PHISHING ATTACKS: A GUIDE FOR IT PROS

Source Material Tech Republic

CADENCE CYBER

TechRepublic

TABLE OF CONTENTS

CADENCE CYBER

WANT TO IMPROVE CYBERSECURITY? TRY PHISHING YOUR OWN EMPLOYEES

BY ALISON DENISCO RAYOME

More than 90% of cyberattacks and resulting data breaches start with a spear phishing campaign—and many employees remain unable to discern these malicious emails from benign ones. To improve cybersecurity education, some companies are turning to a nontraditional method: Phishing their own employees.

Too often, companies offer only annual training on cybersecurity that doesn't keep up with the evolving threat landscape, according to Wesley Simpson, COO of (ISC)2. "Using internal phishing exercises is a very inexpensive tool that helps fight the risk and is an investment in staff's knowledge and education," Simpson said. "It's not something that should happen once a year—it should be continuous."

ISC(2) runs regular internal phishing exercises on employees. The IT team crafts the emails based on ones that employees actually receive, Simpson said: For example, those that mimic a coffee shop offering a free beverage or a postal service package notification.

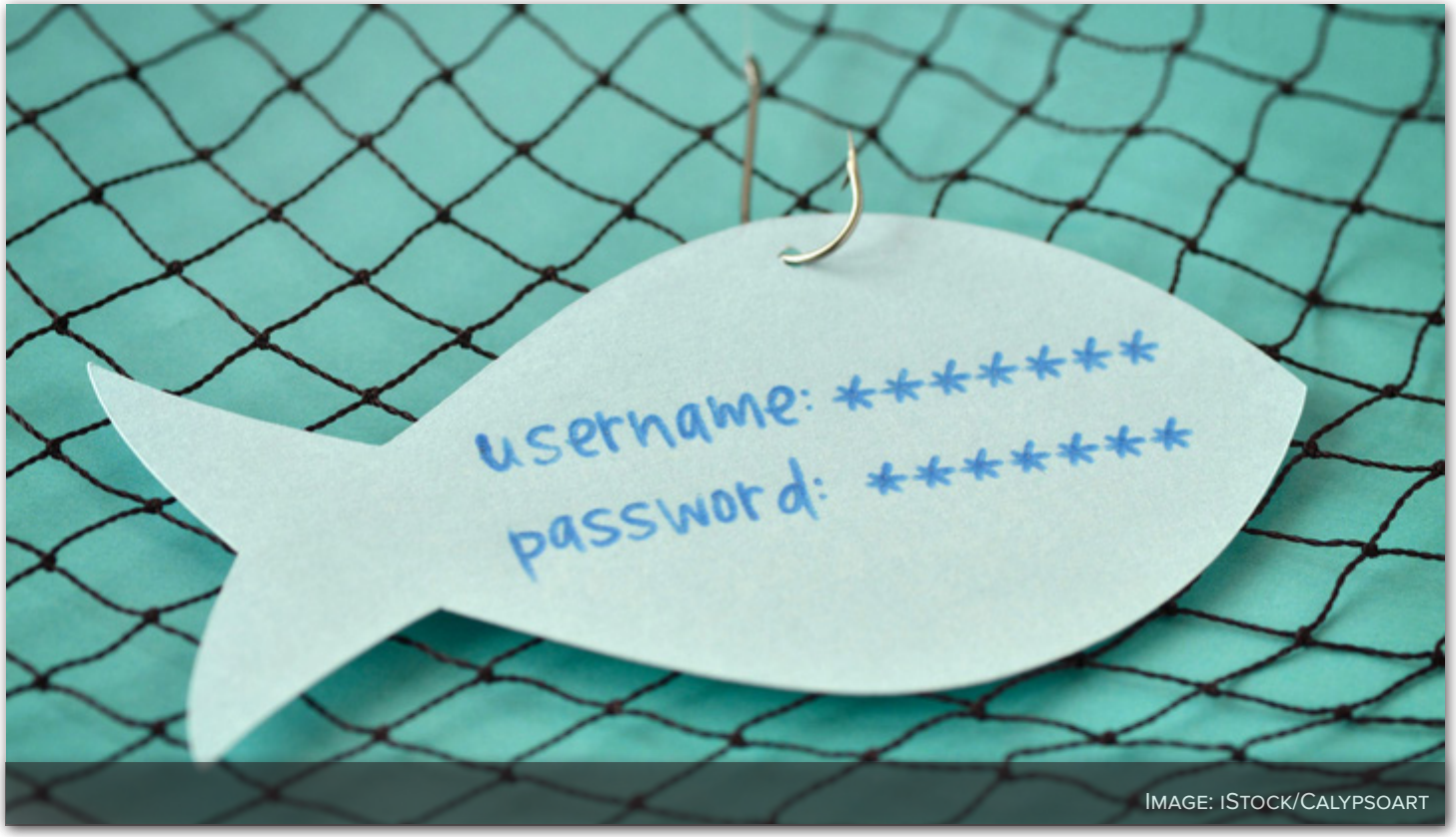

IMAGE: ISTOCK/CALYPSOART

Source: Tech Republic

Before making the campaign public, companies should take a baseline measurement of how employees react to one of the phishing exercises, said Carl Leonard, principal security analyst at Forcepoint. Then, you have a metric to measure improvement against.

"A company's most accurate results will arise from tests conducted when employees have not been forewarned," he said. "Ideally, they will be in a typical frame of mind and not in a heightened state of alertness knowing that a test will be conducted soon. This allows companies to more accurately baseline current status."

From there, you can define what you will measure and what success looks like. ISC(2) examines four main metrics:

- Clicking the link
- Opening the attachments
- Reporting the actual email
- How quickly an employee responds

"You have got to have transparency back to the employees," Simpson said. "Show them the results and hopefully over each month, they can see progress." This helps not only the individuals or teams that are susceptible to risk, but the IT team, which can determine the topics or departments that need more attention.

ISC(2) views results anonymously but can break them down by teams and departments. "You don't want to turn off employees or they won't participate," Simpson said. "Raising it up to a team or department still promotes participation, and people won't feel like they're called out individually. The No. 1 goal is education and awareness, not embarrassment."

The organization also adds an element of competition, with a leaderboard of how each department does to encourage improvement. Companies can consider offering badges for best and most improved performance, Simpson said.

"Tech leaders need to understand that they are not immune to these spear-phishing attacks," he said. "The sooner they assess where they are, the quicker they can start to fill in the gaps."

