New attack vectors fortifying the phishing culture

As phishing attacks change to defeat new defenses, CISOs try to keep up. In the end, attackers are evolving faster than defense strategies are developed. Evan Schuman reports.

Cyberthieves are, for the most part, cleaning up their phishing attacks. The telltale typos and misspellings are disappearing from all but the most blatant efforts to bring back the glory days of the *Nigerian Prince*. Requests to wire funds somewhere are so 2020, having been replaced by efforts to steal less trackable gift cards. Mass phishing attacks are still out there, but what enterprise CISOs need to worry about are sharp increases in well-researched spear phishing attacks.

Another evolving attack vector is the distribution form. Although email attacks continue, security teams need to keep a lookout for social media messaging tweaks (Twitter direct message, LinkedIn messaging, Facebook communications and attacks from similar apps), as well as attacks riding along apparent video meeting requests or, even more likely, communications within those video services. Anything that does not match the phishing profile of the typical corporate anti-phishing training program is desirable — at least from the perspective of bad actors.

OUR EXPERTS: *Phishing*

Doug Barbin, principal and cybersecurity leader, Schellman and Company

Joseph Blankenship, vice president and research director, Security & Risk, Forrester Research

Frank Dickson, vice president, IDC

Curtis Franklin, Jr., senior analyst, Omdia

Patty Luxton, senior vice president of engineering services, Kelser Corporation

Keith Mularski, executive director, EY

Joe Nocera, lead of Cyber & Privacy Innovation Institute, PwC

David Weinstein, expert associate partner, McKinsey & Company

"The attacks today look a lot more sophisticated [than the error-filled phishing messages of the past]. First of all, [attackers] learned how to run spell-check," says Doug Barbin, principal and cybersecurity leader at Tampa-based consulting firm Schellman and Company. He notes that phishing attackers keep on top of the latest anti-phishing training and were especially attentive when training courses started preaching "never authorize a transfer via email." Phishers moved to a new way to cash in: gift cards.

Barbin spoke of a large law firm that, in December 2020, found itself the target of a powerful spear phishing attack. An assistant to several of the firm's partners knew — as did the attackers — that the firm routinely issued generous gift cards to attorneys who had done especially well that year. The attacker then sent the assistant an email that appeared to be from a partners for whom she worked.

The email asked her to purchase a large number of physical gift cards — ostensibly for some of their lawyers — from a nearby merchant and then report back to the partner. The assistant did so. That was when the spear-phishers sprung their trap. The response message said that the partner needed to log the numbers of the gift cards, so the partner impersonator asked the assistant to lay the cards out on her desk and to send him a photo of them, with the numbers showing.

The assistant complied. A moment later, her suspicions kicked in. The assistant called the partner who had no idea what she was talking about.

And even though the assistant quickly

44%

Average share of data breach costs incurred in the first year in highly regulated industries

– Ponemon

contacted the merchant to try and put a block on those cards, it was almost certainly too late. The spear-phishers were likely prepared, either using the cards online or perhaps using the card numbers as the late detail to print bogus gift cards then quickly have a gang out on the street use them within minutes. The attackers knew that between hold times and other matters, they would likely have about 20-30 minutes to cash in the cards before the blocks kicked in. For an organized team, that is plenty of time.

Doug Barbin, principal and cybersecurity leader, Schellman and Company

When the assistant was confronted by the partner, Barbin says, she "said she was busy and didn't think anything of it. She was doing a hundred things for a whole bunch of different partners. [Phishers] count on people multitasking and being busy."

Many phishers have also backed off their classic "ask for credentials" tactic, realizing that capturing local session tokens from a browser is much easier and allows the attacker to use the victim's credentials to log in. This could be dubbed the "Would you like to log in using your Google, Facebook or Amazon account details" method.

> "The attacks today look a lot more sophisticated [than the error-filled phishing messages of the past]. First of all, [attackers] learned how to run spellcheck."
>
> *– Doug Barbin, principal and cybersecurity leader, Schellman and Company*

Even the ultimate anti-phishing advice — never click on an unexpected link or open an unexpected attachment — might not be that useful in 2021. Some malware is now embedded into pictures so merely opening an email will unleash it, assuming the victim's settings permit automatic opening of images.

"The notifications they're referring to are a little different and are like the ones where the website asks permission to track location," he says. "What it does is highlight to the team that web applications are much more complicated than just what is in the URL or shows up on the page in terms of text and pictures. The more complicated an application is with respect to scripts, notifications, etc., the more technical avenues an attacker has to use," Barbin says.

The news gets even worse. Phishers are capturing data about email thresholds and sending him a number of attack attempts that falls just below that enterprise's threshold.

