Building a Security Culture

Why Security Awareness Does Not Work and What to Do Instead

Joseph Opacki
Is responsible for threat research, analysis and intelligence at PhishLabs. Prior to joining PhishLabs, Opacki was the senior director of global research at iSIGHT Partners. Before his career in the private sector, Opacki was the malware reverse engineering subject matter expert and the technical director of advanced digital forensics in the operational technology division of the US Federal Bureau of Investigation.

It is no secret that phishing has become a huge problem. In 2016, the Anti Phishing Working Group noted that there were 1,220,523 total phishing attacks—65 percent increase over the previous year. Between the last quarter of 2004 and the same period in 2016, the number of phishing attacks observed rose from 1,609 to 92,564—a jaw-dropping 5,753 percent increase.[1]

During 2016, phishing attempts grew by 33 percent across the five most targeted industries. While financial institutions remained the most popular target and saw a significant increase in phishing volume, the industry's share of phishing attacks has fallen significantly in recent years in line with a monumental increase in attacks elsewhere.[2]

It is not difficult to understand why phishing has become the favorite attack vector of both novice and professional cybercriminals. No matter what their motives or what enterprise they target, it is almost always easier to trick an employee than it is to penetrate perimeter defenses. Not only that, conducting a phishing campaign requires almost no technical skill whatsoever, meaning that threat actors are free to purchase malware from more advanced actors and use it as the payload for as many phishing campaigns as they desire. Unfortunately, while phishing may boast low barriers to entry for potential cybercriminals, it proves to be a significant headache for security professionals.

Why Technical Controls Are Not Enough

Modern spam filters are excellent pieces of technology, blocking roughly 99 percent of spam emails. The problem, naturally, is that pesky remaining 1 percent. At the time of writing this article, a typical enterprise with 5,000 employees receives an average of 620,000 emails per day.[3] Of those, one in every 722 contains malware, and one in 4,380 is a non-malware-based phishing email.[4]

If one assumes the enterprise's spam filter performs as advertised, it blocks 99 percent of these malicious emails. However, users will still collectively receive 11 malicious emails each day: two pure phishing emails and nine containing malware. That is 4,015 potential breaches every year.

Of course, spam filters are not the only technical controls employed by an average enterprise. In theory, a combination of patch management,

antimalware products and white lists would block phishing sites and prevent malware from gaining a foothold. Unfortunately, what works in theory does not always transition well to the real world.

Since most malware takes advantage of known vulnerabilities, perfect patch management should nullify the impact of most attacks. Sadly, once an enterprise grows beyond a few terminals and, particularly, once it spreads across multiple sites, perfect patch management is no longer feasible. There will always be legacy systems, old terminals or compatibility issues that cannot be remediated so simply.

Likewise, the best antimalware product in the world will never be prepared for a zero-day threat. Even if it could be, the very nature of email as a delivery system enables malware to cause significant damage without exceeding the privileges of an infected user. A ransomware Trojan, for example, can cause tremendous damage, particularly if a highly-privileged user is tricked into running it.

Pure phishing emails pose a different threat altogether. Typically targeting login credentials rather than attempting an infection, phishing emails often link to malicious websites designed to look and feel legitimate. Known phishing sites can be blocked, of course, but keeping up with the sheer rate at which new sites are set up is functionally impossible.

Even low-level threat actors are able to set up phishing sites extremely quickly using so-called "phish kits," which are often distributed freely via social media. Even worse, when PhishLabs analyzed more than 29,000 phish kits during 2016, it discovered that more than a third employed antidetection techniques, making the task of blocking sites substantially more difficult.[5]

In the end, security-conscious enterprises must face the fact that technical controls are never totally effective. As a result, users at every enterprise are constantly at risk of being exposed to phishing emails of varying complexity.

"Patching" the Human Vulnerability

No other topic in the security world is as hotly debated as security awareness training. Some experts argue that training users is usually a waste of money. Security budgets could better be spent, they argue, on more rigorous technical controls.[6] Other experts argue that since technical controls are never perfect and threat actors consistently target people via technology, user training is an essential part of any powerful security program.[7]

There are, of course, persuasive arguments on both sides of the debate. It is important to remember that, in an ideal world, technical controls should be enough to ensure security, but this world is far from ideal. No combination of security products will ever prove 100 percent effective and, even if it could, it is highly unlikely that any security budget would stretch to procuring it. The only choice, then, is to attempt to patch the human vulnerability.

"Even low-level threat actors are able to set up phishing sites extremely quickly using so-called 'phish kits,' which are often distributed freely via social media."