CONVINCING THE C-SUITE

How do you convince company leaders to take such a nontraditional approach to cybersecurity awareness?

"Management usually reacts to money and results," Simpson said. "These phishing exercises are inexpensive and can be done with existing staff. Once you start running them, the numbers speak for themselves. These are monthly reports that can show how the organization is improving."

It also allows security leaders to determine areas of weakness and target training to those areas, rather than taking a blanketed approach. Further, "you don't need an expensive platform or software package to do this," Simpson said. "Most organizations can do this with their staff today, just mimicking what a phishing attack looks like, using their current software or Exchange platform to track metrics."

A number of third-party platforms are moving into this space as well. Smaller organizations that lack technical expertise can consider tapping one of these vendors to help them run an attack. Some services, such as PhishNet, will send phishing emails to employees. If they click on them, PhishNet will immediately send those users to a brief training page, as well as analyzing problem areas.

To convince leadership that this is a worthy educational exercise, IT needs to ensure that it's communicating the risks and needs in business terms, rather than technical jargon, said Roberto Valdez, manager of risk advisory services at CPA firm Kaufman Rossin. It's also key to communicate that employees are not confined to the organization's network, with the rise of BYOD and work from home policies.

"Your people and the cyber risk extend beyond the boundaries of the network," Valdez said. "The footprint of risk is much broader. Invest in your people, train them, and have them understand their role as a stakeholder in the security process."

CADENCE CYBER

DON'T SKIMP ON IT SECURITY TRAINING: 27% OF EMPLOYEES FALL PREY TO PHISHING ATTACKS

BY ALISON DENISCO RAYOME

Cybercriminals are increasingly turning to social engineering to enter a corporate network, as they know that humans are the weak link in any company's security plan, said a recent report from security firm Positive Technologies.

The firm studied its 10 largest pen testing projects performed for clients in 2016 and 2017. These tests included 3,332 emails sent to employees with links to websites, password entry forms, and attachments, mimicking the work of hackers.

"To make the emails more effective, attackers may combine different methods: A single message may contain a malicious file and a link, which leads to a website containing multiple exploits and a password entry form." — Leigh-Anne Galloway

If these emailed "attacks" had been real, 17% of the messages would have led to the compromise of an employee's workstation, giving the hacker a foothold into the entire corporate infrastructure, the report found.

According to the report, phishing was the most effective form of social engineering attack: 27% of recipients clicked the phishing link, which led to a fake website.

