No Phishing beyond This Point

Kristen Greene, Michelle Steves, and Mary Theofanos, NIST

As phishing continues to evolve, what's your organization doing to stay off the hook?

If your organization uses email, you have a phishing problem. Based on FBI data, Trend Micro predicts global losses from business email compromise (BEC) attacks will surpass $9 billion in 2018.[1] According to Symantec, the average number of malicious emails sent to the typical user increased from 8 in January 2017 to 16 in December 2017.[2] Phishing has turned a vital and pervasive means of communication—email—into a prime source of disruption for end users and organizations. In addition to revenue lost directly to malicious actors in BEC and ransomware attacks, significant economic impact also stems from phishing attacks that capture credentials and deliver malware leading to data loss and other security breaches.

WHAT'S AN ORGANIZATION TO DO?

Phishing requires a multi-pronged defense: technological solutions are far from foolproof, so organizations literally can't afford to ignore the important role that users play in organizational security. Many organizations—especially in the government sector—mandate regular user security awareness training. Some have chosen to implement embedded phishing awareness training in particular, where simulated phishing emails mimicking the latest real-world threats are sent to employees. If your organization is conducting or considering such embedded phishing training, make sure you understand what the training can and can't do.

Don't expect zero click rates

First and foremost, you can't prevent email users from falling for every phishing scam. Our prior work[3] has clearly shown that when user context and the premise of a phishing email align, some users will click.

In contrast to most phishing research, which is conducted in artificial laboratory settings with short timeframes, our phishing data was gathered over 4.5 years in an ecologically valid workplace setting and reported click rates for that period along with survey data during the final year (see Figure 1).

Participants told us through their survey responses what made them click or not. Clickers were concerned about consequences arising from not clicking, such as failing to be responsive. In contrast, non-clickers were concerned about

0018-9162/18/$33.00 © 2018 IEEE

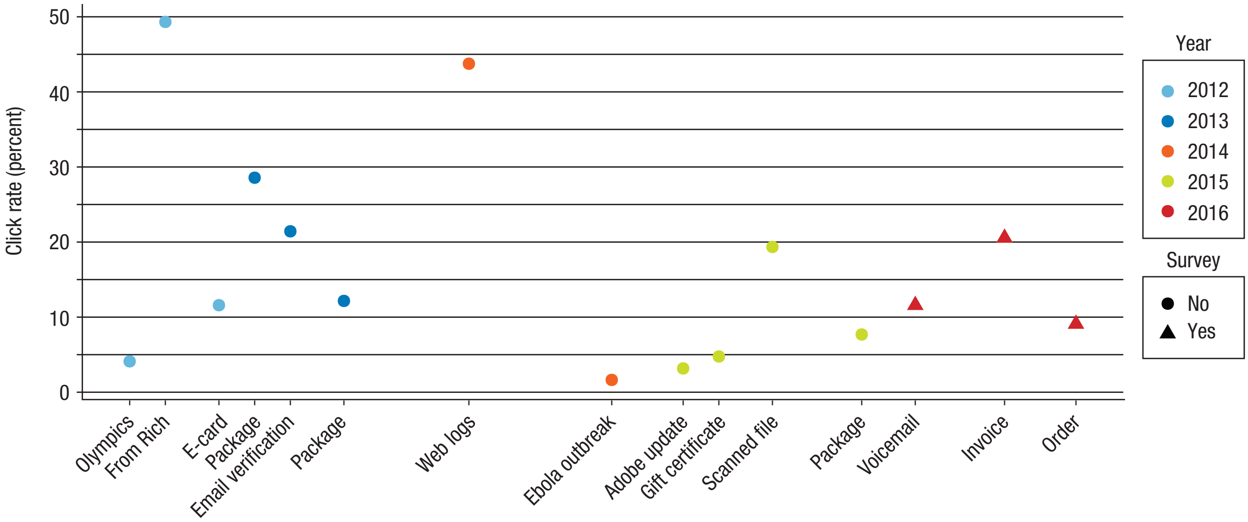

Figure 1. Click rates for various scams used in embedded phishing awareness training exercises, 2012–2016. Source: NIST.

consequences from clicking, such as downloading malware.

