Lowenstein Sandler's Cybersecurity Awareness Series

Session 3-
Phishing: Cybersecurity's Biggest Threat

By Kathleen McGee and Ken Fishkin
OCTOBER 2021

Ken Fishkin: Welcome to Lowenstein Sandler's Cybersecurity Series, where today we're going to discuss cybersecurity's biggest threat, and that deals with phishing.

Kathleen McGee: We're also then going to talk a little bit about some other really common incidents that happen to organizations due to data breach issues, which can include wire fraud and imposter issues. So let's start with phishing. What is it?

Ken Fishkin: Phishing is basically a scam, and it's done through email, and it's a way for a malicious person to send you an email where you think it's coming from somewhere else, and it's really a ... and it's not, and they're trying to get you to either click on a link or open up an attachment where they could take over your machine potentially or get into the corporate network with that malicious software that you've installed.

Kathleen McGee: So, Ken, what are some of the things that an organization can look for in an email that might tip them off that this is actually a phishing email?

Ken Fishkin: All right. Well, the first thing that you should do is take a look at the ... what's called a header, and you can see who, who it's from, and you'll see where it might have a person's name, like Kathleen McGee, in there, but if you look closely at the actual email address associated with it, it'll be complete ... something completely different. So you want to make sure that that name matches up with the actual email address, so that way, you know it's correct. And another thing is a lot of times the signature of that person, if, if it's fake, it's going to come from, if somebody signs their name, usually Dave, and you see it says David, or it says their full name, then you know for sure that it's probably not real. And there's other indications also, the time might be wrong–it might say 4:00 a.m. that email was sent, and the spelling and grammar might be slightly off. So if you have any hesitation at all, you should always–and even if, even if it looks perfect, but it's an odd request–just call that person up or text them separately. Don't email, don't email them back and say, is this really you?–that's the last thing you want to do–but you want to make sure that that person definitely sent that email. So use a different way of communication to verify that request.

Kathleen McGee: And what should an organization do if they suspect that they're seeing an increase in phishing email traffic, which might, might indicate that they're, they're increasingly becoming a target for a potential attack?

Ken Fishkin: Yeah, so what you need to do is you have to look at third-party solutions out there, and there's plenty of companies that basically launder your email. And so the email goes through this laundry cycle, and then you get clean messages, and it's not 100 percent, and that's why you still have to do education, but it is ... it, it, it knocks out thousands upon thousands of emails that you would normally get.

Kathleen McGee: Everything goes to the junk file.

Ken Fishkin: Right, exactly.

Kathleen McGee: Right.

Ken Fishkin: So it filters out the ones that are definitely junk, and the ones that are questionable, it tells you that they're questionable. And so it's not foolproof by any stretch of the imagination. And it's another cat-and-mouse game where the technology tries to, you know, prevent these types of attacks, but they're always coming up with new, clever ways. And it's my job to educate our employees on those different techniques, whether it's gift cards or wire fraud attempts. It's, it's something that needs to be done.

Kathleen McGee: When a phishing exploit is successful, we are also seeing a lot of circumstances where clients then face more than just ransomware. And I thought it might be useful for our audience if we've talked through a couple of those very common situations that they may find themselves in because of a phishing exploit.

Ken Fishkin: Yeah. So, identity theft is definitely one of them where, you know, they, they want to learn more information about you, so they'll, they'll, they'll keep you engaged in a conversation. And, and then the next thing you know, they could be buying a house under your name or something like that, or, you know, it's, it's something you have to really pay attention to. And they prey on your fears and your inattention because you're busy doing other things, so they'll say urgent requests in the subject ... Any, anytime there's a sense of urgency in an email, give it a second thought when you're ... before responding, unless you know for sure that that person was legit. But that's another way, and they also, especially during times with COVID, they use scare tactics also. And they, they, they look at your Facebook accounts sometimes, they'll, they'll see what activities you're involved with, and they, they will go in deep and do their best if they really want to get you. So it's pretty serious.

Kathleen McGee: One thing that I wanted to highlight for our viewers today was another aspect of, sort of, bad things that happen because of phishing, and those are corporate wire fraud concerns. We're seeing an increasing number of clients who have an employee who makes that bad click because of a phishing email and then ends up opening up their whole system to the bad guy. But what the bad guy does is orchestrates on the back end a whole series of changes to the infrastructure of the email system. They might change rules, for example, in your, in your Outlook for email so that you think you are

getting all the emails you're supposed to, but it turns out they're being diverted to the bad guys. And the second thing they do is then start to orchestrate fake requests from real customers for wire transfers. So we've seen several substantial wire fraud cases over the past few years that really started out from a simple click on an email.

Kathleen McGee: And there's nothing worse than realizing three days too late that you sent a lot of money to the wrong address, because it's really difficult to get that back, and obviously that's when you call your counsel because you're gonna need their help in trying to recoup, you notify your bank. There are certainly some emergency measures that you take, maybe even notifying the FBI, but it's important to be aware that hand in glove with training your staff on how to identify a phishing email, you also think about how to protect when something like that happens by training them on, for example, wire transfers and financial transfers and being extra sure you're actually sending it to the right place.

Ken Fishkin: Yeah, so that's a, that's a great point. It is very important to have policies in place so that if there's any kind of change of address, oh, anytime you're sending money, if any, if there's any kind of change in the wiring instructions, you contact that person, not through email–you call that person, you figure out a different means to verify that that address is actually correct, because otherwise, you can easily fall victim to that. And that's a very good point. Absolutely.

Kathleen McGee: The other thing that we are seeing more and more, and I would say, especially since the pandemic started and remote, remote work from home became a real viable option or a necessary option for a lot of people, is entire company impersonation where someone will pretend to be your entire recruiting agency; they'll set up a fake LinkedIn profile, they may use a phishing exploit, a phishing expedition, to try to get in and learn more about who your head of recruiting or HR is, for example, so that they can act as if they were your company. And then they start recruiting people to work for your company remotely, encourage them to buy their own personal laptops and phones and then–quote, unquote–send them to us for specialization and then we'll send them back to you. And we're hearing more and more, and we're contacting law enforcement on behalf of our clients because they're getting complaints from strangers about how they fell prey to these scams thinking they were interacting with a legitimate organization. So while it may not hurt your bottom line in terms of cyber concerns, it's hurting your reputation for sure, and it's something that is still going to be left to you to clean up. So you may not think about it when you click on that email, but it's not just ransomware, it's not just exposing your own sensitive information, it's also potential wire fraud and wholescale company impersonation at this point.

Ken Fishkin: Yeah, absolutely. I mean, that is a huge thing with hackers making up legitimate websites that look really professional, and they even have privacy policies and, you know, contact-us information–it is very, very scary right now.

Kathleen McGee: It’s part of a whole underground enterprise, but I'm really appreciating that you could share with us a little bit today some of the basic things to look for to try to avoid and the importance of ongoing training on that.

Ken Fishkin: Yeah. Thank you, it's been a pleasure.

Kathleen McGee: Thank you.