"To make the emails more effective, attackers may combine different methods: A single message may contain a malicious file and a link, which leads to a website containing multiple exploits and a password entry form," said Leigh-Anne Galloway, cybersecurity resilience lead at Positive Technologies, in a press release. "Malicious attachments can be blocked by properly configured antivirus protection; however, there is no surefire way to prevent users from being tricked into divulging their password."

Employees not only open unknown files and click suspicious links, they sometimes correspond with attackers. The report found that In 88% of cases of correspondence, the employees worked outside the IT department. However, 3% of security professionals corresponded as well.

At times, employees complained that the malicious files or links would not open. In some situations, these employees tried to open the files or enter their password on the fake site 30-40 times, the report said. Frustrated employees unable to open files sometimes forwarded them to the IT department for help—further increasing the risk to the organization, as IT staff are more likely to trust their colleagues and attempt to open the file.

Hackers have also learned that sending messages from fake companies is less effective than in the past, causing only 11% of risky actions from employees. However, sending messages from the fake account of a real company and person increases the odds of success to 33%.

These attackers carefully select email subject lines to illicit a response from employees, including "list of employees to be fired" (which caused 38% of risky actions) and "annual bonuses" (which caused 25%).

The report highlights the need for companies to implement continuous employee security training. A number of companies run internal phishing attacks to identify weak links and strengthen their cybersecurity posture.

"To reduce the risk of successful social engineering attacks, it is important to hold regular trainings and test how well each employee follows security principles in practice, "Galloway said. "Whilst people are often the weakest link in your organization, businesses can benefit a lot by fostering a security positive culture."

CADENCE CYBER

COMBAT PHISHING ATTACKS BY STUDYING THE PSYCHOLOGY BEHIND DIGITAL FRAUD

BY MICHAEL KASSNER

The proverb "Fool me once shame on you, fool me twice, shame on me" seems a bit harsh when it comes to phishing, a type of online fraud. Being tricked by a phishing email or online scam a second or even third time is not out of the question.

As to why, indications are that those involved in phishing are figuring out what offers the best chance of success, and thanks to the internet, have access to more usable information than Robert Redford and Paul Newman had in *The Sting*.

That said, there is something in play when it comes to all types of fraud: human psychology. Marika Samarati, in the article The psychology behind phishing attacks, suggested phishing is the act of psychologically manipulating people into performing actions or divulging confidential information they normally would not.

"Phishing campaigns are all about human behavior and psychology," Samarati said. "They require only limited technical skills. Their success depends on understanding human nature well enough to anticipate how people will behave and react to the bait."

Samarati offered the following examples of how online fraudsters maximize the success of their phishing emails:

- Emails are sent when people are most vulnerable and stressed—for example, late in the afternoon, on Fridays, or at the end of the month.
- C-level managers' email addresses are spoofed to make sure employees do not question the request.
- Phishing campaigns employ fear tactics and request immediate responses.

A STAGGERING INCREASE IN PHISHING ATTACKS

There is an extensive amount of data on why we humans fall for online con games. There are also all sorts of user-training regimens and tools aimed at curbing phishing attacks, but they don't seem to be working.

According to the APWG, phishing has had a resurgence. There was a 250% increase in phishing attacks from 2015 to 2016, and during 2017 an average of 1.4 million unique phishing websites were created each month.

STUDYING ADVERSARIAL BEHAVIOR MIGHT BE THE ANSWER

Two researchers working in Carnegie Mellon University's Department of Social and Decision Science decided to look beyond the reasons why users fall for online fraud attacks. "Psychological research on human adversarial behavior is necessary to uncover factors that determine how deception and phishing strategies originally manifest in phishing emails," said Prashanth Rajivan and Cleotilde Gonzalez in their coauthored paper Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks. "Currently, there is a severe lack of work on the psychology of criminal behaviors in cybersecurity."

The two decided to change that, looking specifically at:

- The importance of incentives
- How much of a role creativity plays
- The effect of adversarial strategies on attack success

To determine the importance of each item above, Rajivan and Gonzalez developed a two-part experiment consisting of these phases:

- Adversarial phase: 105 participants were given the task of creating phishing emails that would evade detection and persuade end users to respond.
- End-user phase: 304 participants were asked to examine and classify the phishing emails generated in the adversarial phase that were intermixed with benign emails.

The diagram below offers a visual of the two individual phases of the study.

