CUSTOMERONE

Symantec

Phish Fight: Empowering Our Employees Against Con Artists

Dan and Nancy run a small business out of their Wisconsin home. Just before Christmas they discovered that cyber-thieves had stolen $1,800 from their online bank account. Another $800 had been charged to their credit card for "escort services." [1]

Bryan was at home when someone logged into his Facebook account using stolen credentials. The scammer messaged Beny, one of Bryan's friends, saying Bryan had just been robbed in London and needed $1,143 to get back to Seattle. Beny wired the money.[2]

Dan, Nancy, and Bryan (and Beny, indirectly) were all victims of phishing. Countless others have been victimized as well—some due to their own naiveté and others because their personal information was stolen in a corporate breach.

We pay close attention to stories like these. We get targeted in phishing attacks all the time, and we know that if we lower our guard even briefly we might end up subjecting our employees and customers to the same misery that these four suffered.

We won't let that happen. **Not on our watch.**

We safeguard our customer and employee information as tightly as we do our confidential source code. We leverage our most sophisticated enterprise technologies, of course, but we also teach our employees how to be hyper-vigilant against phishing attacks.

In this CustomerONE paper we'll show you how we train our staff to be our first and strongest line of defense against phishing. We'll also discuss how we conduct stealth testing to make sure the training sinks in.

This is meant to be a high-level overview. If you'd like more details, or if you want to learn how to adapt our technologies to suit your needs, we invite you to join us for a customized executive briefing.

Phishing: an attempt, usually by email, to trick someone into sending money or revealing personal information (e.g. passwords, credit-card numbers) by posing as a trusted entity. The term derives from the act of 'fishing' by using bait to entice a victim

Spear phishing: A highly personalized phishing attempt from an apparently trustworthy source. A spear-phishing mail may address you by name and include personal details such as your home address or partial bank-account number

Whaling: A spear-phishing attempt aimed at a high-value target such as a CEO or CFO. It may masquerade as a legal subpoena, customer complaint, or company emergency

Social engineering: An attempt to trick people into divulging information, generally by taking advantage of the human desire to be helpful or social. Examples: An email, supposedly from your boss, asking you to provide employees' W-2 information; or an email, purportedly from a friend, suggesting you click on an enclosed link for a cute cat video

Phishing scams used to have obvious tip-offs—spelling errors, poor grammar, etc. But phishers have refined their techniques so much that today it can be hard to distinguish between a phishing attempt and a legitimate email. At Symantec we protect ourselves from phishing in two ways: with strong network technology and with vigilant employees who are trained to stay on their toes.

Our training is a little unusual but demonstrably effective. We use rigorous teaching modules followed by a continuous stream of both random and targeted phishing tests. This paper is written to inform CIOs, CTOs, CISOs, and other senior managers about how we use our Blackfin technology to engage our employees with phishing training, and how we make sure the lessons have sunk in.

Training our staff to spot phishing emails isn't as easy as it sounds. Some employees think they're too smart to fall for a scam. Others hate the idea of being trained on a topic they think they already know enough about. And others relax their guard because we have sophisticated technologies protecting them, and they're happy enough to let the cyber-tools bear the responsibility of being vigilant.

Kelley Bray - Employee Trust Lead

These were the challenges confronting Kelley Bray, our lead corporate trainer.

"If we manufactured widgets, security would be interesting for our employees because it's something they don't already know," Kelley says. "But when you have cybersecurity people who are already great at what they do, the challenge becomes how to spark their interest. We want them to really care about this."

Previously we relied on the same training strategy that most corporations use—long, boring PowerPoint lectures. But we noticed our staffers would just go back to their desks and return to business as usual. There was no long-term change in behavior.

So we turned to a new strategy. This one involved a combination of the security-simulation technology we acquired when we bought Blackfin in 2015, and techniques Kelley used in a previous role with the TSA (in which she helped train 55,000 people for 400 airports nationwide).

Our strategy involves a regimen of internal phishing tests managed with our Blackfin software. Within a year of rolling out the program to all 11,000 employees around the world, we've seen **a nearly 70 percent decrease** in the percentage of employees who clicked on suspicious links.

Here's our four-step process:

Step 1: Establish a baseline

We began by testing a random sample of employees. We sent them three phishing emails over a three-month period. Some were designed to look like LinkedIn invitations, while others appeared to be requests from a top executive seeking financial information or employee reports.

One test group received three "easy" emails. Those had obvious errors, poor grammar, misdirecting links, etc. The other group received emails that went from "easy" to "medium" to "hard," with the red flags becoming more difficult to spot.

