Phishing training is more than phishing testing. Integrating computer-based training, simulated attacks, and timely, tailored feedback addresses today’s market need.

### Phishing Training Evolution: Moving from Reactive to Proactive

**June 2019**

**Written by:** Frank Dickson, Program Vice President, Security Products

---

**Introduction**

Cybersecurity is an increasingly sophisticated and complex discipline as companies struggle to prevent their digital assets from becoming comprised and their names publicized as "one of the breached." The adversary is increasingly cunning, clever, and motivated and may be an individual, a criminal cybergang, or even a nation-state.

A troubling reality is that the user is an active yet unintended participant in most breaches. Phishing, the act of soliciting unsuspecting end users to click on a malicious link or attachment, is the attack method of choice. According to the Verizon 2018 Data Breach Investigations Report, phishing and pretexting represent 93% of all social breaches. Email is the attack vector of choice in 96% of all phishing instances.

**Why Phishing?**

Phishing is easy and cheap and works for miscreants. Cybermiscreants may be evil, but they are certainly not stupid. Why recreate the wheel when the current approach works so well? In fact, the barriers to entry for phishing attacks have been lowered even further as inexpensive yet powerful dark web tools make even the unsophisticated hacker sophisticated.

Existing cybersecurity measures are very effective; however, no defense is 100% effective. The first issue to tackle is complexity of the task. Cybermiscreants are creative and clever, making emails look extremely creditable. In fact, phishing may not include a malicious payload at all. The second issue is scale. Even if your defenses stop 99.9999% of phishing emails, odds are that you will get breached if your organization sees a million phishing emails — and we know phishing emails are getting through. Research by the sponsor of this paper, Cofense, found that 1 in 7 emails reported as malicious in 2018 was indeed malicious. The result was 55,404 credential-harvesting attacks; 27,501 campaigns delivering malicious attachments; and 4,152 business email compromise (BEC) attacks.

---

**AT A GLANCE**

**KEY STATS**

- 1 in 7 emails reported as malicious in 2018 was indeed malicious.
- The result:
  - 55,404 credential-harvesting attacks
  - 27,501 campaigns delivering malicious attachments
  - 4,152 business email compromise (BEC) attacks
A Different Approach to Prevent Phishing

Given that end users accurately identify malicious emails frequently, one conclusion that can be drawn is that users are able to detect malicious emails that other defenses cannot. Humans are effective at solving unstructured problems. Phishing training is the tool that enables users to be another layer of defense. Employees can spot malicious emails that get past other "tools." For example, consider the issue of BEC. Few protections exist to prevent email account takeover. An example of BEC would be if the credentials of a CEO were phished, allowing a cybercriminal to send emails created in the CEO's legitimate, authenticated account to accounts receivable to pay an attached invoice immediately. Such fraud offers no malware to analyze because it is created with legitimate applications but with compromised credentials. The most typical types of BEC scams are as follows:

» Bogus invoices
» CEO fraud
» Account compromise
» Attorney impersonation
» Data theft

Technology is being applied to the problem, but techniques such as machine learning are practical only in very limited use cases. The reality is that machine learning models can be unproven and noisy. Additionally, the tactics, techniques, and procedures of the attacker are evolving fast, presenting machine learning with stable data set challenges. Abuse of legitimate software features and cloud services "hiding" malicious payloads in normal business communications are very difficult to defend against; thus, how do we determine the good from the bad?

Effective phishing training is not a single "thing" or method; rather, it is an integrated set of techniques that provides comprehensiveness and addresses the different ways that users learn. Computer-based training provides the foundational insights to allow users to know what to look for and supplies context to the problem. Simulated attacks provide users with realistic practice. Although the point may be obvious, to be effective, simulated attacks must be representative of the real threat actor tactics and techniques that are emerging or those that are actually being used against the organization. Thus, simulations must constantly evolve and reflect the context of individual organizations. Further, feedback on reported phishing attempts is key. Users can then learn in real time and from real emails.

The goal of training is to include the user as part of the process. Frankly, users have primary jobs to do; detecting phishing is not among them. Thus, participation must be a positive experience. Programs need to focus on engaging the end user to be an active part of the defense of the organization and reinforce desired behaviors even in the event of a harmful click.

