Phishing Our Employees

Readers of this magazine know the severity of phishing and are familiar with the risks from spear phishing. Among the best-known examples was the 2011 attack against employees of RSA, resulting in compromised RSA SecurID tokens.

In the January/February 2014 issue of this magazine, “Going Spear Phishing: Exploring Embedded Training and Awareness” (D. Caputo et al., vol. 12, no. 1, pp. 28–38) described an experiment in which employees of an unnamed company were phished (with the permission of the company’s management) to see whether training would reduce their susceptibility to being phishing victims. To the disappointment of the researchers, many users thought that the popup training window shown when the user clicked on the phishing link was itself malware, and they never proceeded to the training.

Just after that article was published, The Washington Post reported a phishing test by an unnamed US Army organization to test its employees (“Gone Phishing: Army Uses Thrift Savings Plan in Fake E-mail to Test Cybersecurity Awareness,” www.washingtonpost.com/politics/gone-phishing-army-uses-thrift-savings-plan-in-fake-email-to-test-cybersecurity-awareness/2014/03/13/8ad01b84-s9f3-11e3-b61e-8051b8b52d06_story.html). The test, which apparently had not been approved by higher-ups, told employees to reset their passwords for the Thrift Savings Plan (a US government employees retirement plan). Employees didn’t take the bait and reported the phish attempt, which led to an investigation. According to the article, not a single employee clicked on the phishing link, which seems improbable, to say the least! (Perhaps they were particularly cautious because a real phishing attack used the same Thrift Savings Plan ruse in 2006. In that case, “TSP officials have no tally of how many people got the phony e-mail or how many responded and turned over personal financial information. … Some people did fall for the scheme, the officials said”; www.washingtonpost.com/wp-dyn/content/article/2006/03/19/AR2006031900827.html.)

In my own field of voting, phishing is a particular concern. An increasing number of voters receive their blank ballots online, but what if fake ballots are sent to voters, causing them to open (malicious) attachments? This isn’t just hypothetical; in April 2014, the Maryland State Board of Elections (SBE) warned on its website: “Potential phishing alert! Legitimate emails from the State Board of Elections end with maryland.gov. If you receive an email stating that it is from ‘The State Board of Elections’ from an email address that does not end with maryland.gov, do not open the email and delete it immediately.”

As readers of this magazine know, a phishing attack could just as easily claim to be from maryland.gov as any other domain, so this advice isn’t particularly useful. In response to a request for additional information, the Maryland SBE wrote, “We received several reports that candidates and committee members received emails from The State Board of Elections. We did not send the email, and the email address associated with the email was a gmail account. The email informed the recipients that a document had been uploaded and included a link for the recipient to click.”

But what if the phishing is neither by outsiders trying to steal secrets, like the RSA and Maryland SBE examples, nor by insiders training and testing, like the other two examples—rather, what if it isn’t phishing at all? What if instead it’s a message sent by a trusted insider who unintentionally sends email that looks like phishing messages to fellow employees? Antispam tools might flag these (false positives), but even if they don’t, such tools are at best approximations, and users must sometimes make decisions whether a message is spam (or phishing).

Over the past few years, I’ve collected emails sent by organizations to their own employees that have the characteristics of phishing emails but are in fact legitimate. These include messages from corporate security personnel, telling employees with security clearances to “click here to read this important message about your clearance,” and messages from human
resources departments about longevity awards, telling employees to “click here to select your award for five years with the company.”

These messages occur because of a presumed efficiency on the part of the sender (for example, the human resources department), but they create inefficiency on the part of the recipient, who has to figure out if the information is genuine and of interest. But is this efficiency by the sender real, or are we too often spamming people—rather than targeting them—because it’s so easy to do so? In general, when I questioned people who send me what I think might be phishing messages, they’re accepting, but occasionally they’re annoyed that I didn’t just “click the link.”

Are-they-phishing-or-are-they-real messages point to the real question of how an email recipient can verify the sender's identity. In today’s Internet, this is an unusually difficult problem to solve. While the technology is well understood (PKIs and digitally signed emails were designed to solve the problem), readers are painfully aware that there’s been minimal adoption of such technologies.

The issue isn’t new. In “Insiders Behaving Badly,” in this magazine’s July/August 2008 issue (J. Predd et al., vol. 6, no. 4, pp. 66–70), the authors defined an insider taxonomy and pointed out that we need to pay attention to legitimate insiders who inadvertently do things on our systems that we don’t want them to do. Sending legitimate messages that look like phishing emails is an example of insiders accidentally harming their organization, albeit in a way significantly different from what’s usually thought of as insider threat.

Do legitimate but phishing-like messages cause harm? Even if we assume that all the attachments and links in the messages are safe, I believe phishing-like messages are still harmful because they teach employees to trust messages that look modestly legitimate, thus lowering their guard if a real phishing email appears. Even for those employees who question the authenticity of such messages, a few “don’t worry, it’s real” responses will lower their level of caution.

So what can we do, short of a worldwide authentication mechanism for email? Technical approaches might be a partial solution. Some organizations add a tag to subject lines of any email that comes from an external email gateway (“[EXTERNAL]”) to warn the user that if the message appears to be from a company insider, it probably isn’t. But even if we assume that the notion of “external mail gateway” is still meaningful in an era where firewalls are crumbling, this doesn’t help if the “attack” truly comes from within.

For the small fraction of organizations that issue keys and digital certificates to all employees, this technology could be leveraged to reduce risk. For example, mail servers could rewrite links to point to an intermediate server that would ask the user if he or she really intended to click on the link; links in emails could be left unchanged if the message is signed with a certificate recognized by the organization (such as internal users). This would allow organizations to send links to be used by employees while protecting against potentially malicious links. Of course, this doesn’t protect against insiders including links that point to malicious sites, but it allows some degree of control for insiders sending messages that contain links. (Encrypted emails can’t be rewritten, of course, but for the foreseeable future, that isn’t a meaningful limitation.)

In a similar vein, mail clients could be modified to require an extra level of confirmation before opening attachments if the message isn’t signed by a known insider—perhaps solving a CAPTCHA to emphasize to the user that the action isn’t trivial. This isn’t unique to solving the fake-phishing problem, but would allow distinguishing legitimate insider requests from outside phishers.

These certainly aren’t the only technical solutions, but they could be implemented relatively easily by leveraging existing technology. For now, the main approach should be a two-pronged educational effort. The first is obvious—continuing existing efforts to teach the public about resisting phishing, recognizing that new approaches will be necessary because existing techniques haven’t been adequate. The second is more complex—teaching those in nontechnical roles, such as human resources, payroll, and facilities organizations, to avoid sending unexpected messages that have the characteristics of a phishing message, lest they serve to train employees to reduce their vigilance.

Perhaps over the longer term, a combination of technical assistance and training could help—a plug-in to a mail client might analyze an email before it gets sent and warn the user if the message has the characteristics of a phishing message. This could be useful to help nontechnical users avoid sending phishing messages, but it could also be useful to attackers in crafting their messages to minimize the risk of detection. For now, we need to be careful—but recognize that some of the suspicious-looking messages really are legitimate.