being an individual being targeted and a business being targeted?

– Well, so with the business, they often could be going after, say, an administrator's logins. And so in that scenario, very similar. They would be potentially searching for a website, go on this, or get an email that looks urgent. They go on it, and they steal these login credentials. That can be a bigger deal. So when that happens, you know, there's lots of ways. It can trigger lots of notifications and alerts and things. But one thing that I've also seen is these bad actors, once they get in, they may identify your email and all of a sudden you get a thousand emails. And so the challenge of some of the old notifications alerting you is that you have to surf through or sift through hundreds of emails. And so... The methods are very similar, but they're basically going after the people that have control of either the systems or the money, trying to convince them to move money or get access to information.

– I assume over the years, just like everything else, that phishing attempts have evolved in their technology, that the tools look differently now. How are you educating employees now on identifying or

flagging phishing emails?

– I think they certainly have changed, although I could say, you know, seven years ago, some of the emails that I got almost look word for word to the ones that are still going out. But it's, you know, it's definitely a lot different than an email, you know, quite a while ago that might have been sent to a thousand people or a hundred thousand people. And it's all the same exact wording. So they're gonna specialize these emails to what they're trying to do. So that may actually look like they're coming from the actual user. So often it comes from an odd email address. That's one way that most people would get a red alert. Occasionally, though, an email is actually compromised. So, you know, if your email is compromised, Shari, and I got an email, I might trust it. And so, you know, if you said, "Hey, check out this item," you mentioned a good product earlier. If you sent me the link, I'd probably click on it. And then that might put me at risk. So it's definitely something that's a challenge. How it's evolved, I think they're getting better at getting information, potentially that information that people just giving up themselves. So, you know, on LinkedIn, people like to advertise how great they are and, you know, tell potential future employers about what they do, but they're telling the whole world. So if I'm a bad actor and I wanna figure out who controls the money at a company, all I have to do is go to LinkedIn and start looking who's the HR manager, who's the CEO, who's the person that controls money. And those are the people that I wanna target. So people are giving up a lot of information. There's lots of news out there about breaches. And so some of these breaches that have happened, this information ends up getting into the cyber world and these bad actors either share it or sell it to each other. And so that's another way that these people get a lot of information. But certainly people are giving it up voluntarily, regularly too.

– Yeah, for sure. I... You know, I remember a couple of years ago, there was a phishing attempt going around that enticed you with an ad for a free Chipotle burrito. And there were so many people that clicked on that because they didn't do their due diligence. You know, fortunately where we work, we have a lot of due diligence in educating our employees on what phishing emails look like. Not only do we have annual training, but we have actual fake phishing emails sent to us to test our response to that, which I absolutely love. Additionally, we have giant red banners on anything that comes in outside of our organization. So it is a tool to help us do a little bit of a double check. Beyond those things that I mentioned, how should employers and IT professionals think about educating their employees to get them really bought into this whole idea of cybersecurity being part of their responsibility and not just the IT team?

– Well, I think the things that we do at Paylocity is kind of what I'd recommend to any company. So having that regular training. We have an LMS system that gets that training. One thing I like about some of our

training is they have some that are a little funny and so it makes it less boring. You know, if you do the same training every year, if there's a way to skip to the end, there's gonna be some employees that will. But if you have some training that is kind of engaging and a little funny, you're gonna remember that in ways that you may not think about until you're about to click on something and you kind of remember that weird joke that they were talking about on that funny training. And so, I think that's a good resource. If you're a Paylocity client or a future client, look into that LMS system. And so, that would be a great tool. Like you said, there's phishing testing that you can do. And I've even had clients come to us saying, "Hey, this email looks like it came from Paylocity. Is it?" And they're really worried. And we end up finding out it was them, their internal testing. And so, you know, we had them kind of follow their normal procedures. And but they went from really being alarmed to, "Oh, good, we're actually secure and everything's good." So I basically would do kind of all the steps that you mentioned.

- I like that you mentioned the point about if you get an email that you think is fishy, instead of responding to that email, create a separate email to that person that you know is a known contact and just ask them or call them and say like, "Hey, did you send this to me?" It's such a simple step. And sometimes I think in the minutiae of our jobs, we just get so busy, we don't think to do that simple step. So I really appreciate that example. You know, what are some big mistakes that you've seen companies do that leaves themselves vulnerable to cyber attacks?

- Well, you know, we talked about kind of clicking on links from an unknown source, that is a big one, you know, completing some sort of request, you know, that can obviously cause problems. So, if you get an email requesting that direct deposit change, you make that change, the money's gone. It's very hard to get back. If you start helping with resetting passwords or provide credentials. Sometimes it's the easier path for someone that is out there and they just want to be helpful. And honestly, there's a lot of employees out there that need help logging in. And so, you know, a good HR rep probably deals with that on a regular basis. And so, you know, just trying to help out, they end up going a little too far and end up helping the wrong person. Now, as far as IT security, not necessarily the expert on that. And so, you know, there's certainly things that you wanna do to make sure you're secure. So, having the proper software, you know, VPNs are great. Any multi-factor authentication that you can enable, I always recommend the highest level of that. And so, definitely wanna work with your IT to make sure you have, you know, the endpoint protection, cloud-based security, and they monitor all the network traffic. But also, one of the big things is you wanna have a plan. So, having that disaster plan, recovery plan in place, you're gonna know what to do and what group of people to get together if something happens. But education employees is really kind of, I think, at the

top of the list on how to help, for sure.

