Are you a hack waiting to happen? Your boss wants to know

February 12 2015, byBarbara Ortutay

In this June 16, 2013 file photo, users browse the Internet in an underground station in Hong Kong. As hacks abound, some companies are testing workers' security-savvy by sending spoof phishing emails to see who bites. (AP Photo/Kin Cheung, File)

Are you a hack waiting to happen? Your boss wants to find out.

High-profile hacks have companies on the defensive, trying to prevent

becoming the next Sony Pictures or Anthem. And data shows phishing emails are more and more common as entry points for hackers—unwittingly clicking on a link in a scam email could unleash malware into a network or provide other access to cyberthieves.

So a growing number of companies, including Twitter Inc., are giving their workers' a pop quiz, testing security savvy by sending spoof phishing emails to see who bites.

"New employees fall for it all the time," said Josh Aberant, postmaster at Twitter, during a data privacy town hall meeting recently in New York City.

Falling for the fake scam offers a teachable moment that businesses hope will ensure employees won't succumb to a real threat. It's even a niche industry: companies like Wombat Security and PhishMe offer the service for a fee.

Phishing is very effective, according to Verizon's 2014 data breach investigations report, one of the most comprehensive in the industry. Eighteen percent of users will visit a link in a phishing email which could compromise their data, the report found.

Not only is phishing on the rise, the phish are getting smarter. Criminals are "getting clever about social engineering," said Patrick Peterson, CEO of email security company Agari. As more people wise up to age-old PayPal and bank scams, for example, phishing emails are evolving. You might see a Walgreens gift card offer or a notice about President Barack Obama warning you about Ebola.

The phishing tests recognize that many security breaches are the result of human error. A recent study by the nonprofit Online Trust Alliance found that of more than 1,000 breaches in the first half of 2014, 90

percent were preventable and more than 1 in 4 were caused by employees, many by accident.

Fake phishing emails are indistinguishable from the real ones. That's the point. In one sent out by Wombat, the subject reads "Email Account Security Report - Unusual Activity." The email informs the recipient that his or her account will be locked for unusual activity such as sending a large number of undeliverable messages. At the bottom there's a link that, were this a real phishing email, would infect the recipient's computer with malicious software or steal password and login information.

If you click?

Up pops a web page: "Oops! The email you just responded to was a fake phishing email. Don't worry! It was sent to you to help you learn how to avoid real attacks. Please do not share your experience with colleagues, so they can learn too." It also offers tips on recognizing suspicious messages.

In the 14 years since PhishMe CEO and co-founder Rohyt Belani has been in the information security field, he says it's changed from something a "geek in the back room" was supposed to take care of to something companies now handle at the highest level of management. The nature of the intruder also has changed, from pranksters to criminal organizations and nation-states.

As the security industry developed, he said, so did the idea of the user as "stupid" and the "weakest link," destined to continue to fall for phishing attempts and other scams. Belani disagrees with that, faulting the security industry for not better training workers.

"We posted posters in hallways, gave out squishy balls, (made) screen

savers," he said. "When was the last time you changed your password because of a squishy ball?"

While phishing training emails are a "good cautionary measure," they aren't "actually going to strike at the core of the issue," believes Agari's Peterson. He, along with large Internet companies such as Facebook Inc., Google Inc. and Microsoft Corp., support establishing a standard that makes it impossible for scammers to impersonate your bank, social network or other business in an email. Think of it as a verification system for emails. For now, though, this seems a long way off.

So, at Pinnacle Financial Partners in Nashville, Tennessee, employees will continue to receive fake phishing emails, about one a quarter. The results are reported to the company's audit committee and board of directors, said Chief Information officer Randy Withrow. Since the 800-employee company started the Wombat program Withrow said it has seen a 25 percent drop in successful phishing attempts.

Workers "take it very personally" when they fall for it, he said. "They become apologetic and wonder, 'how did I miss it?"

Luckily for Pinnacle, it was only a test.

© 2015 The Associated Press. All rights reserved.

Citation: Are you a hack waiting to happen? Your boss wants to know (2015, February 12) retrieved 4 April 2024 from https://phys.org/news/2015-02-hack-boss.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.