BTB SECURITY

PHISHING 2.0:

OLD TRICKS STILL NET BIG BUCKS

We've all heard stories of employees who got an email from their boss asking them to purchase gift cards or share sensitive corporate information. Who would fall for that, you might think? But spoofed emails purportedly from company execs or vendors are on the rise. They still rely on the same old social engineering tricks, although sometimes they're dressed up in new ways.

Plenty of employees still fall for phishing. An advisory published by the U.S. Securities and Exchange Commission last fall describes how nine publicly traded companies were hacked through phishing emails that impersonated company executives. The firms lost a combined $100 million before they became aware of the scams.

"It's easy to say, in hindsight, 'how could these companies let this happen?'" says Matt Wilson, BTB Security's Chief Information Security Advisor. "But it can be really hard to distinguish between a real email and a fake one."

In fact, business email scams have caused almost $6 billion in losses since 2013, according to the FBI. That's the highest estimated out-of-pocket losses from any cyber-related crime during that period. Verizon's 2019 Data Breach Investigations Report revealed a large number of social engineering hacks, usually phishing, targeting C-suite executives. They were 12 times more likely to experience a social engineering incident than during the previous year.

Technology alone won't solve the problem, although some vendors want you to believe that.

"Just building higher walls and deeper moats isn't going to solve all security problems," he says. It takes a comprehensive strategy, "a trifecta of people, process and technology."

Most people are savvier than they used to be; few fall for the Nigerian prince scam. But today's hackers are more sophisticated, more careful, and more organized. They research their targets in order to craft especially relevant messages that are hard for the recipient to disregard. And there are new ways to dress up phishy messages. For example, hackers use URL shorteners like bit.ly to cover up suspicious-looking links.

"They hide in plain sight by using something that's normalized, like a Word or PDF attachment," Wilson says. In fact, BTB has noticed an increase in malware being delivered through such attachments.

The bad guys have also found more ponds in which to phish.

"The attack surfaces have multiplied," says Wilson. "Ten years ago, there was no Facebook, no smartphone apps."

The bottom line is that hackers are creative, constantly coming up with new ways to trick you. And they have increased their odds by scaling up the size of their operations. "They continue to do this because it works," says Wilson. "They can send 10 million emails about as cheaply as they can send one, and all they need is a couple of people to fall for the trick."

Given this scale, persistence and sophistication, businesses need to be realistic and assume that hackers will get through all their defenses at some point. Which is why that trifecta of security is so important.

KEY ELEMENTS

1. **PEOPLE:** All employees, including executives, should get regular, rigorous training. Make sure it's more than just a recitation of the same rote rules. Wilson recommends turning up people's "spidey senses," recharging the natural instinct people have when something feels, well, phishy. One way to do that is to present the danger within the employees' personal context. Ask, for example, how they would feel if their Social Security numbers were stolen from their employer's HR department. "Show them they've got some skin in the game," Wilson says.

2. **TECHNOLOGY:** Having good tools is critical, but they should be used in conjunction with good training and good processes. "Any company that buys technology and thinks they are done – no matter how good the technology is – is making a mistake."

3. **PROCESS:** Qualified tech staff should monitor the tools, watching the alerts and determining which present real danger. But just as important is to have a process in place – an incident response plan – for when a serious breach happens. How will you know when and how the hackers got in? Where in your environment did they go? What information did they take? "These are the first questions that your leadership, and any regulators, will ask," says Wilson.

This three-pronged approach protects not just against phishing.

"If you really want to stop phishing, you need to adopt a comprehensive approach," Wilson says.

The good news is you'll increase protection from all cyberattacks.

MATTHEW WILSON
Chief Information Security Advisor

> They can send 10 million emails about as cheaply as they can send one, and all they need is a couple of people to fall for the trick."

TYPES OF PHISHING ATTACKS

- **SPOOFING:** Using a familiar but subtly changed username, corporate name, brand name and/or domain. For example, a hacker might use john.doe@xyz-company.com as opposed to the correct john.doe@xyzcompany.com.
- **URL PHISHING:** Using a fake URL that is obfuscated. Either it is not shown – the email just says "click here," or is hidden behind in some way, perhaps by using a link shortener such as bit.ly or owl.ly.
- **POP-UP PHISHING:** Messages pop up on a website, which when clicked upon redirect to a fake site that steals login credentials.
- **VISHING:** Phishing done by voice/over the phone. The caller may impersonate a colleague, customer or business. Hackers research social media for details that can make this quite convincing.
- **SMISHING:** Phishing by SMS. An alert might inform you of an order you never made and include a cancellation link, which goes to a site designed to gather personal details.
- **SEARCH ENGINE PHISHING:** Hackers create a fake webpage based on specific keywords. Searchers click on the link, assuming it's a valid result.
- **SPEAR PHISHING:** Well researched messages, specifically targeted to particular users.
- **WHALING:** Like spear phishing, but even more specific. Whaling usually targets C-suite executives.
- **CLONE PHISHING:** Hackers use the text of a previously sent, valid email with a link or attachment, substituting their own malicious link or attachment.
- **IMAGE PHISHING:** Attackers use images or other media files to deliver malware.