Training users, however, does not function the way a software patch would. Modern phishing emails often use varied and sophisticated social engineering tactics to hoodwink unsuspecting users, but there is no prepackaged product that perfectly resolves human vulnerabilities or even a list of which vulnerabilities exist. Instead, security-conscious enterprises must work to install and maintain a culture that promotes security as a collective responsibility rather than an "IT problem."

Forget Security Awareness Training

There is one thing that all security experts should be able to agree on: The vast majority of security awareness training programs are utterly worthless. Users are dragged from their desks once a year to sit in a stuffy room while a terrified help desk employee tries to explain why "fluffy1" is not a secure password. Or, even better, users are told to complete a five-minute online training package and perhaps answer a couple of multiple-choice questions at the end. Clearly, this approach to patching the human vulnerability is not effective. The problem, though, runs even deeper.

Think about the term "security awareness training." Almost everything about it is wrong. For a start, a typical user will almost always consider security to be an IT function and not something for them to worry about. For the most part, this is true, as no normal user will ever need to understand or get involved with the vast majority of security activities.

Second, what good is awareness? Security is an activity, not a concept, and simply understanding something is not the same as doing it. There is, ultimately, a huge difference between understanding that not all email is legitimate and being able to identify potential phishing scams. Rather than working to improve awareness, what is really needed is a change in security behaviors.

Finally, the word "training" must be taken more literally. In every other walk of life, training comprises a consistent and ongoing cycle of education and practice, where a built-in feedback loop informs necessary adjustments. If the human vulnerability is to be patched effectively, this approach needs to be adopted by security training providers.

If the security world is going to start taking user training seriously, a radical shift in perspective is needed. Training programs must focus on only those aspects of security that are relevant to the average user and where a change in security behaviors will directly enhance the enterprise's security.

Creating a Culture of Security

Of course, creating a culture that promotes security requires energy, careful planning and investment, not to mention a mechanism for tracking improvement. Given that, beyond simple negligence, malicious email poses by far the most significant threat to the average user, antiphishing training should take a central role.

"If the security world is going to start taking user training seriously, a radical shift in perspective is needed."

So if behavioral change rather than awareness is the goal, how should antiphishing training be approached? The first step is simple, and yet regularly overlooked: Obtain executive buy-in.

The thing about behavioral change is that it is not an overnight fix. There is no one-off course, incentive or punishment that can reliably change behaviors in the long term. As a result, a long-term project, including the investment and resources that go along with it, should be the expectation. For any project to be a success, executive buy-in is essential.

There is a problem with obtaining executive buy-in, of course. Senior executives traditionally do not have a strong understanding of security and may not understand the need for investment in a long-term behavioral change program. If that is true, a strong business case will be required to demonstrate the benefits of such a program. In particular, pains should be taken to highlight the substantial savings associated with a well-structured and well-funded program, which far outweigh the cost of investment.[8] Over time, once the program is in place, evidencing its continued

need through fewer security incidents and lower overall costs will be a simple matter. Such a program's costs, including tools and personnel, are a fraction of what organizations spend to acquire the latest security technologies (which attackers can then evade by phishing users).

So how can security behaviors be improved? Simple: Regular simulated phishing campaigns should be used to gauge current levels of phishing susceptibility and inform targeted training interventions.

For obvious reasons, this type of initiative should start with a classroom or e-learning session to cover objectives and provide initial training. After that, once per month (for example) users receive a simulated phishing email. If the email is deleted or reported to their enterprise's designated phishing team, they are considered to have passed the exercise. If they are persuaded to click a malicious link or otherwise follow the instruction of the simulated phish, they have failed.

As soon as users react to a simulated phish, they are either congratulated or directed to online training relevant to that specific campaign. If the email in question was designed to capture login credentials, for instance, the follow-up training will help users identify this type of phish in the future. This part is critical. In order for behavioral change to be achieved, immediate gratification or correction is needed. Not only does this method enable training to be focused on only the users who fail, it also incorporates the most important element in any skill-building program: deliberate practice. For this to be possible, two components are required:

1. A "Report Phish" button, made directly available within users' email client
2. An automated response, designed to congratulate success and provide further guidance in the event of failure

If either of these components is missing, the program's impact will be substantially lessened.

Beyond this immediate response, it is also vital that the program not be left to function in isolation. Results, particularly if they are positive, should be discussed during monthly or quarterly meetings, ensuring the subject remains top of mind for users and establishing security as a priority.

> **"Reported phishing emails are exponentially more valuable than ignored or deleted phishing emails."**

Experience shows that, on average, an enterprise implementing phishing simulations for the first time will see a phishing susceptibility rate of around 30 percent. In practice, that means for every 10 phishing emails that make it past the enterprise's spam filter, three successfully trick users into (for example) following a malicious link.

