Reducing Employee Phishing Risk with Mindfulness Training

Dr. James Robinson
University of Dayton

University *of* Dayton
Center for Cybersecurity & Data Intelligence

OHIO CYBER RANGE INSTITUTE

Overview

Given that 75% of small businesses don't have sufficient personnel to address IT security, it's no wonder that 60% of small businesses victimized in a cyberattack go out of business within six months. Training employees to recognize and avoid phishing attempts is a critical component to reducing risk, but typical cybersecurity awareness training focuses on outdated or unhelpful cues, like avoidance of links. This paper draws on social science research to suggest a more effective, attention-based approach to reducing employee phishing susceptibility.

About the Author

James D. Robinson, Ph.D. (Purdue, 1982) is a professor in the Department of Communication and a Professor of Practice in the Center for Cybersecurity and Data Intelligence at the University of Dayton. His interest in cybersecurity focuses on persuasion and social influence theory as explanations for the effectiveness of social engineering attacks.

University of Dayton
Center for Cybersecurity and Data Intelligence
937-229-1929
udaytoncyber@udayton.edu

Find more tools at **go.udayton.edu/cybersecurity**

Reducing Employee Phishing Risk with Mindfulness Training

Dr. James Robinson

Professor, Department of Communication

University of Dayton

Introduction

More than 99% of US businesses are considered small to medium sized, yet they employ ~62 million workers or ~50% of all working Americans. 80% of all small businesses are run by a single owner and 29% of these businesses do not have a website. Given 25% of all business is conducted online and 75% of all shoppers visit business websites, reliance on social media is not a good business plan. A company that is unable to create and/or maintain a website is going to have trouble when it comes to cybersecurity and one reason 50% of all small businesses fail within the first five years.

The average employee receives fourteen malicious email messages annually and phishing accounts for 80% of all cyber-attacks. Phishing relies on deceptive email messages to trick employees into providing personal and account information. Approximately 43% of all phishing attacks target small businesses and 47% of all small business owners report having no idea how to protect themselves from cybercriminals. Given 75% of small businesses do not have sufficient personnel to address IT security, it is no wonder that 60% of small businesses victimized in a cyber-attack go out of business within six months (US Cyber Security Alliance, 2023).

Phishing

People are susceptible because they lack knowledge and practice identifying phishing attacks. Traditional training provides that knowledge and is often effective (Cranor, 2008; Kumaraguru et al., 2010; Nyeste & Mayhorn, 2010). Training focuses on the avoidance of link use and recognition of poor-quality images in email messages. The problem with using these cues in training is that almost all email messages contain links. Dodgy images, on the other hand, are largely a thing of the past. Below are some of the more helpful cues you can use to protect yourself and your organization.

Look first for unusual requests. Email messages requesting account verification, announcing you won the Irish Sweepstakes, or the need to renew your driver's license should be ignored. There are no exceptions to this rule. You should never provide account credentials, payment information or other personal information in an email message or into a webpage you were directed to by an email message.

Phishing attacks often contain unusual email addresses. Unusual can mean strange symbols or letter configurations, incomplete email addresses or addresses that contain country codes and deserve attention. The country code is a two-letter abbreviation that follows the domain name (e.g., .ru means the account is housed in Russia). Be on the lookout for country codes, strange symbols, and domain names used primarily by individuals (e.g., Yahoo, Google, or AOL). Amazon's domain name is Amazon and American Express's domain is AE. Remember reputable companies use their own name in email addresses because it's good for business.

Ignore email messages that contain threats. A legitimate email message may communicate urgency (e.g., 24-hour sale or a limited time offer) but never a threat. Businesses and government agencies (e.g., IRS, FBI, or Immigration & Customs Enforcement) never send threatening email. Businesses will see you in court and government agencies make their threats face-to-face in the wee hours of the morning but they won't threaten you in email.

Phishing messages often contain spelling, writing, grammatical, or typographical errors. Such writing errors are uncommon in email from reputable organizations or businesses. Take a look at the quality of the writing, appropriate use of tenses, punctuation marks, and prepositions. Multiple writing errors in a business email means something is wrong – do not comply with any request they make.

Becoming Cybermindful

Jensen et al (2017) recommends mindfulness training to supplement phishing training. Mindfulness training encourages being attentive to the tasks at hand while remaining attentive to the other things happening around you. Mindfulness training helps people make good decisions and helps them with their allocation of attentional resources.