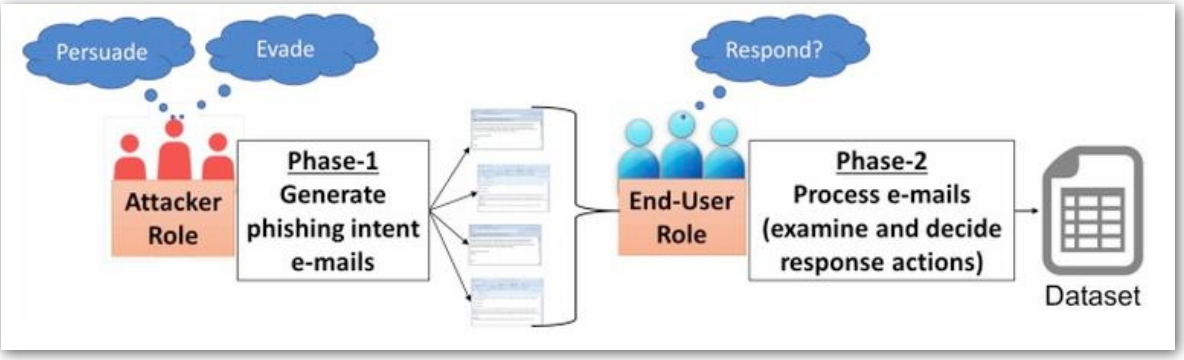

IMAGE: CARNEGIE MELLON UNIVERSITY, PRASHANTH RAJIVAN, CLEOTILDE GONZALEZ

THE RESULTS

After analyzing the data with regard to phishing effort and persuasion performance, Rajivan and Gonzalez came to the following conclusions:

Incentives: The amount of effort (based on the number of edits made per email) given to create a phishing attack was very much related to when the reward was obtained. The researchers found participants who received high rewards early on exerted more effort; Rajivan and Gonzalez concluded that delaying rewards might be one way to lessen phishing's impact.

Creativity: The researchers determined that participants with a high degree of creativity were more likely to spend more effort developing their phishing emails. "However, contrary to expectations from the cybersecurity criminal literature we did not find any evidence for creativity being a key predictor of phishing success," the authors said. "Hence, we could theorize attackers with higher creativity could be capable of changing and adapting their emails to evade detection, but their creativity may not determine their success in persuading end users to respond to their emails."

Strategies: Perseverance in using a certain strategy appears to be a key to success. Rajivan and Gonzalez compiled the strategies most likely to be viewed and responded to immediately by end users:

- Sending notifications
- Using an authoritative tone
- Pretending to be a friend
- Expressing shared interest
- Communicating failure

The researchers also identified the least successful strategies, which were:

- Offering deals
- Selling illegal materials
- Using an "obvious" positive tone

THE RESEARCHERS' CONCLUSION

Interestingly, Rajivan and Gonzalez were able to show that creativity and receiving sufficient payback quickly are key to incentivizing individuals to defraud users online. They are optimistic that these insights and others presented in their paper can be used to improve training programs and current anti-phishing technology.

CADENCE CYBER

HOW FACT-CHECKING COULD THWART PHISHING ATTACKS

BY MICHAEL KASSNER

"Research from the field of cognitive psychology indicates people are naturally poor fact-checkers," said Lisa Fazio, assistant professor of psychology at Vanderbilt University, in this article in The Conversation. "It is very difficult for us to compare things we read or hear to what we already know about a topic."

And it's a safe bet that cybercriminals—in particular, those who spear-phish—understand and use the research described by Fazio to improve their success rate. Besides relying on poor fact-checking, digital fraudsters place a great deal of importance on crafting official-looking, malicious emails and websites.

"In phishing attacks, cybercriminals utilize manipulation and deception to trick users into providing the requested information (i.e., social engineering)," said Ina Wanca and Ashley Cannon in their paper How human behavior and decision making expose users to phishing attacks (PDF).

HOW MANY ANIMALS OF EACH KIND DID MOSES TAKE ON THE ARK?

The above question has been part of surveys used by psychologists since the 1980s, and most participants miss that Noah, not Moses, was on the Ark. The Moses Illusion (also known as knowledge neglect) occurs when relevant information is available but not used in the decision-making process—a human trait that cybercriminals count on, unfortunately.

One reason why the Moses Illusion works so well is that people typically spend more time and effort trying to understand what's being heard or read than determining whether the information is true.

Truth bias is another reason why the illusion works. People tend to believe what they hear or read is true regardless of the source or any prior knowledge they may have about the subject. In other words, people expect information they receive to be correct.

