KnowBe4
Human error. Conquered.

WHITEPAPER

The Phishing Breakthrough Point

Effectiveness of Phishing, Training & Understanding the Human Response

Executive Summary

Utilizing security awareness training and phishing security tests can be a useful and effective tool to reduce unintentional insider threats. However, if robust metrics are not put in place to effectively gauge the click rate patterns from a human landscape perspective, phishing tests can create organizational social engineering blind spots. Meaningful phishing assessment metrics should go beyond the click rate, and understand human patterns relative to their job and work environment.

Key Takeaways

- Awareness training makes a difference in the short and long term. IT and business decision makers should consider how effective training is in the long term when assessing the value of training services.
- "Low hanging fruit" phishing emails still work. It is important to understand the employee level of awareness in terms of levels of phishing email sophistication.
- IT and business decision makers need to be aware of how some types of jobs, and working hours of their employees can affect responses to phishing emails.
- Data-driven phishing evaluations on who is clicking what, and when, can more effectively indicate patterns of phishing vulnerabilities within an organization than the blanket click rate of the overall organization.
- Clear communication with employees regarding IT updates or HR processes can play a vital role in preventing misunderstandings and blocking phishing attempts based on generic company email themes.

About this Whitepaper

This whitepaper reports the results of a 6-month experimental study testing the effectiveness duration of the 40-minute KnowBe4 "Kevin Mitnick Security Awareness Training". The scope of the experiment was on common workplace phishing emails tested among small to medium size companies. This whitepaper was sponsored by KnowBe4.

"The adage is true that the security systems have to win every time, the attacker only has to win once."

—Dustin Dykes, CISSP
Founder Wirefall Consulting

State of Affairs in Phishing

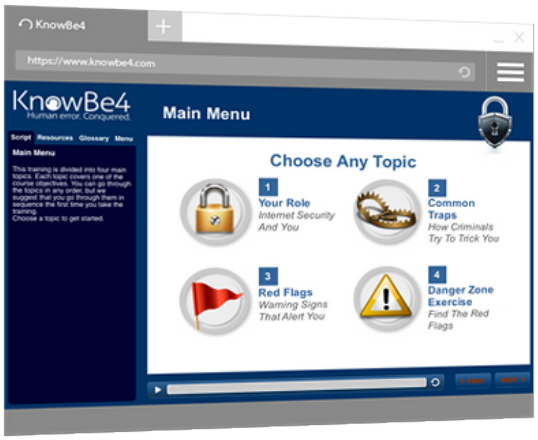
The estimated annual cost of cybercrime to the world economy in 2015 was $450 billion dollars.[1] That is a staggering amount in losses. The most concerning aspect is that 90-95% of all successful cyber-attacks begin with a phishing email.[2] It's been estimated that around 156 million emails are sent each day, 16 million make it through the filters, and 800,000 of them are not only opened, but the phishing links are clicked, and out of those who clicked it is estimated that around 80,000 share compromising information.[3] On top of this, each quarter some 250,000 new phishing URLs are identified.[4]

Even though phishing can be automated in mass campaigns, the most successful campaigns are those which are tailored to an organization or person – spear phishing. However, a significant amount are successful with mass emails that appear to come from a fake or spoofed email.

Getting through the mass phishing email hurdle is a breakthrough point in an individual's or organization's phishing awareness level. Like in the learning of a new language, a *breakthrough point*[5] is a turning point when the structure of a language starts to make sense and everything from that point on becomes easier to learn.

Similarly, in phishing, a breakthrough point is where one becomes clearly aware of the tell-tale signs, and can more easily learn and pick up on new phishing techniques. In the case of a phishing breakthrough point, once achieved, a user would consistently and systematically not click on phishing links over an extended period of time.

Testing the Breakthrough Point in Phishing Experiment:
How effective is phishing awareness training?



In the breakthrough point experiment, the effectiveness of the KnowBe4 "Kevin Mitnick Security Awareness Training" was tested over the course of half a year. Users representing five different small to medium size companies in critical infrastructure sectors participated in the experiment with a total of 1090 participants.

The training includes a web-based interface with an interactive learning platform. Using interactive, browser-based training the participant goes through the course by clicking through items, watching videos and testing their knowledge. The average time to complete the training is 40 minutes.

The experiment tested the most common workplace emails relating to Human Resources and IT. All participants were sent a baseline phishing email, which asks them to change their password immediately, and if they clicked, they were taken to a '404 Not Found' link.