The alignment of user context and the phishing attack premise was a significant explanatory factor in phishing susceptibility. To illustrate, for participants who handled financial matters, the unpaid invoice and order confirmation phishing premises were particularly believable. Clickers said things like "I pay invoices so it could have been something I missed," "I am responsible for ensuring that payment is made," and "I have several orders open." Likewise, the voicemail phishing premise aligned especially well for participants who were teleworking: "I am always interested in ensuring that I get any messages and act on them," one wrote. "It could have been my supervisor or other person requiring an action on my part."

It's impossible to train the human out of people: our brains have evolved to conserve effort by relying on fast, intuitive cognitive processing using habits and heuristics.[4] This type of quick processing makes phishing detection difficult. Furthermore, given the wealth of publicly available information online, it's easy to target phishing emails to individuals, organizations, and their business processes. Add to this the ever-changing nature of phishing attacks and their increasing technological sophistication, and it's abundantly clear that click rates will never be zero.

Aim for an early warning system

Users can still significantly contribute to your organization's security if they know what to look for and how to report it. Early detection can substantially reduce phishing recovery effort and cost. Moreover, users might be your only option to catch phishing emails that get through your technological defenses.

- Make sure your users are familiar with real-world phishing threats. As tactics are constantly evolving, this requires an ongoing commitment to user education, not one-time training.
- Make sure your users know how to report suspected phishing incidents, and make it easy for them to do so.

Embedded phishing awareness training can address these points, as it uses simulated phishing emails based on current real-world threats to train users to report. But it's only as good as its implementation.

THE DEVIL'S IN THE DETAILS

If your organization decides to, or is mandated to, implement embedded phishing awareness training, realize that implementation details matter—quite a lot actually. To get a meaningful return on your investment, do more than check a training requirements box. Inform staff that your organization will be conducting phishing exercises and make sure they know how to report suspect emails. People who learn after the fact they've been phished by their own organization might feel tricked and can become resentful. At the conclusion of each exercise, recap the results to your staff: explain the premise of the exercise, what real-world threat it was based on, and what the click and reporting rates were. Never report individuals who clicked; phishing exercise data should always be aggregated and anonymized. The post-exercise recap is crucial in ensuring all staff benefit; otherwise, those who didn't see the emails miss out on the training entirely. Furthermore, it provides positive reinforcement to those users who correctly identified phishing emails and reported them appropriately.

The aim of phishing awareness training is for users to report as well as spot real-world phishing emails. For this to work, reporting mustn't be onerous. Honestly assess your current reporting mechanism: can users simply and quickly forward a suspect email to a memorizable address, or must they submit complicated help tickets with attachments? At one organization, we observed that information on how to report phishing was buried multiple pages deep in the internal help archives; only the most dedicated and persevering users would find it there. Remember that security isn't most employees' primary task, so reporting must be fast and easy.

User reporting shouldn't be a black hole. Receipt of a reported phishing email should be acknowledged immediately. You can help incentivize users to participate in bolstering organizational security by regularly reporting back to staff with statistics such as the number of reported phishing messages, the number of users who identified a new phishing threat, and so on. If you engage staff in a positive way to be part of your organization's security defenses, they'll reciprocate.

Effective phishing awareness training isn't as simple as buying a phishing software package or subscription. Effort is required behind the scenes to carefully tailor a program to your organization. Actively involving IT security officers or the equivalent can make a positive difference.

UNDERSTAND AND LEVERAGE YOUR METRICS

With phishing awareness training, it's crucial to understand what you're measuring and how you interpret that data. All too often, organizations focus only on their phishing click rate, but one number can't tell the whole story. How many users report and how quickly they report are also revealing. Timing is important in an early warning system: the sooner users report, the better.