Don't forget MFA and thresholds

Patty Luxton, senior vice president of engineering services at Glastonbury, Conn.-based consulting firm Kelser Corp., has discussed that tactic a lot recently with her clients. "[Attackers] opt to send phishing emails in smaller batches, both because of the trend toward increased personalization, but also because they are reverse engineering what the volume threshold [for corporate antispam software] is and creating batches of emails just below it," Luxton says.

"Think about it," she continues. "A phisher can buy an [anti-phishing application], install it, and start testing. What gets in? 999 emails? 499? 99? 49? It would be pretty easy to determine the limit if you can run experiments and there's no reason phishers can't."

Another issue that Luxton says is problematic are enterprises putting too much faith in major vendor partners.

"I often talk to IT executives who are using the built-in spam filter on [cloud-based office

70%

Respondents who said remote work due to COVID-19 would increase costs of a data breach

– Ponemon

suites].” Cloud-based suites are great for email, she says, but the vendor “isn’t making its money on having the top-notch cybersecurity that today’s enterprises need. It just doesn’t have an incentive to create a truly stellar spam filter. Most of its users wouldn’t know what to do with it if they did,” Luxton says.

“If large companies are not getting the results they need from existing products, we could potentially see them create their own custom, proprietary spam filters in-house. If phishers can’t buy [an anti-phishing application], it’s going to be hard for them to learn anything about how it works,” she continues.

David Weinstein, expert associate partner, McKinsey & Company

Luxton also complains that some very large enterprises are still not routinely deploying sufficiently robust multifactor authentication (MFA) tools, assuming they are using MFA at all.

“The value of MFA can’t be understated. Whatever you do, don’t stop using it,” she warns. “But it’s not the foolproof line of defense against phishing that it once was. Today’s hackers are patient. They may phish an email account just to bypass MFA later on a system that houses more valuable data. I continue to be shocked by mainstream players that do not offer MFA or at least don’t make it easy to enable.”

Picture this

Another phishing issue that is going to get more problematic in 2021 is the huge array of different levels of phishing attacks, making it difficult to efficiently defend against all of them.

“There are the most novice script kiddie hacks out there and the most sophisticated,” says David Weinstein, an expert associate partner with McKinsey & Company, where he specializes in cybersecurity. He argues that the best defense is to downplay technological defenses — “The phishing tactics are evolving faster than the techniques that can mitigate them” — and spend more time dealing with “the human culture,” he notes.

Many point to the sharp weakening of the ever-present, anti-phishing poster campaigns in corporate buildings since March 2020 when employees were sent home to telecommute due to the COVID-19 pandemic. Those posters, often ridiculed initially by CISOs and CSOs, proved quite effective as they subliminally reinforced anti-phishing training, he maintains.

Employees might have believed that they simply ignored the posters, but when the workforce went remote, successful phishing attempts soared, according to various published reports. These include the Dept. of the Treasury’s Financial Crime Enforcement Network reminding financial services organizations about attacks related to COVID vaccine scams and phishing fears that are causing workers to reject legitimate emails.

> “The value of MFA can’t be understated. Whatever you do, don’t stop using it.”
>
> *– Patty Luxton, senior vice president of engineering services, Kelser Corporation*

Weinstein argues that “there are virtual analogs to posters” such as sending emails with signatures that reinforce the latest anti-phishing strategies.

Curtis Franklin, Jr., a senior analyst at the London-based market analysis firm Omdia, agrees and proposes that enterprises get aggressive and creative about taking those anti-phishing reinforcement messages to where the employee lives.

$26B

Worldwide losses to business email compromises in a single month in 2019 from 166,459 incidents

– FBI IC3 2019 Internet Crime Report

"Own the real estate in front of their eyes. You can force someone to go to that screen, depending on the MDM (mobile device management software) that you're using. It's the same way that you can force sign-ins to enterprise email," Franklin says, adding that some efforts can try and match the corniness of those HQ posters. "Send them a nice coffee mug that has anti-phishing messages. Send them tea bags [or] bags of popcorn."

Curtis Franklin, Jr., senior analyst, Omdia

The video call phishing attack

One of the biggest areas of worry are the video conference calls that seem take up so much of everyone's time these days. Franklin paints a worrisome phishing scenario predicated on the fact that many calls today feature people that the invitee does not know well, if at all. Those calls often begin with an invite from a trusted colleague, supervisor or client who ultimately does not show up for the call.

Here is how this type of attack works: The victim receives an email or direct message from that trusted individual and asks them to attend a video call at 2 PM. The trusted individual — the ubiquitous "Joe in accounting" for example — is vague on what the meeting is about that, sadly enough, is also common these days. The victim then receives the anticipated video invite, including credentials. The victim clicks on the impossibly long URL and sees two unfamiliar faces.

"Unfamiliar Face tells the victim that he has just been messaging with Joe, who will not be able to join immediately. Unfamiliar Face then says that the enterprise is experimenting with a new product document workflow process and they need "to establish some file-sharing and create an initial password." If the phishers feel especially bold, Franklin says, "they could ask for your network ID or even ask for additional email addresses of team members."