Following this, participants were given a month to take the 40-minute online training, and after this, four rounds of phishing emails were sent on a monthly basis. For those who clicked on the emails sent after the baseline, they were taken to a landing page notifying them it was a phishing email and provided them with a quick rundown of things to watch out for.

Awareness, Click Rate Reduction and Understanding the Human Factor of the Persistent Clickers

There were four main findings of the study:

(1) Achieving an organizational phishing breakthrough point was possible with the "Kevin Mitnick Security Awareness" training and was sustained for the duration of the study;

(2) Moving past the click rate, patterns can be identified in organizations of those who click – in this study there were many who clicked after working hours;

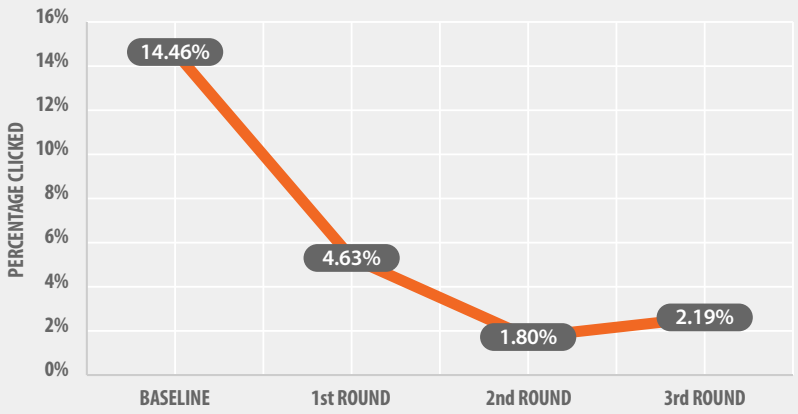
(3) Work culture and profession can play a role in phishing susceptibility;

(4) The phishing emails in this experiment could have been easily identified had there been clear communication regarding HR procedures and IT issues relevant to employees.

Sustained click rate. The results, as illustrated in the graph, showed a sustained and consistent low click rate, starting with a sharp drop after the training and then slowly decreasing. The sustained low click rate, months after the training was taken, indicated that those who fell for the phish previously did not do so again.

Once the overall sample of an organization has dropped their click rate and maintained it for a steady period after the training, the next challenge is not only to maintain the low click rate, but to understand the human aspect of those who are persistent clickers.

Breakthrough Point in Phishing Experiment Click Rate



After-hour clickers. The study examined the small percentage of those who did click even though they were trained and pieced together context and meta-data clues in efforts to understand the human factor of the persistent clicks. It turns out that depending on the organization, 25%-70% of the clickers clicked in the evenings and late at night after working hours. The combined overall percentage of those who clicked after hours was 57%. There are many factors that could be involved in these click timings, however one factor that could contribute to this is evening and graveyard shifts. While understanding this element was beyond the scope of this experiment, it was interesting to note that a significant amount of the remaining 2-4% who clicked did so after traditional office hours (8am - 5pm).

Work culture. Recognizing that each office or department within an organization has its own culture, the experiment controlled to see differences between them. For example, more often than not, it is in the job description of receptionists, human resources, customer support, medical professionals, and public relations employees to engage with others, build rapport, and be helpful both with members of their organization as well as with outsiders.[6]

"You could spend a fortune purchasing technology and services, and your network infrastructure could still remain vulnerable to old-fashioned manipulation."

—Kevin Mitnick

People in these roles tend to be targets for social engineers because of their helpful nature towards outsiders, while those working in IT, security, and legal offices tend to be guarded with their information and more often than not incorporate operational security in their day-to-day lives. The study found that those whose jobs have them interacting with outsiders were more likely to click than those who weren't.

Clear communication. The emails used in the study were simulated generic emails relating to Human Resources and IT issues. Some of these phishing emails could be easily avoided through clear communication with employees regarding updates to emails, operating systems. In the human resources domain, HR processes should be clearly communicated to prevent misunderstandings and successful phishing attempts based on generic company email themes. Open channels of effective communication to clearly manage expectations on the employee side regarding technical IT issues and HR items can go a long way in preventing clicks on generic phishing emails about updating email passwords and HR procedures. A good example: "IT will never ask you for your password".