THE ILLUSORY TRUTH EFFECT

Another successful psychological phenomenon cybercriminals employ to deceive their targets is called the illusory truth effect. In the research paper Knowledge Does Not Protect Against Illusory Truth (PDF), Fazio, along with Nadia M. Brashier (Duke University), B. Keith Payne (University of North Carolina at Chapel

Hill), and Elizabeth J. Marsh (Duke University), suggested that it's human nature to attach more validity to information that has been repeated multiple times.

"Research on the illusory truth effect demonstrates that repeated statements are easier to process and subsequently perceived to be more truthful than new statements," the paper said. "Contrary to prior suppositions, illusory truth effects occur even when participants know better."

PRIOR KNOWLEDGE HELPS FIGHT ILLUSORY TRUTH

Prior knowledge does help, but not as much as previously thought. "Expertise did not eliminate the illusion, even when errors were bolded and underlined, meaning that it was unlikely that people simply skipped over errors," said Allison D. Cantor and Elizabeth J. Marsh in their paper Expertise effects in the Moses illusion: detecting contradictions with stored knowledge. "The results support claims that people often use heuristics to judge truth, as opposed to directly retrieving information from memory, likely because such heuristics are adaptive and often lead to the correct answer."

The authors said, "Even experts sometimes use such shortcuts, suggesting that overlearned and accessible knowledge does not guarantee retrieval of that information."

IS THERE A SOLUTION?

Fazio and her colleagues tried several methods to improve fact-checking ability. Most failed, with some making the situation worse. Fazio offered an example:

"We tried highlighting the critical information in a red font. We told readers to pay particular attention to the information presented in red with the hope that paying special attention to the incorrect information would help them notice and avoid the errors. Instead, they paid additional attention to the errors and were thus more likely to repeat them on the later test."

There is good news. It seems that survey participants avoided misinformation (being phished) when asked to edit a story and highlight inaccurate statements or read the stories—sentence by sentence—and decide whether each sentence contained an error.

Still, it is far from a perfect solution. "It's important to note that even 'fact-checking' readers miss many of the errors and retain false information from the stories," Fazio said. "For example, in the sentence-by-sentence detection task participants caught about 30 percent of the errors. But given their prior knowledge they should have been able to detect at least 70 percent."

CADENCE CYBER

HOW TO ACT LIKE A FACT-CHECKER

If acting like a fact-checker helps, it might be useful to look at how professionals fact-check. Alexios Mantzarlis, director of International Fact-Checking Network at Poynter Institute, helped develop a Fact-Checkers' Code of Principles. These are several of the concepts Mantzarlis feels strongly about that might improve our ability to zero in on what is truth and what is misinformation:

- Follow the same methodology for every fact-check and let the evidence dictate conclusions
- Be concerned if sources are not transparent, paying particular attention to funding sources
- Have a willingness to correct perceptions when fact-checking provides a different answer

With both fake news and spear-phishing attacks trending high on the internet, it might behoove each of us to start wearing our fact-checking hat.

CADENCE CYBER

10 TIPS FOR SPOTTING A PHISHING EMAIL

BY BRIEN POSEY

Every day, countless phishing emails are sent to unsuspecting victims all over the world. While some of these messages are so outlandish it's obvious they're frauds, others can be a bit more convincing. So how do you tell the difference between a phishing message and a legitimate message? Unfortunately, there is no one single technique that works in every situation, but there are a number of things you can look for.

1: THE MESSAGE CONTAINS A MISMATCHED URL

One of the first things I recommend checking in a suspicious email message is the integrity of any embedded URLs. Oftentimes the URL in a phishing message will appear to be perfectly valid. However, if you hover your mouse over the URL, you should see the actual hyperlinked address (at least in Outlook). If the hyperlinked address is different from the address that is displayed, the message is probably fraudulent or malicious.

2: URLS CONTAIN A MISLEADING DOMAIN NAME

People who launch phishing scams often depend on their victims not knowing how the DNS naming structure for domains works. The last part of a domain name is the most telling. For example, the domain name **info.brienposey.com** would be a child domain of **brienposey.com** because brienposey.com appears at the end of the full domain name (on the right-hand side). Conversely, **brienposey.com.maliciousdomain.com** would clearly not have originated from brienposey.com because the reference to brienposey.com is on the left side of the domain name.

I have seen this trick used numerous times by phishing artists as a way of trying to convince victims that a message came from a company like Microsoft or Apple. The phishing artist simply creates a child domain bearing the name Microsoft, Apple, or whatever. The resulting domain name looks something like this: **Microsoft.maliciousdomainname.com**.

