SC MEDIA

Phishing reference guide

ALTERNATIVE MEDICINE TO PHIGHT PHISHING

Despite following their training, users are still baffled and defeated by phishing hustlers. CISOs and CIOs unleash their red teams to help users recognize the pernicious attacks.

By Evan Schuman

DECONSTRUCTING PHISHING

A phishing thief's playbook is essentially the same as that of a street con artist running a three-card monte hustle: pure deception. When asked what he would say to CISOs who ask how to successfully defend against all phishing attacks, the CIO of a Wall Street investment house focuses on the healthcare space, pauses for a moment, then responds knowingly.

"My first reaction [for the CISO] is to quote Drago in *Rocky IV*: 'You *will* lose,'" says Paul Cottey, CIO of Water Street Healthcare Partners. "Users will always find ways to do silly things. That seems defeatist, though."

It might sound defeatist but it is not necessarily wrong. There are approaches that slightly reduce the number and effectiveness of phishing attacks that get through to your employees, but to block them entirely? Drago might well have had a point.

Still, there are non-traditional tactics that CISOs can use that sharply decrease the success rate, especially as attacks move to off-premises venues, including the cloud and mobile. And red team attackers — sometimes

referred to as a penetration tester, ethical hackers or white hat hackers — are also perfecting new tactics to trick employees so the employees and their bosses learn their lesson before the real bad guys come calling.

A clever approach some security training firms use is a social engineering scheme where a con artist/ethical hacker calls on the phone and says that an email with an attachment is about to come and then waits on the phone until it arrives. Suddenly, the attachment is no longer unexpected. This approach could require some companies to redefine what they mean when they tell employees not to install "unexpected attachments." Just because an attachment is *expected* does not mean it is *safe*.

Phishing, like so many other IT issues, is running into a familiar enterprise challenge: Line of business (LOB) managers, as well non-technical C-level executives, see email as so mission-critical that they resist any recommendations for more aggressive email phishing protections that will impact productivity. This is why many experts see far too few uses of technologies such as Domain-based Message Authentication, Reporting & Conformance (DMARC), DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF) and Brand Indicators for Message Identification (BIMI) (see sidebar).

"Mobile apps themselves that are insecure can, in fact, exposure users to phishing. Upwards of a third of the apps in iTunes and Google Play have certificate validation or man-in-the-middle exposures. There is no curated Good Housekeeping Seal of Approval or Underwriter's Laboratory that says which apps are safe or not."

Brian Reed, chief mobility officer, NowSecure

BYOD vs corporate devices

Brian Reed, chief mobility officer at Chicago-based NowSecure, a mobile penetration testing firm, argues CISOs might be underestimating how different phishing attacks really are in a mobile world. He says a large number of apps in the Google Play and Apple's iTunes app stores fail certificate pinning, do not validate hostnames, and engage in other "network-based failures that open vulnerabilities that can be exploited by [attackers] redirecting to phishing sites or links."

Why is the world of mobile devices so often treated in security circles as an afterthought? "Mobile, in general, tends to be the forgotten stepchild," Reed says. "Mobile is a different animal."

Although email content filtering is common, the desktop and mobile environments are quite different. "You need alternative strategies," Reed says.

Unlike desktop phishing efforts, which focus on deceptive attachments and URLs, mobile phishing adds malware-laden — or simply password-stealing — bogus apps placed in Android and Apple app stores.

"Mobile apps themselves that are insecure can, in fact, expose users to

POPULAR PHISHING ATTACKS

- **BEC Phishing –** sophisticated and highly targeted Business Email Compromise (BEC, sometimes called CEO Fraud) phishing are attacks without initial attachments or malicious content, just an interaction between the attacker and target until there is a download, link click, or other action request by the attacker
- **eCommerce and Entertainment Phishing –** shift from fraudulent bank requests to authentic-looking email from a popular company that discusses billing difficulty, new order, order canceled, and asks target to click a link
- **Smishing –** Phishing attacks conducted via SMS (also through communication apps Slack, Teams, or Facebook Messenger)
- **"March Madness" Phishing –** preys on March Madness bracket makers (can also target online fantasy leagues such as MLB fantasy leagues, Master's golf, Olympics, royal births and similar high-profile events.)
- **Social Manipulation Scams –** not exactly phishing but there has been a significant uptick in scammers physically calling individuals and getting money sent to them (e.g., famous person impersonators such as the "Patrick Dempsey Scam"), IRS tax fines, or police/law enforcement impersonation to pay fines, etc.). Can occur at home or work.