– So let's say worst case scenario happens. You've been compromised, you've had a cyber attack. Potentially your client data is compromised. What is your legal obligation as an employer to both potentially your clients and your employees to really mitigate damage and prevent any future incidents?

– So, it varies by state, and so the legal obligation can vary by state and what sort of data may have been involved. So, in that scenario, you would basically want to refer to your legal counsel. and have them review and advise. So, I'm not the expert on that. I know there's some states that require notification a lot more than others. And so, if you're in one of those states, you might have a little more work to do, but it's definitely something you wanna get in contact with the right person to confirm.

– I absolutely agree. You know, so many things in HR, it depends or contact a lawyer, but we mean that with the best intent because you wanna make sure that you are crossing those T's and dotting those I's, especially if it's very sensitive client data. Like you talked about direct deposit information or social security numbers or any of that, you know, PII that we've talked about in the past that we're all really familiar with. So you know, as we were talking, one of the things that I was thinking about was, the videos I have seen now online that are being generated by AI, you know, considering them deep fakes per se, and I've heard stories where people are receiving, quote, unquote, "FaceTime calls" from loved ones asking for, you know, money for whatever, and they're very believable. What are your thoughts on that and how we can start to think about putting things in place to protect us from that?

– Yeah, I think AI and these deep fakes is gonna get to be a challenge that it's gonna continue and get worse. You know, there's a talk of zero trust. But, you know, if my mom were to FaceTime me and I see her face and I hear her voice, I'm gonna immediately go to a very high trust level. And now if she asks me to send money through a pay card right away, I'm gonna have some red flags. But, you know, I think AI is gonna be a tool these fraudsters are gonna use to be able to collect information and make these attacks way more believable and make it at a speed that is just faster than it is right now.

– I agree. I did hear one tip, a personal tip is, you know, for those that are your loved ones or the people that you're really close to create some sort of code word that, you know, you don't post anywhere and make it something ridiculous so there's no way you would accidentally say it. And I thought that was such a creative idea, just such a simple way to make sure that, you know, hey, if you have a red flag, is there something you can ask this person to, you know, to say to you that would help identify them as the real deal. As we wrap our

conversation, I'd love to hear as you look ahead, what are some new cybersecurity challenges that you foresee for businesses and how do we prepare for those?

– I think it's gonna continue to evolve. So these guys, they always wanna take the easiest path available for the most money they can steal. But as technology evolves, automation evolves, and AI, what might have been the easiest path in the past may not be the easiest path in the future. So it's gonna be something that I, you know, I'm kind of waiting to see what happens. I don't know if I've got big predictions. I do think that automation and that AI, like I mentioned, it's gonna be a big part of it. Things like these fake websites, I don't think are going away. You know, when you can get a website shut down, but if they've got an automated process to set up a new one with one click of a button, you know, it's probably a lot harder to shut it down than it is to restart it. And so I think that it's gonna be a scenario where people are gonna be a little less trusting across the board and remote work isn't going away. And so you don't have the ability to, you know, stand up and walk over to someone's desk and just mention, "Hey, I got an email that looks a little weird. Was that you?" And so you might have to make this phone call. And so... In a way, I'm kind of excited to see the weird things that these guys are gonna do, but I also, you know, kind of anxious as well. And I hope that everybody can kind of stay one step ahead of them, you know? I think a lot of the fraudsters that I may have, or the work that I see from some of these fraudsters, I think a lot of them are overseas, and that makes it challenging. There's not necessarily too many ways to confirm that, but there's has been quite a few indications. So, I hope there is some sort of way that becomes better to be tracked and legally stopped and so maybe a better coordination between these countries. It's hard to say.

– Yeah, for sure. There's a lot of complexity when it comes to this, but Nate, this was such a great conversation. I know our audience is dealing with these kinds of things on a daily basis. So thanks for all the tips on how to educate our employees and keep our organization safe. I appreciate you jumping on the podcast with me.

– You know, I'm gonna share some links. So you mentioned the breach. I've got a guide that FTC has regarding breaches. And then there's some other things from Paylocity that we can share that kind of go over. You know, if you have an incident where something has been compromised, a lot of the steps are kind of basic. You're gonna reset your password. You're gonna change your username and security questions if possible. You know, I mentioned MFA and then really go into your IT and go into the experts and saying, you know, what else do we need to do? And they hopefully will take it from there.

– Wonderful. Well, I will make sure to include those in our show notes.

– All right. I appreciate your time. Thank you so much.

– I hope you enjoyed today's episode. You can find show notes and links at thehrmixtape.com. Come back often and please subscribe, rate, and review.