3: THE MESSAGE CONTAINS POOR SPELLING AND GRAMMAR

Whenever a large company sends out a message on behalf of the company as a whole, the message is usually reviewed for spelling, grammar, and legality, among other things. So if a message is filled with poor grammar or spelling mistakes, it probably didn't come from a major corporation's legal department.

4: THE MESSAGE ASKS FOR PERSONAL INFORMATION

No matter how official an email message might look, it's always a bad sign if it asks for personal information. Your bank doesn't need you to send it your account number. It already knows what that is. Similarly, a reputable company should never send an email asking for your password, credit card number, or the answer to a security question.

5: THE OFFER SEEMS TOO GOOD TO BE TRUE

There is an old saying that if something seems too good to be true, it probably is. That's certainly the case with email messages. If you receive a message from someone unknown to you who is making big promises, the message is probably a scam.

6: YOU DIDN'T INITIATE THE ACTION

Just yesterday, I received an email message informing me I had won the lottery!!!! The only problem is that I never bought a lottery ticket. If you get a message telling you that you have won a contest you did not enter, you can bet that the message is a scam.

7: YOU'RE ASKED TO SEND MONEY TO COVER EXPENSES

One telltale sign of a phishing email is that you will eventually be asked for money. You might not get hit up for cash in the initial message. But sooner or later, phishing artists will likely ask for money to cover expenses, taxes, fees, or something similar. If that happens, you're looking at a scam.

8: THE MESSAGE MAKES UNREALISTIC THREATS

Although most phishing scams try to trick people into giving up cash or sensitive information by promising super deals or instant riches, some phishing artists use intimidation to scare victims into giving up information. If a message makes unrealistic threats, you're probably being phished. Let me give you an example.

About 10 years ago, I received an official-looking letter that was allegedly from US Bank. Everything in the letter seemed completely legit except for one thing. The letter said my account had been compromised and that if I did not submit a form (which asked for my account number) along with two picture IDs, my account would be canceled and my assets seized.

I'm not a lawyer, but I'm pretty sure that it's illegal for a bank to close your account and seize your assets simply because you didn't respond to an email message. Not only that, the only account I had with US Bank was a car lease. There were no deposits to seize because I did not have a checking or savings account with the bank.

9: THE MESSAGE APPEARS TO BE FROM A GOVERNMENT AGENCY

Phishing artists who want to use intimidation don't always pose as a bank. Sometimes they'll send messages claiming to have come from a law enforcement agency, the IRS, the FBI, or just about any other entity that might scare the average law-abiding citizen.

I can't tell you how government agencies work outside the United States. But here, they don't normally use email as an initial point of contact. That isn't to say that law enforcement and other government agencies don't use email. However, they follow certain protocols. They don't engage in email-based extortion—at least, not in my experience.

10: SOMETHING JUST DOESN'T LOOK RIGHT

In Las Vegas, casino security teams are taught to look for anything that JDLR—just doesn't look right. The idea is that if something looks off, there's probably a good reason why. This same principle almost always applies to email messages. If you receive a message that seems suspicious, it's usually in your best interest to avoid acting on the message.

CADENCE CYBER

TOO SMART TO FALL FOR A SPEAR-PHISHING MESSAGE? THINK AGAIN

BY MICHAEL KASSNER

Let's face it: Phishing attacks—where cybercriminals disguise their malware-laced digital messages to give the appearance of official communiqués—are way more successful than anyone would like. Verizon's 2017 Data Breach Investigation Report (DBIR) said:

"There were a little over 1,600 incidents and more than 800 breaches featuring social actions in this year's [2016] corpus (all external actor driven). Phishing was again the top variety, found in over 90% of both incidents and breaches."

The DBIR continued:

"In last year's report, we discussed how the majority of remote breaches began with the same chain of events; phishing to gain a foothold via malware, then leveraging stolen credentials to pivot off of the foothold. It also holds true this year—95% of phishing attacks that led to a breach were followed by some form of software installation."

Digital bad guys hope to keep spear phishing—a more work-intensive, but lucrative form of phishing that focuses on a specific victim or company—off the radar screens of cybersecurity professionals. Experts at GreatHorn, a cloud-security company with a vested interest in spear phishing, said in the company's 2017 Spear Phishing Report that more than 90% of phishing emails captured from March to November 2016 contained spear-phishing components designed to impersonate a person familiar to a business user to fool the recipient into thinking the message came from a trusted source.