SOURCE: THE CHERTOFF GROUP

phishing. Upwards of a third of the apps in iTunes and Google Play have certificate validation or man-in-the-middle exposures," Reed says. "There is no curated Good Housekeeping Seal of Approval or Underwriter's Laboratory that says which apps are safe or not."

Like other mobile security issues, defensive strategies overwhelmingly rely on whether the enterprise uses a bring-your-own-device (BYOD) or company-owned device strategy.

Both approaches have their pluses and minuses. Beyond the anticipated lower costs often associated with an employee-owned device, BYOD means that the company cannot impose any meaningful restrictions on what is downloaded, which attachments are opened or, most critically, which apps are downloaded.

Much depends on the company's acceptable use policy and how that policy deals with personal devices. With BYOD deployments, some companies will insist on strict partitions to separate corporate content and apps from personal content and apps. Enterprises certainly can insist on specific corporate apps to be downloaded, such as a company-selected virtual private network (VPN) or anti-virus, and it can prohibit downloading any unauthorized app into the corporate side of the partition.

However, it is very difficult for even an enterprise using partitions and BYOD to prohibit what the employee can download onto the personal side of the partition.

A trickier matter is remote wipe. Some enterprises that need to have their employees access highly-sensitive data — for example, top secret military information — can sometimes insist the cost for allowing such data on the mobile device is that the employee agrees to immediately report to IT if the phone is lost or stolen and, critically, agrees that it can remotely wipe the entire device, including any personal data and apps. If nothing else, it tends to encourage employees to backup mobile data.

The acceptable use policy outlines what can and cannot be done on the corporate partition and ultimately what might or might not happen in case the device is lost or stolen. This could include actions ranging from a wipe of the device to the extreme case of bricking the device remotely, making it completely unusable.

MOBILE PHISHING ISSUES

- **Risk: Downloaded malicious apps, rather than just links and attachments**
- **Both Google's Android and Apple's iOS do terrible job at screening apps**
- **iOS slightly more secure**

Even requiring security tools such as a corporate VPN be installed on a personal device, partitions to separate corporate and personal data and even mobile application containerization (MAC) typically will not help much.

"The VPN doesn't really help when dealing with an app that is exploitable," Reed says.

Reed argues that all of the major mobile platforms, especially Google and Apple, do little in terms of investigating apps for security holes, given that both Google and Apple are more focused on making sure that developers comply with their terms and conditions. "Apple doesn't security certify," he says.

But to the nature of their mobile environments and not any security measures taken by either mobile operating system company, Apple, which has to deal with just one handset manufacturer worldwide, is far more secure than Google, which must work with well more than a thousand handset makers globally, Reed says. This means that Apple iOS can afford to have a much more proprietary and closed system than does Google's Android, he says.

"iTunes has much less malware on it. Apple is more limited and Google has a much more open system," Reed says. "Apple has the closed model that [it] was designed for. It makes it easier to write a safe app. On the Android side, it's the Wild West."

The security conundrum

Reed strongly encourages enterprises to pen test apps and then place those that pass the pen tests on a strict approved list. "CISOs can't trust that Apple and Google are certifying apps" in the same way that aggressive pen testing would. In short, IT and security teams must test apps themselves before letting employees download them. Of course, it is a lot easier to insist that employees only download company-approved apps when the company has not gone BYOD.

Chris Duvall, senior director of the Washington, D.C.-based security

consulting firm The Chertoff Group, says the big problem he sees today with enterprise phishing efforts is another familiar security conundrum. Traditional phishing defenses rely on rank-and-file employees to not click on attachments, links, or to use unfamiliar apps. But given the clever tricks phishers use, employees, who often are not well trained in security protocol, are relatively ineffective at blocking all attacks.

While training reduces the success percentage that the attackers will experience, cutting phishing effectiveness from, say, 34 percent to 20 percent, this still leaves one-out-of-five attacks being able to access credentials, sensitive data, or both.