The aim of phishing awareness training is for users to report as well as spot real-world phishing emails.

Ask yourself what the click rates and reporting rates from your exercises really represent. For example, a high click rate might indicate more than phishing susceptibility. In a recent training exercise, we heard from one participant who knew it was an exercise and clicked on a suspect link or attachment out of curiosity. If the reporting process is onerous or unknown to your users, reporting rates wouldn't actually measure the number of users who "caught" the phish but rather the number who were willing to jump your organization's reporting hurdles.

Ultimately, employee performance on training exercises isn't what you care about: it's whether employees are aware of the latest scams and how they respond to real phishing emails in the course of their work. You want users to quickly report suspected spear phishing in particular, because uniquely tailored and personalized emails are the ones most likely to sneak through filters. To have an early warning system rather than merely a reporting system, you need to be proactive—that means investigating suspected emails that users caught but filters didn't.

Once you understand your phishing awareness training metrics, commit to making use of the data and dedicate appropriate resources. Continually assess phishing threats and your organization's vulnerabilities to improve resiliency. Proactively update email filters based on the real-world phishing emails your users report. Use data analytics to track phishing attack patterns over time.

ENGAGE, DON'T PENALIZE, YOUR USERS

We firmly advocate a nonpunitive approach to phishing awareness training. Our study showed unequivocally that those who clicked on suspect links or attachments were trying to be responsive to their job duties.[3] Cybersecurity isn't baseball: "three strikes you're out" might not be an effective way to deal with otherwise good workers who take phishing bait. If employees become afraid to click on any link or attachment, even from colleagues they know, productivity could plummet.

It's entirely unreasonable to expect an impenetrable human firewall. Instead, engage your users. Help staff realize how important they are in protecting your organization against phishing threats. Many employees have unrealistic confidence in organizational IT security measures and don't realize how many emails can get past filters.[3] Encourage and even incentivize users to report phishing attempts through, for example, a "phish

DISCLAIMER

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products mentioned are necessarily the best available for the purpose.

of the month" competition or award. Examine other successful early warning systems like that of the Centers for Disease Control and Prevention, in which doctors are encouraged to report flu symptoms, and the Federal Aviation Administration, in which pilots are encouraged to report near misses.

Embedded phishing awareness training isn't the only way to train and engage your workforce to participate in IT security. Explore alternatives. Find what works best for your organization. Regardless of the mechanisms you use to combat phishing, have reasonable expectations of your staff. The user is neither the enemy nor the entire solution. No matter how good your training and reporting mechanisms are, don't expect your employees to catch everything that gets through your email filters. Nearly anything can be spoofed by more sophisticated attackers, and users can't be expected to become security experts. Regardless of what type of user awareness training you use, be sure you know what your metrics mean and how you will use that data to help your organization be more proactive in phishing defense. C

REFERENCES

1. L. Remorin, R. Flores and B. Matsukawa, *Tracking Trends in Business Email Compromise (BEC) Schemes*, Trend Micro, 18 Jan. 2018; https://documents.trendmicro.com/assets/TrackingTrendsinBusinessEmailCompromise.pdf.
2. Symantec, *2018 Internet Security Threat Report*, vol. 23, 2018; www.symantec.com/security-center/threat-report, access 4/10/2018.
3. K.K. Greene et al., "User Context: An Explanatory Variable in Phishing Susceptibility," to be published in *Proc. 2018 Workshop Usable Security* (USEC 18), 2018.
4. D. Kahneman, *Thinking, Fast and Slow*, Farrar, Straus and Giroux, 2011.

KRISTEN GREENE is a cognitive scientist at NIST. Contact her at kristen.greene@nist.gov.

MICHELLE STEVES is an information systems analyst at NIST. Contact her at michelle.steves@nist.gov.

MARY THEOFANOS is a computer scientist at NIST. Contact her at mary.theofanos@nist.gov.