IMAGE: ISTOCK/ EHRLIF

NEW RESEARCH ABOUT SPEAR PHISHING

For several years, security researchers Zinaida Benenson and Robert Landwirth, both from Friedrich-Alexander-Universitat, along with Freya Gassmann from Universitat des Saarlandes, have been interested in what they consider unexplored territory related to spear phishing. In their paper Unpacking Spear Phishing Susceptibility (PDF), the researchers explore the decision-making process of users when they are enticed by an advertised link in a variety of spear-phishing messages.

Once the researchers were happy with their spear-phishing messages and survey questions, they recruited volunteers. The selected participants were sent either an email or a personal Facebook message with a link from a nonexistent person, claiming the link led to pictures from a party. "When clicked, the corresponding webpage showed an access denied message," the report said. "We registered the click rates and later sent the participants a questionnaire asking about their clicking behavior."

RESULTS OF THE SURVEY

Out of 720 participants, 117 clicked on the link, 502 did not, and the remaining 101 participants could not remember if they clicked or not. The proverb "Curiosity killed the cat" seems applicable, as the number-one reason for clicking on the link was curiosity (**Figure A**). "The participants explained that they knew the pictures could not be for them, but were interested in the supposedly funny or private content."

Category	N	%	κ	Explanation
Curiosity	40	34.2	0.91	Curios about the pictures, interested to see their content
Context	32	27.4	0.82	Reception of the message fits the situation of the New Year's Eve celebration
Investigation	21	17.9	0.84	Wish to find out more about the situation that caused this message
Known sender	19	16.2	0.62	Certainty or assumption that one knows the sender
Technical context	13	11.1	0.9	Technical features (operating system, browser, antivirus, university's network) will thwart threats
Fear	8	6.8	0.92	Fear that a stranger may have pictures of the receiver
Automatic	4	3.4	0.71	Clicked without thinking, impulsively

FIGURE A (IMAGE: ZINAIDA BENENSON, ROBERT LANDWIRTH, FRIEDRICH-ALEXANDER-UNIVERSITAT, FREYA GASSMANN, UNIVERSITAT DES SAARLANDES)

As to why 520 participants did not click on the link, the number-one reason was not knowing who sent the message (**Figure B**).

Category	N	%	κ	Explanation
Unknown sender	254	50.6	0.90	Sender of the message is unknown
Suspicion of Fraud*	250	49.8	0.93	Assumption that the message is fraudulent, phishing, might contain a virus
Situation context*	195	38.8	0.96	Reception of the message does not fit the situation of the New Year's Eve celebration
Life context*	58	11.6	0.75	There are no circumstances in the life of the recipient that would cause such a message
Rule of conduct	47	9.4	0.91	A behavioral rule prohibits clicking on links in such messages
Privacy	28	5.6	0.93	Private message sent to a wrong person
Message context*	27	5.4	0.87	Wrong communication channel or email address for a message like this
Message form*	25	5.0	0.91	Anonymous message, not addressed by name
Link form	20	4	0.93	Link looks suspicious
Bad experience	11	2.2	0.8	Unpleasant experience in a similar situation

FIGURE B (IMAGE: ZINAIDA BENENSON, ROBERT LANDWIRTH, FRIEDRICH-ALEXANDER-UNIVERSITAT, FREYA GASSMANN, UNIVERSITAT DES SAARLANDES)

FINDINGS OF INTEREST

After analyzing the survey results, the researchers came up with the following:

- Participants tend to trust their instincts when deciding whether to click on the link. "Many participants indicated they suspected the link to contain malware or be fraudulent without explaining how they arrived at this conclusion. It seems they relied on their intuition."
- Facebook users were more click-happy, with more than 40% clicking on the link compared to 20% of those using email. As to why, Benenson, Landwirth, and Gassmann suggested that social networks, such as Facebook or LinkedIn, might be considered more trustworthy by users.
- Using first names to personalize messages made a significant difference, particularly when it came to email participants.

REALISTIC CONSIDERATIONS

The researchers showed a refreshing awareness of how challenging it is to defend against spear phishing because of the perceived legitimacy of the message's fake content. "Because of this ambiguity, asking people to be permanently vigilant when they process their messages might have unintended consequences."

The researchers offered an example:

"If a person's job requires processing invoices sent via email, they might click on an infected file called 'invoice,' as it fits their job expectations. And if they are taught to be careful with invoices, they might start ignoring real

ones, which stands in direct conflict with their job requirements. Under these circumstances, the employees are likely to disregard their training, as the only way for them to get their job done in time is to process their emails as quickly as possible."