To security groups, that means deploying stricter limitations on what the system permits employees to do — some enterprises have considered blocking all active links — and that raises entirely expected objections both from LOB managers as well as non-technical, C-level executives.

Duvall compares the resistance to aggressive phishing defenses to the kind of pushback IT staffs and CISOs experience when mandating the use of multi-factor authentication (MFA).

In short, LOB and some corporate executives dislike and fear anything that adds friction for employees, customers, or prospects. For MFA, it is friction in logging in. For aggressive phishing defenses, the LOB manager is worried that it will block an attachment or link that is critical to finalizing a large contract or that it might throw roadblocks in front of any employees, especially those who work in sales.

"This is a fundamental security challenge: 'We don't want to lose current or potential customers based on some new security,'" Duvall says. This makes it critical for CISOs to do a better job at persuading LOB and corporate executives that aggressive phishing defenses are ultimately in the company's best interest. "One slight deal delay is annoying, but in the long run, it's worth it."

Duvall also points out that once a phishing attacker accesses credentials — typically by tricking the targeted employee who has the desired credentials to log-in to a look-alike corporate page — the attack looks identical to an insider attack. In effect, it is similar to an insider attack in that it uses the credentials to get through various layers of defense. It then falls on behavioral analytics tools to recognize that the credentials might belong to an employee who has a specific profile, for example the head of payroll, but the user is not acting in accordance to that profile.

From a tactical perspective, that is somewhat irrelevant. Whether it is a rogue executive trying to re-route salaries to a numbered bank account in Switzerland or a phisher who stole the payroll chief's credentials, the response is the same: shut the effort down and disable the credentials until humans can determine definitively what is happening.

With email, for example, Duvall recommends aggressive use of DMARC, DKIM, SPF and BIMI.

"We advise our clients to strongly consider implementing DMARC, and the associated DMIK and SPF protocols. When implemented properly and within their supply chains, these tools can significantly reduce both sent and received spoofed emails, which is the single, biggest tactic used in successful phishing attacks.

"There are three key benefits to an organization implementing DMARC. It is a method of distinguishing between authorized/good and unauthorized/bad domains and it can drastically reduce spam and phishing email and, ultimately, it can help organizations protect their brands," Duvall says.

"On a fundamental, security-oriented level," he continues, "this means that CISOs can worry a bit less about volume-based click rates. The industry average success rate for phishing is about 20 percent, so the greater the number of phishing emails sent and making it to end users, the greater potential for a breach."

> **"Even if you're fooled by phishing, autofill won't be. It gives an opportunity for the user to rethink."**
>
> **Michael Coates, CEO, Altitude Networks; former CISO, Twitter**

Duvall also sees DMARC helping CISOs overcome reluctance from lines of business leads. This means that if your marketing team's emails are proven as coming from your company versus being spoofed, more of them reach their potential customer destination as opposed to being blocked due to the domain and IP addresses appearing to be malicious and blacklisted.

Duvall finds BIMI helpful as it "allows an organization to display its

logo alongside outgoing, authenticated messages. The logo appears where a photo or initials appear next to the *From:* line of an email," he says.

"Although this can already be done by some mail providers," Duvall continues, "those advocating BIMI hope that it will eventually come to mean that the email is truly from the sending organization and signals conformity to the DMARC, DKIM, SPF protocols, meaning it has not been spoofed. Participating organizations appear to like BIMI as it is a low-cost marketing add-on and it signals that the sending organization has taken action to reduce fraudulent email and better security recipients."

Michael Coates, who served as the CISO at Twitter from January 2015 until the spring of 2018 and is now co-founder and CEO of the security startup Altitude Networks, says the social media giant discovered various, non-traditional ways to fight phishing. For example, Twitter found that many ordinary password manager applications had the unintended effect of halting quite a few phishing attacks. How? The autoconfig function.

Specifically, when a user visits a legitimate site and then password manager application memorizes that site, its login procedure format, and its username and password/PIN. It memorizes the process precisely. That is why such programs are sometimes flummoxed when a site redesigns or makes some material change in its login process. That also is why such programs will not be fooled by a look-alike site. Hence, they do not work on a decoy site created by a phisher, giving the end-user a big heads-up that the site might not be legitimate. At the very least, it gives the user a reason to pause and hopefully to examine the site and its URLs more carefully.