We tracked a number of variables in real-time:

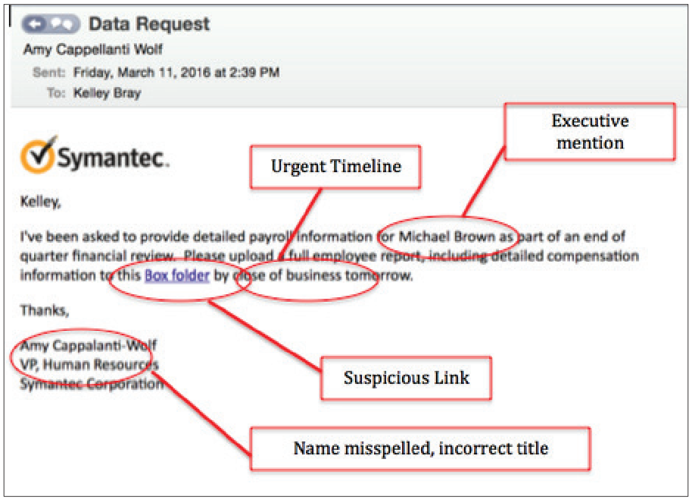
- the percentage of people who opened the emails (not considered a failure)
- the percentage who clicked on links (considered a failure). Within this group we tracked:
  - where they were located geographically
  - their roles by business unit
  - whether they accessed the emails on their laptops or mobile phones
  - whether their training was up to date

Step 2: Test everyone—and we mean everyone

Once we developed a baseline we used that information to expand testing strategically to everyone.

We phish every Symantec employee—including our CEO—multiple times a year. We do even more frequent testing of certain populations such as executives, members of our financial and legal teams, and engineers who handle confidential source code.

We also test employees in low-profile administrative roles. These folks have access to information that makes them high-value targets, so they need to be vigilant as well.



Data Request
Amy Cappellanti Wolf
Sent: Friday, March 11, 2016 at 2:39 PM
To: Kelley Bray

Kelley,

I've been asked to provide detailed payroll information for Michael Brown as part of an end of quarter financial review. Please upload a full employee report, including detailed compensation information to this Box folder by close of business tomorrow.

Thanks,

Amy Cappalanti-Wolf
VP, Human Resources
Symantec Corporation

Several red flags should cause you to distrust this email.

Step 3: Use failures as an immediate training opportunity

Employees who fail our test by clicking on a fake link are taken to a landing page that explains exactly what was fishy about the email.

They also have to retake our training module, a 4-minute video that reinforces proper phishing vigilance.

Step 4: Continue testing to make sure the lessons are retained

The bad guys never stop with their phishing attempts, so we never stop with the phishing tests. As Kelley notes, "If we're not phishing our users regularly we're not doing a good job of assessing whether they know how to do the right thing."

Clues to help identify a phishing scam:

Reply address: The reply-to email address is unusual or not quite right (e.g. name@symantec-inc.com)

Odd greetings: The email addresses you by first and last name (e.g. "Hey, John Doe" instead of "Hey, John") or with an odd degree of formality ("Hello, Mr. Smith" from a close friend)

Unusual tone: The message conveys urgency, asks for secrecy, and/or discourages questions

Common errors: There are basic spelling or grammar mistakes, and/or awkward phrasing that doesn't match how the supposed sender usually talks

Attempts to appear legitimate: It includes publicly available information irrelevant to the message, such as your phone number or colleague's name

Requests for sensitive info: It asks for W-2 documents, employee data, Social Security numbers, or for large amounts of money to be wired

Misdirecting links: The links go to unfamiliar or mismatched URLs

Signatures: The email is signed with the name of your CEO, CFO, board member or other executive

***Bottom line:** If an email asks you to disregard your company's normal procedures, treat it as highly suspicious*

Our early results show promise—fewer test fails, greater vigilance

So how well is our program working? The results to date are promising.

From the spring of 2015 to early 2016, the percentage of employees who clicked on our phishing links in comparable tests **fell nearly 70 percent**. In addition, those who completed the phishing training were **25 percent less likely** to fail again.

"One thing we observed was how positively people reacted to the tests," says Tim Fitzgerald, Symantec's chief security officer. "The more testing we did, the more proud they were of their ability to spot phishing attempts."

Our assessments are educational, not punitive

One reason we've gotten so little pushback is because no one wants to be the weak link in Symantec's defenses. The tests allow them to reinforce what they already know and point out the areas where they need to brush up.

More important, we've gone out of our way to reassure them that we're not trying to get anyone in trouble. No one who fails an assessment gets a black mark on his or her record. Here's why.

First, our corporate culture is to build positive relationships with our employees, not to create a punitive atmosphere. We want them to be vigilant because they care about keeping Symantec safe, not because they think we're looking for an excuse to get rid of them.

We also remember that a failure isn't always a failure. For example, we've had engineers tell us they knew a phishing email was a test but they took the bait just to see what would happen.

Finally, we're a globally diverse company, so language can be an issue. Before we assume our employees are doing something wrong we'll assume they didn't fully understand the message of our training.

Learn more with an executive briefing

There's more to our story, but these are the highlights. We encourage you to learn more with an executive briefing. That's where we can explain how you can adopt our model in your own environment, and how you can personalize it for your specific needs. We'll also give you a sneak peek at new threats on the horizon and the latest Symantec technologies that can keep you ahead of the curve.

We have Executive Briefing Centers at our U.S. headquarters in Mountain View, California, and in Reading, U.K.

› CONTACT SYMANTEC TODAY

[1] http://www.washingtonpost.com/wp-dyn/articles/A59349-2004Nov18.html

[2] http://www.cnn.com/2009/TECH/02/05/facebook.impostors/index.html

customer_one@symantec.com

CustomerONE Team
350 Ellis Street
Mountain View, CA 94043
800-745-6054

Symantec's CustomerONE team can facilitate discussions between you and our IT security practitioners to help you address your security questions and concerns. Please contact us directly or through your Symantec sales team.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.