Effective phishing training is not a single "thing" or method; rather, it is an integrated set of techniques that provides comprehensiveness and addresses the different ways that users learn.
Why Stop at Reactive Tactics? Turning Training into Proactive Intelligence

Creating a feedback loop is a valuable part of training. However, the ability to report creates intelligence feeds. Organizations spend huge sums on threat intelligence from third-party providers. Intelligence resulting from phishing reporting is not only "free" but also comes from your network and reflects your attacks. This characteristic of the intelligence makes it incredibly actionable because it is focused solely on the threats that have bypassed defenses and are underway inside the organization right now.

While the intelligence is essentially "free" (organizations technically don’t have to pay a fee for it), making good use of the intelligence requires investment and effort.

Turning reported phishing attempts into intelligence requires a platform for ingest. Every organization has tried the old-school method of emailing the help desk, and most have found it horribly inefficient. The help desk is quickly overwhelmed with emails and ends up subverting the process so that it can get the rest of its work done. In the process, the manual feedback loop to the user disappears and users stop participating. Also, remember that the help desk is staffed not by malware experts but by PC generalists. Often help desk teams are provided with a "playbook" on how to analyze reported emails. They often lack the understanding of the evolving phishing threat landscape and do not possess the skills to effectively analyze these evolving threats. Help desk teams rely on third-party threat analysis tools, which are not completely accurate, and this approach can lead to false negative results (i.e., the help desk confirms an email is safe, and then the end user clicks and is compromised).

Self-reporting also needs to be easy for users to do. The ingest needs automation. Feedback improves learning and motivates participation.

Turning reported phishing attempts into intelligence requires a platform for analytics. The scarcest resource in security is not tools or data but people. Skilled security professionals are hard to find and hard to retain. Creating unnecessary work for precious security professionals is not sustainable. Thus, the platform needs to cut through the noise to find the "bad" quickly, shifting analyst workload from spending lots of time on analysis to taking action on threats. Security professionals then deal with only the higher-value problems and not the mundane tasks. Additionally, APIs leverage the existing security architecture as automated control points for enforcement.

Considerations

The reality of any cybersecurity tool is that if it isn’t properly installed, configured, and maintained, it provides little protection. The same is true for a phishing training platform. However, much like getting value from an identity management platform, an additional challenge must be overcome for phishing training in that it requires people, processes, procedures, and management commitment to make it successful.

Programs must be transparent regarding goals and be nonpunitive in nature. Mature organizations introduce programs such as "phish bounty" to financially reward employees when malicious emails are reported. Essentially, phishing training needs to be part of the everyday processes and culture of an organization to be truly successful.
Conclusion

Let's state it emphatically: Phishing testing is not phishing training. As we have argued, effective phishing training is an integrated set of techniques that provides comprehensiveness and addresses the different ways that users learn. Computer-based training, simulated attacks, and timely and tailored feedback are foundational aspects of a successful phishing training program. Users can then learn in real time and in real emails. Capitalizing on the feedback loop to create custom intelligence feeds from your network and that reflect your attacks can provide intelligence that is especially actionable because it is focused solely on the threats that have bypassed defenses and are faced by the organization. However, such an approach to phishing is not the result of a product, a service, or a process. All three combine to offer a complete solution; in security, we need more solutions!

About the Analyst

Frank Dickson, Program Vice President, Security Products

Frank Dickson is a Program Vice President within IDC's Security Products research practice. In this role, he provides thought leadership and guidance for clients on a wide range of security products including endpoint security, identity and access management, authentication, threat analytics, and emerging products designed to protect transforming architectures and business models.
MESSAGE FROM THE SPONSOR

About Cofense

Cofense is the evolution of PhishMe, which was founded in 2008. In 2018, PhishMe was acquired by private equity and rebranded Cofense to emphasize the company's movement from providing a pure phishing training solution to an end-to-end platform for employee-sourced phishing attack intelligence. Today, Cofense employs over 400 employees around world provide phishing training and integrated anti-phishing intelligence. Among its 2,000-plus customers, Cofense includes over 50 of the Fortune 100 companies.