Returning to the earlier example of a typical enterprise with 5,000 employees, where 4,015 malicious emails make it into user inboxes each year, that equates to more than 1,200 serious security incidents annually.

By systematically exposing users to phishing emails of increasing complexity and differing types, and delivering relevant multimedia training to users who react in an undesirable way (e.g., clicking links), phishing susceptibility rates can be dramatically reduced.

Again, experience shows that any enterprise can bring its phishing susceptibility rate down to around 5 percent and, in some cases, as low as 1 to 2 percent. Now, instead of 1,200 security incidents each year, it can expect to see somewhere between 40 and 200. Clearly, this improvement facilitates a substantial reduction in incident response costs, not to mention dramatically reducing the chances of a data breach.

The Finer Points of Phishing

In principle, building a security culture based on consistent training and testing seems a simple thing. There are, however, two details that differentiate a truly powerful security training program from one that is mediocre.

When users receive a suspected phishing email, they typically have two choices: Delete it or comply with it. A truly security-conscious culture, though, would provide users with a third choice: reporting the email to a designated response team.

The simple truth is that reported phishing emails are exponentially more valuable than ignored or deleted phishing emails. They serve as an early warning mechanism and provide an opportunity to quarantine similar emails before other users are exposed. They can also be analyzed to inform improvements to technical security controls. Finally, they can be modeled and used to produce realistic ammunition for future simulated phishing campaigns.

Of course, there must be an easy and instantaneous reporting process in place. Most users, no matter how engaged, will not have time to pick up the phone every time they see a suspected phishing email. They will, however, have a few seconds to click on a "Report Phish" button in their email client.

The second detail, which has already been touched upon, is that simulated phishing campaigns must be based on real, recent phishing samples. The whole purpose of a simulated phishing campaign is to test and train users on their ability to identify phishing emails in the real world. However, it is amazing how often these campaigns use outdated phishing techniques that bear no resemblance to those used by modern phishers.

Professional phishers use a wide range of tactics, including holiday-themed scams and seemingly legitimate spoofed email addresses, to maximize their chances of success. Unless a simulated campaign can imitate these techniques effectively, it is unlikely to provide real-world benefits.

While products to prevent phishing attacks exist, a product is not the same as a program. The two details mentioned previously are not accomplished through commercial solutions. Organizations train users, but put little focus on reporting threats. When threats are reported, organizations may not analyze them. And products may craft unrealistic phishing simulations based on news headlines or generic scenarios instead of basing them on real samples.

Building Muscle Memory

To truly master any skill, a lot of deliberate practice is needed. Building and maintaining a culture of security is no different.

Reducing phishing susceptibility from 30 percent to below 5 percent is achievable for any enterprise, but it is not an overnight fix. Even once the desired rate is achieved, employee churn rates and the inevitable decline of unpracticed skills mean that a continued effort is required to maintain it.

This approach, then, must be considered a continual investment in security excellence. Certainly, the reduction in spending on incident response and data breach costs will hugely outweigh the cost of investment, but it must not be considered a one-off patch for human vulnerability.

> **"The cost of building a culture of security should be considered as necessary as the cost of employee keycards or any other direct cost of employment."**

Instead, the cost of building a culture of security should be considered as necessary as the cost of employee keycards or any other direct cost of

employment. Any single user has the potential to enable a massive data breach, and with breach fines reaching new heights every year, enterprises of all sizes have little choice but to take this risk seriously.

Only by investing in employees, rather than attempting to take them out of the equation, can a security-conscious enterprise flourish in the coming years.

Endnotes

1 Anti Phishing Working Group, *Phishing Attack Trends Report 4Q 2016,* 23 February 2017, *http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf*

2 PhishLabs, *2017 Phishing Trends and Intelligence*, February 2017, *https://info.phishlabs.com/2017-phishing-trends-and-intelligence-report-pti*

3 The Radicati Group, *Email Statistics Report, 2015–2019*, March 2015, *www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf*

4 Symantec, *Monthly Threat Report*, January 2017, *https://www.symantec.com/security_response/publications/monthlythreatreport.jsp*

5 *Op cit,* PhishLabs

6 Schneier on Security, "Security Awareness Training," 27 March 2013, *https://www.schneier.com/blog/archives/2013/03/security_awaren_1.html*

7 SearchSecurity, "Data Supports Need for Security Awareness Training Despite Naysayers," September 2012, *http://searchsecurity.techtarget.com/news/2240162630/Data-supports-need-for-awareness-training-despite-naysayers*

8 PhishLabs, "How and Why You Should Calculate Your Enterprise's Cost of Phishing," 15 November 2016, *https://info.phishlabs.com/blog/how-and-why-you-should-calculate-your-enterprises-cost-of-phishing*