The researchers also offered insight into the practice of testing users by sending them fake phishing emails. "Trying to involve users in perimeter defense by means of catching them clicking links in fake phishing emails might have negative consequences. For example, employees of an organization may become disgruntled and unmotivated if they find out they are being attacked by their own security staff."

If that's not bad enough, the report concluded in a rather alarming way:

"By careful design and timing of a message, it should be possible to make virtually any person click on a link, as any person will be curious about something, or interested in some topic, or find themselves in a life situation that fits the message's content and context."

That is a chilling thought. But knowing that is half of the battle. The other half is to remain vigilant and not always take the path of convenience—and try to determine the legitimacy of the link being asked to click on.

CADENCE CYBER

PHISHING ATTACKS: HOW HUNTING DOWN FAKE WEBSITES IS MAKING LIFE HARDER FOR HACKERS

BY DANNY PALMER

Cybercriminals are finding it more difficult to maintain the malicious URLs and deceptive domains used for phishing attacks for more than a few hours because action is being taken to remove them from the internet much more quickly.

That doesn't mean that phishing—one of the most common means of performing cyberattacks—is any less dangerous—but a faster approach to dealing with the issue is starting to hinder attacks.

Deceptive domain names look like those of authentic services, so that somebody who clicks on a malicious link may not realise they aren't visiting the real website of the organisation being spoofed.

One of the most common agencies to be imitated by cyberattackers around the world is that of government tax collectors. The idea behind such attacks is that people will be tricked into believing they are owed money by emails claiming to be from the taxman.

However, no payment ever comes, and if a victim falls for such an attack, they're only going to lose money when their bank details are stolen. They can have their personal information compromised, as well.

To combat phishing and other forms of cyberattack, the UK's National Cyber Crime Centre—the internet security arm of GCHQ—launched what it called the Active Cyber Defence programme a year ago.

It appears to have had some success in its first 12 months because despite a rise in registered fraudulent domains, the lifespan of a phishing URL has been reduced and the number of global phishing attacks being carried out by UK-hosted sites has declined from five percent to three percent. The figures are laid out in a new NCSC report: Active Cyber Defence—One Year On.

During that time, 121,479 phishing sites hosted in the UK, and 18,067 worldwide spoofing UK government, were taken down, with many of them purporting to be HMRC and linked to phishing emails in the form of tax refund scams.

An active approach to dealing with phishing domains has also led to a reduction in the length of time these sites are active, potentially limiting cybercriminal campaigns before they can gain any real traction.

Prior to the launch of the program, the average time a phishing website spoofing a UK government website remained active was for 42 hours—or almost two days. Now, with an approach designed around looking for domains and taking them down, that's dropped to 10 hours, leaving a much smaller window for attacks to be effective.

However, while this does mean there's less time for the attackers to steal information or finances, it doesn't mean that they're not successful in carrying out attacks.

The increased number of registered domains for carrying out phishing attacks shows that crooks are happy to work a little bit harder to reap the rewards of campaigns—and the NCSC isn't under any illusion that the job of protecting internet users is anywhere near complete.

"The ACD programme intends to increase our cyber adversaries' risk and reduces their return on investment to protect the majority of people in the UK from cyberattacks," said Dr Ian Levy, technical director of the NCSC.

"The results we have published today are positive, but there is a lot more work to be done. The successes we have had in our first year will cause attackers to change their behaviour and we will need to adapt."

A focus on taking down HMRC and other government-related domains has helped UK internet users, but cyberattacks aren't limited by borders, with many malicious IPs hosted in practically every country used to carry out cyberattacks around the world—meaning every country should be playing a part.

"Obviously, phishing and web-inject attacks are not connected to the UK's IP space and most campaigns of these types are hosted elsewhere. There needs to be concerted international effort to have a real effect on the security of users," the report said.

CREDITS

Global Editor in Chief
Jason Hiner

Editor in Chief, UK
Steve Ranger

Managing Editor
Bill Detwiler

Editor, Australia
Chris Duckett

Senior Features Editors
Jody Gilbert
Mary Weilage

Senior Editor
Conner Forrest

Senior Writers
Dan Patterson
Teena Maddox

Chief Reporter
Nick Heath

Staff Writer
Alison DeNisco Rayome

Associate Editor
Amy Talbott

Multimedia Producer
Derek Poore

Associate Social Media Editor
Leah Brown

Cover image:
iStock/ weerapatkiatdumrong