"Even if you're fooled by phishing, autofill won't be," Coates says. "It gives an opportunity for the user to rethink." To the extent that it does that, the password manager becomes a friend to the CISO and an enemy to the phisher.

Coates also supported internal security penetration testers' internal phishing schemes where his team tried to trick fellow Twitter users into revealing credentials. He referenced one such effort where his people called employees to discuss password security, claiming to be from IT. The red team hacker repeatedly stressed to users that they should not say the password, but that the IT worker merely wanted to establish whether it was sufficiently secure.

The ethical hacker would then direct the user to visit an "internal" IT site, but he did not give them a traditional word-based URL. Instead, he gave a specific IP address, given that it is much more difficult for a user to recognize that numerical address as fraudulent.

Once there, it asked them to type in their password — which appeared as the typical string of asterisks — and then gave them the number it assigned. Ostensibly, the number was an indicator of how strong a password they typed. In truth, the number was just distraction. Once the credential was typed in, the phishing attempt succeeded.

Another favorite social engineering technique from Coates was calling employees at about 11:30 a.m. — "right before lunch," he says — and asking them to engage in a two-hour security mechanism. After a lot of bogus patter, the pseudo-attacker would say something like, "I am not supposed to do this, but we have a program for the executives to run without their involvement. I can put your information

PHISHING DEFENSES EXPLAINED

- **DMARC builds on the widely deployed SPF and DKIM protocols, adding linkage to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email**
- **DKIM is an email authentication technique that allows the receiver to check that an email was indeed send and authorized by the owner of that domain**
- **SPF is an email-authentication technique used to prevent spammers from sending messages on behalf of your domain**
- **BIMI is an effort to use brand logos as indicators to help users avoid fraudulent emails**

into the script and it can run over night." Again, credentials obtained.

Another phishing security specialist, Randy Armknecht, the managing director at the Protiviti consulting firm in Menlo Park, Calif., is also a strong proponent of creative red team efforts to find the weak employee link in an enterprise's phishing defenses.

Armknecht found that the red team's email success rate was about 20 percent (mostly involving bogus links instead of attachments) whereas phone social engineering efforts did much more poorly, typically succeeding only about 5-10 percent of the time. But when the two tactics were combined — meaning that an employee was called and, while they were on the phone, the caller promised to send an email to them and indeed did — the success rate soared to about 40 percent.

To get that high a rate, though, his people did what real phishing con artists do. They did their homework. The typical approach would be to call and say that they were calling from IT. By procedure, they had to call from outside the building (no fair using actual internal extensions) and they would typically say that they are calling from a mobile one. That meant that the call displayed a local area code, but that was as far as the phone-number-fakery needed to get.

They would use an actual name of someone who worked in IT, so that the employee victim could run a quick LinkedIn search and the name would seem legitimate. If the target actually knew the voice of the person being impersonated, the attack usually failed. The larger the enterprise, the better the chances at that not being an issue.

This type of attack potentially works because it exploits employee training that they should never open an attachment that they are not expecting. In this case, the employee is indeed expecting to receive the email because the "attacker" just said that he was sending it.

Armknecht also agrees that corporate politics — LOB managers fearful of email delays or blocks — is a massive impediment to aggressive phishing defense deployment.

"Emails [are] the lifeblood of any organization so email [restrictions] will be viewed with caution. CISOs aren't able to make unilateral decisions when it comes to email," Armknecht says. "It's often the business units that will be leery of IT and security making changes that they fear will put emails at risk. They are worrying about the big deal they might lose because a client email won't get through."

3 EFFECTIVE PHISHING RED TEAM TACTICS; 1 DEFENSIVE TACTIC

- **Call and email simultaneously**
- **IP Addresses are more effective at tricking employees than URLs**
- **Call right before lunch. Employees will be eagar to get you off the line**
- **However, the hidden, anti-phishing talents of password-management apps can defeat look-alike sites**

Extreme prejudice

Another security consulting firm expert is Tyler Hudak, the incident response practice lead at TrustedSec in Akron, Ohio, and a former security specialist at the Mayo Clinic and General Electric. He finds value in the rather extreme route of full email link removal.