Combining Data Driven Analysis of Phishing & the Human Factor

Whether it is for legal, audit, educational or security reasons, many organizations have enlisted security awareness training companies to help them reduce the risk of successful phishing attacks. However, sometimes Boards and auditors are only interested in low click rate numbers without delving deeper into the human aspect of those who clicked, and this can create an organizational social engineering blind spot. As it is said in cyber security circles, the defenders need to be good at preventing 100% of the attacks, while the attackers only need to be successful with one attack. With hundreds of millions of phishing emails being sent each day, it is an overwhelming endeavor on behalf of the defenders. Employees can be an effective line of defense if educated properly, and when data-driven analytics help direct appropriate training to the right audience.

Achieving a phishing breakthrough point in the organization with sustained low click rates is the first step, the next step is understanding the few that do click, and addressing the human factor of it. If an organization is trying to reduce the risk of phishing it needs to go beyond the click rate and understand the human element of the click to help contribute to a more robust counter-phishing posture.
We achieved an organizational phishing breakthrough point – now what?

What happens after an individual or an organization has reached the phishing breakthrough point? What next? -- Time to up the level.

The breakthrough point is a launch pad for more strategic and sophisticated follow on education. Just as we don't expect those who just learned to read to be able to read classical literature; we cannot expect those who just got trained in phishing awareness to be able to respond to advanced persistent threat spear phishing emails. Since infancy, the acquisition of human knowledge has been a gradual process – luckily it is one that can be improved and built on with education and experience.

The next step is to do iterative adjustments to the levels of phishing. During this time it is important to have open communication channels with the internal or external phishing service provider. For phishing email service providers, coaching should be incorporated into phishing services where phishing coaches can help organizations figure out how best to increase their awareness in a tailored way that addresses their specific organizational culture, sector and employees.

Security Culture Supporting the Front Line Human Defender

Ultimately it boils down to awareness and education. The reason why many people are familiar with the "Nigerian Prince" scam emails are because it has been featured countless times over and over in the news,[7] and a significant amount of people have encountered it either personally, through someone they know; or even through jokes which are a great way to spread awareness. The bottom line is that the more people are aware of what a phishing email looks like, the better they are at avoiding it.

Habits take time to form and become part of one's daily life – the same applies to being cyber street-smart and phishing prevention. Taking a whole organization from zero to front line defenders against cyber criminals, industrial espionage and savvy hackers takes gradual education, and patience in understanding the human landscape of an organization.

About the Author

Dr. Lydia Kostopoulos (@LKCYBER) holds a PhD in Security Policy and is a certified social engineering pentester. She is actively engaged in the U.S. and international cyber community on several fronts fostering collaboration and raising awareness to mitigate human vulnerability risks in cyber security. She participates in NATO's Science for Peace Program (SPS), teaches graduate courses on intelligence and cyber statecraft, and is a member of the FBI's InfraGard Alliance.

About KnowBe4

KnowBe4 provides you with the world's popular integrated Security Awareness Training and Simulated Phishing Platform. Thousands of enterprise accounts are using it with great results. Based on Kevin Mitnick's 30+ year unique first-hand hacking experience, you now have a tool to better manage the urgent IT security problems of social engineering and phishing – allowing you to create your "human firewall".

This is a high quality web-based interactive training combined with frequent simulated phishing attacks, using case-studies, live demo videos and short comprehension tests. Kevin Mitnick Security Awareness Training specializes in making sure employees understand the mechanisms of spam, phishing, spear phishing, malware and social engineering, and are able to apply this knowledge in their day-to-day job. You are able to send unlimited simulated phishing attacks to your employees year-round using our extensive library of phishing templates. **For more information, please visit www.Knowbe4.com**

REFERENCES:

i. CSIS McAffee Report - http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
ii. TrendMicro Research - http://www.techworld.com/news/security/91-of-cyberattacks-begin-with-spear-phishing-email-3413574/
iii. Get Cyber Safe - http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx
iv. McAfee - http://www.mcafee.com/es/resources/misc/infographic-phishing-quiz.pdf
v. Neil Jones (2014). Studies in Language Testing: Multilingual Frameworks – The construction and use of multilingual proficiency frameworks. Cambridge University Press
vi. Christopher Hadnagy (2010). Social Engineering: The Art of Human Hacking. Wiley.
vii. Blake Ellis. (2013). CNN Money. 5 most common financial scams - http://money.cnn.com/2013/09/12/pf/financial-scams/

KnowBe4
Human error. Conquered.

KnowBe4, Inc | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com