Jensen et al (2017) contend mindfulness can be increased by self-questioning, maintaining awareness, and reflecting on the consequences of their behavior. Mindfulness training helps people forestall judgments, use environmental cues in decision making (Baer, Smith, & Allen, 2004; Ndubisi, 2012), maintain higher levels of behavioral control and self-regulation (Brown, Ryan, & Cresswell, 2007; Leary, Adams, & Tate, 2006).

Jensen et al (2017) used a strategy they called stop, think, and check before replying to email. Stop is a reminder not to behave automatically or out of habit. Think is a reminder to examine the email and the request carefully. This is where that traditional phishing training is most useful. A little awareness can help you identify a poorly written email, an unusual request or an unusual address. Check is a reminder to determine if the email request is legitimate before you comply with the request. This invariably involves a phone call but even a discussion with a coworker can reduce susceptibility to a phishing attack.

The Effectiveness of Mindfulness Training

Jensen et al (2017) found that the addition of mindfulness training significantly reduced phishing susceptibility. About 24% of the untrained study participants fell for the phishing email. After traditional training, victimization dropped to 11.8%. When employees received traditional and mindfulness training, only 7.5% were victimized in the phishing attack.

Traditional Training & Attention

Traditional training works because people learn to identify phishing attacks. Unfortunately, susceptibility to phishing is more than a failure to recognize email cues. Our ability to pay attention is limited – we can only attend to so much and then we miss things. A person engaged in a complex task is more susceptible to victimization because they can only attend to so many things at one time. People preoccupied with other thoughts are less likely to notice the cues they could use to protect themselves.

Simons and Chabris (1999) asked students to watch a video of people passing a basketball. All wore white shirts and once they passed the ball they would move to a new position on the floor. Three other people were passing a basketball and wearing black shirts. Both groups of basketball players were behaving identically – the only difference being the color of their shirt.

Study participants were asked to count the number of times the white team passed the ball and ignore passes made by people in black shirts. Participants were then asked, "How many passes did the white team make?" and "did anything unusual happen during the game?" Most people could accurately count the number of passes but about half failed to notice the gorilla walking through the game. You can see what respondents could have seen in the video https://www.youtube.com/watch?v=hstDjrQNPz4.

Respondents didn't notice the gorilla because they were so focused on the task – counting passes. This phenomenon is called inattentional blindness and a problem whenever people are multitasking. Devoting a lot of effort attending to one thing makes us less able to notice other things. Spelling errors, dodgy email addresses and unusual requests may not be noticed if someone is worrying about completing a project. In short, people who can recognize phishing cues are still susceptible if they don't maintain their mindfulness.

The Experiment

Langer, Blank, and Chanowitz (1978) identified another reason people are susceptible to attacks even after receiving phishing training. They observed people often rely on heuristics instead of carefully considering the information available to them when making decisions.

In the experiment, Langer interrupted people about to make copies with the following statements: "Excuse me, I have 5 pages." "May I use the Xerox machine?" This is a small request (only 5 pages) with no reason for the request is provided and sixty percent of the participants complied with this request.

The next twenty people were interrupted with the statements: "Excuse me, I have 5 pages." "May I use the Xerox machine, because I'm in a rush?" Here a small request is followed by a reason for that request (they are in a rush) and 94% of the respondents complied.

In condition three, twenty people were interrupted with the statement: "Excuse me, I have 5 pages." "May I use the Xerox machine, because I have to make copies?" In this case, the request is small and the reason for the request is not very reasonable. Everyone involved needs to make copies and yet 93% complied with the request. The question being examined is "Why would people comply at the rates that they did?"

Langer argues that the word because functions as a heuristic and indicates a reason for the request will follow. Once the heuristic is noticed, people ignore the reason and simply comply with the request. This study illustrates that when a request is small and the word because is included before the reason for the request, people do not scrutinize the reason for the favor. Once they hear that the request is small and that a reason is coming right after the word because they stop processing the information and simply comply. It is easier ore takes less cognitive effort for them to comply than to consider the reason for the request.

In study two, Langer told study participants the individual making the request was going to make 20 copies instead of 5. She found it made no difference if the participants were given a reason (I am in a rush), no reason, or a bad reason (I have to make copies). In each condition, 24% complied with the request.