Joe would like the victim to be a test subject. Unfamiliar Face would then either text or email the victim, ideally from within the video conference app. Why from the video app? "When the call is broken, the forensic evidence goes away," Franklin points out.

The message includes an expected attachment, the victim opens it and the malware is launched. The phishers can then either disconnect — their mission is complete — or they can discuss it for a moment and then quickly end the call until the victim has a chance to play with the program. Victim is then to report back to Joe, who will presumably be quite baffled.

A common and effective defense against the less-sophisticated attacks is for the user to double-click — or, sometimes, just mouse-over — the sender's address to see if it claims to really be from the company touted. But as more messages are moving from desktop devices to mobile phones and ultimately wearables, critical context is being lost. That will make the job of a phisher far easier.

> "Send them a nice coffee mug that has anti-phishing messages. Send them tea bags [or] bags of popcorn."
>
> *– Curtis Franklin, Jr., senior analyst, Omdia*

Isolation

Two popular techniques are to use network segmentation and browser isolation "to limit how much damage [the phishers] can do

56%

Percentage of BEC attacks that used gift cards as a cash-out method

– APWG Phishing Activity Trends Report Q3, 2019 on your network. You’re putting in another tripwire to detect [bad] activity,” says Joe Nocera, the leader of PwC’s Cyber & Privacy Innovation Institute in Chicago.

Joseph Blankenship, vice president and research director, Security & Risk, Forrester

What is the catch? “From a budget perspective, this is a large and complex project,” Nocera says, adding that, even worse, there are often intra-corporate battles in the way. “The CISO doesn’t own network infrastructure. There are then some fiefdoms and politics involved.”

Joseph Blankenship, vice president and research director for security and risk at Forrester Research, encourages CISOs to train their people to switch communication methods immediately if a message looks even a little suspicious. Reach out to the alleged sender and try and verify before doing anything. “If it’s a phone call, send an email. If it’s an email, call. Go out of band to figure out if it’s legitimate or not,” Blankenship says.

Frank Dickson, a security and trust program vice president at research firm IDC, argues that today’s horrible phishing situation took years of slow attacks. “We’ve gotten to this position incrementally over the passage of time,” he says.

Dickson encourages CISOs to focus on human resource departments, which receive massive numbers of job applicants, almost all asking that someone open the attached resume. He recommends strict browser isolation, so that “every link clicked goes into some kind of virtualized environment,” akin to a developer’s sandbox.

When an employee falls victim to a phishing attack, they are embarrassed and understandably hesitant to report the breach to superiors. But concluding that the incident will be traced back to them eventually, employees who goof often will report it. One wildcard here is if a company vilifies an employee who makes an error. That, experts say, can change the equation from being able to remediate a problem quickly or not learning about a possible introduction of malware until it causes serious problems.

The much bigger challenge is getting employees who did not fall for the phishing attack to take the time to report it to IT or security. Getting those employees who did everything right and did not click or open the attempted phish to report it is the only way to alert all employees to be on the lookout for this specific phishing attempt. The challenge, of course, is to get employees to take that final step after overcoming the hurdle not to click a potentially dangerous link.

Keith Mularski, executive director in the cybersecurity practice at EY (formerly Ernst & Young) and a 22-year veteran as an FBI special agent, wants CISOs and CIOs to make it as easy and effortless as possible to report a failed phishing attack. “Everybody is busy. Put a button right in the email browser so people can just click a button to report it,” Mularski says.

> “If it’s a phone call, send an email. If it’s an email, call. Go out of band to figure out if it’s legitimate or not.”
>
> *– Joseph Blankenship, vice president and research director, Security & Risk, Forrester*

Making matters worse today in the world of fighting phishing attacks are the increased usage of cloud — both shadow and authorized — along with employees using their personal computers to do whatever they like.

CISOs “no longer control the environment”

89%

Percentage of respondents who use SIEMs and endpoint detection and response systems (EDRs) for threat hunting

– SANS 2020 Threat Hunting Survey

in the way that they used, says Forrester's Blankenship. The first needs to be that users cannot use their work machine for anything else. Others have suggested creating a separate LAN for all work activities, to prevent consumer-grade IoT from ever accessing your VPN and then the enterprise network.

Blankenship proposed a strict "culture of awareness" among users, adding that in the January attack on the U.S. Capital building, "people left their computers unlocked."

"It all comes down to the human filter," he says. "Is an email good and legitimate or is it bad? We are wired to think it's good. We have to train [employees] to be skeptical and to then implement controls to protect users from themselves. Make sure that any emails that come in are stripped of any HTML. Defang all of the links on that email." ■

44%

Percentage of respondents who use data stacking, the process of using telemetry from endpoints and the network to enable a search for outliers in the data

– SANS 2020 Threat Hunting Survey