"I have seen some, but not many, organizations utilize systems that completely remove all HTTP links from emails," Hudak says. "Although this can definitely affect some valid emails or workflow, it is effective at preventing phishing emails with links to external sites from working."

Another extreme move is for an enterprise to intercept all web traffic, Hudak says.

"It is definitely not common, but some organizations are using services that intercept all web traffic, similar to the way a proxy server does, but the web page shown to the user is actually an image of the page and not the real web page. Typically, this is only done for certain categories of websites or ones that are not whitelisted," he adds.

"What this allows is a user to still click on links in emails, but if the link goes to a phishing site, the user cannot interact with it," he continues. "The service still allows some form of interaction, but the protections are in place to prevent a user from submitting credentials to a phishing site. This also works great for stopping phishing that comes into the user's personal webmail account."

A similar extreme tactic is isolating attachments in a sandbox before the user can interact with it.

"All attachments in email are sent to an internal sandbox and opened. The sandbox, which is just a virtual

machine that gets reset after every use, is watched for anything malicious after the attachment is opened," Hudak says. "If something suspicious occurs, such as the system attempting to reach out to the internet, the attachment is deemed suspicious enough and the email is blocked."

Water Street Healthcare Partners CIO Cottey says the most effective way to fight phishing is to get rank-and-file employees to be more vigilant and, candidly, more cynical and suspicious. This is not merely about getting employees to care more about phishing risks. It is more fundamental: It is getting those employees to truly believe that they really are potential victims.

"What I don't think that the typical Fortune 1000 CISO gets is that their end-users really don't think that they are important enough to be phished. The CISO has to break through that mentality," Cottey says.

Cottey tested his own employees by doing his own red team phishing effort.

"On Jan. 31, I sent out a fake W-2 form to all employees, knowing employees "were in active discussions with HR about updating their W-2. They clicked on it because they were expecting it."

It worked so well, Cottey says, because of the date he sent his trap and his knowledge of when HR was pushing that issue. "But the bad guys are also situationally aware and they're aware at the macro level," Cottey says.

Cottey also says that he is worried about mobile phishing efforts. "There is some level of complacency within the Apple environment. If I were relying on mobile apps, I would absolutely sandbox what I provided and limit what people are allowed to do. I have to turn the screws tightly enough. I don't think we've given mobile the attention it needs," he says.

> **"We advise our clients to strongly consider implementing DMARC, and the associated DMIK and SPF protocols. When implemented properly and within their supply chains, these tools can significantly reduce both sent and received spoofed emails, which is the single biggest tactic used in successful phishing attacks."**
>
> **Chris Duvall, senior director, The Chertoff Group**

OUR EXPERTS

Randy Armknecht, managing director, Protiviti

Michael Coates, CEO, Altitude Networks; former CISO, Twitter

Paul Cottey, CIO, Water Street Healthcare Partners

Chris Duvall, senior director, The Chertoff Group

Tyler Hudak, incident response practice lead, TrustedSec

Brian Reed, chief mobility officer, NowSecure

But why does Cottey worry more about the Apple iOS space when it comes to phishing concerns when Apple has made a concerted effort to present itself as offering better security than Android offerings?

"There have been enough stories and enough publicity about Android [security problems] that people recognize how much the [Android] marketplace is fragmented. There are an awful lot of apps running around that are just garbage. You're less screwed in iOS because the chance that you're running something that is twelve OS versions out-of-date is much less. [Apple] nags you to the point that you'll update. Still, if you jailbreak [an iOS device], all bets are off."

How much is too much

Every enterprise must decide at the most senior levels — the case must have the backing of the CEO and, ideally, much of the board — the level of phishing damage that is acceptable. For some, getting the penetration down to 10-15 percent might be acceptable. But for most, it will not be, which is when the more extreme anti-phishing need to be very strongly considered.

That is not necessarily a bad thing. It will force a conversation among the top company leaders about a risk strategy. If minimal risk is to be tolerated, then the board must accept far greater restrictions on communications.

Fighting phishing successfully is possible, but at what price? Get the senior management answer to that and most CISOs will learn about a lot more than email strategies. They will learn what senior management values and at what cost. ■