People were no longer using the heuristic because to evaluate the reason provided because the request size changed. Once they realized they would have to wait for 20 pages to be copied, they scrutinized the reason provided by the person asking for the favor. A bad reason or no reason is not very compelling and understandably only 24% of the people complied under those conditions. Most interesting is that a reason like "I am in a rush" is not adequate for larger requests. Keep in mind that even when a request was small request compliance dropped from 90% to 60% if the word because and/or a rationale for the request was not provided. People don't care what the reason is because it is not a big request but they do care that a reason is provided. The heuristic because replaces the reason.

If you look at a phishing message as an analog of the request made in the Langer study, it is easy to see why people are susceptible to attacks even after they receive traditional training. If the request is small (verify your account) and the word because is followed by a reason, some people just comply instead of carefully processing the request and the reason for that request. If they are preoccupied with other thoughts – they may not even notice cues that could help them. You will notice that phishing attacks seldom make large requests of their victims. The hacker does not make larger requests because they do not want to move the victims from relying on heuristics and processing the request carefully. Mindfulness training is effective because it helps people notice the cues they were taught in traditional training and it reduces the likelihood that they will rely on a heuristic when faced with a small request.

Conclusion

Jensen et al (2017) point out that victimization rates for people who received no training were 24% and that dropped to just under 12% with traditional phishing training. Those individuals who received traditional training would NOT have been victimized if they had followed the rule “don’t click on a link embedded in an email” and yet nearly 12% of the study participants fell prey to the attack. It is interesting to note the no-training group and the traditional training group believed they were knowledgeable and skillful enough protect themselves from a phishing attack. Obviously, they were mistaken because participants receiving traditional training or no training were almost twice as likely to be victimized than the group given mindfulness training.

The addition of mindfulness training reduced victimization to 7.5% and works because it helps people avoid routinized or mindless replies to requests. Once routinized behavior is disrupted – that is to say people are paying a modicum of attention to the information available to them – they are more likely to notice unusual things within the attack message and consider the request and the reason for the request more carefully. Simply reminding people to stop, think, and check can significantly reduce victimization rates because it helps break habitual responses and reliance on heuristics in evaluating information.

What happens during this process is clear. When the request is carefully examined the potential victim is faced with some of the following questions: (1) “What is my relationship with the sender?” (2) “Does the request ask for private or proprietary information?” (3) “Is the email message written in a manner that leads you to believe it is legitimate?” (4) “Does the email occur at an unusual time?” (5) “Is the request unexpected and/or urgent?” (6) “Has this sender ever requested anything from me before?” (7) “Were the previous requests like this or were they different?” (8) “What are the consequences of complying with the request if it is a scam?”

Finding an email message unusual necessitates request verification. One telephone call can determine the legitimacy of the request. The hacker is banking on people responding with little thought. Let them wait. If the request is legitimate – you will get another email or a phone call. Verifying the request should not make anyone in the organization unhappy. But even if it does make someone unhappy – they will be a lot less happy if there is a breach. You are checking for the greater good – that’s how organizations must view cybersecurity consciousness.

References

- Baer, R., Smith, G., & Allen, K. (2004). Assessment of mindfulness by self-report: the Kentucky inventory of mindfulness skills. *Assessment, 11(3)*, 191–206. https://doi.org/10.1177/1073191104268029
- Brown, K. Ryan, R., & Cresswell, J.D. (2007). Addressing fundamental questions about mindfulness. *Psychological Inquiry*, 18(4) 272-281.
- Cranor, L.F. (2008). Can phishing be foiled? *Scientific American*, 299(6), 104–110.
- Jensen, M., Dinger, M., Wright, R., & Thatcher, J. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, 34, 597-626.
- Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, 10(2), 1-31.
- Langer, E., Blank, A. & Chanowitz, B. (1978). The mindlessness of ostensibly thoughtful action: The role of ‘placebic’ information in interpersonal interaction. *Journal of Personality and Social Psychology*, 36, 635-642.
- Leary, M. R., Adams, C. E. & Tate, E. B. (2006). Hypo-egoic self-regulation: Exercising self-control by diminishing the influence of the self. *Journal of Personality*, 74, 1803–1831.
- Ndubisi, N. (2012). Mindfulness, reliability, pre-emptive conflict handling, customer orientation and outcomes in Malaysia's healthcare sector. Journal of Business Research 65(4),537-546
- Nyeste, C. & Mayhorn, P. (2010). Training users to counteract phishing. Work (Reading, Mass.), 41 Suppl 1, 3549–3552. https://doi.org/10.3233/WOR-2012-1054-3549
- Simons & Chambris (1999). Gorillas in our midst: Sustained inattentional blindness for dynamic events. *Perception*, 28, 1059-1074.