How to Stop Whaling Attacks From Sinking Your Biotech Firm

Posted by Steven Vigeant on 10/11/16 8:30 AM

You don't need to be a hardened sea dog to know the bigger the fish, the harder to catch — but the bigger the payoff. Cybercriminals understand this concept, too. And as their phishing techniques become increasingly polished, they're turning their harpoons on the leviathans of the business world: the C-suite.

When cybersecurity experts talk about **whaling,** they could mean one of two types of attack:

- A spear phishing attack directed against senior executives, with the goal of accessing customer data, bank account numbers, passwords, or any other valuable information. (As described in this recent Kaspersky article.)
- A spear phishing attack in which the attackers digitally impersonate a senior executive, in the hopes of tricking lower-level employees into making a wire transfer or revealing sensitive information. (As described b Mimecast here.)

Thar She Blows! Whaling Is on the Rise

According to a recent Mimecast survey, the frequency of cyber-whaling is steadily climbing. The FBI, which term it "business e-mail compromise" (BEC), issued a warning about whaling just this June. In the past three years, th FBI reported, large and small businesses worldwide have lost a combined $3.1 billion to whaling.

It's worth noting that whalers are not necessarily the most technologically sophisticated group of hackers. Their power comes not from their code-cracking wizardry, but from the wealth of information available about each of u publicly on social media networks and websites.

(For example, this teen explains how he hacked the CIA director's personal email simply by looking up his telephone number and then posing as a Verizon employee.)

Here is how a typical whaling scenario might unfold:

- A hacker will learn all they can about your company's CEO from their online bio, their LinkedIn profile, and news articles about them.
- The hacker will target someone in your company with the authority to make a wire transfer, an accountant, f example.
- The hacker will set up a spoof email account using a fake domain name only a character or two off from you company's real domain.
- The hacker will send a few innocuous emails to their target to establish trust: "How are you? Are you in today?" The hacker will replicate their whale's writing style based on information they found online, referencing personal details to round out the ruse.
- Trust secured, the hacker will strike, asking the target in the voice of your CEO to transfer money to a certa account. The target, thinking they're doing the CEO's bidding, will unknowingly transfer the money directly into the hacker's waiting pocket.

Protecting Your Biotech Firm From Whalers

Whaling is so hard to stop because it's so simple; whaling emails often include no links, no attachments, and none of the machine-generated hallmarks of spam. But the consequences can be devastating.

Just imagine what would happen if your CEO inadvertently revealed your latest experimental data to a hacker, who in turn sold it to a competitor? Or if a hacker posing as a top executive convinced an employee to email protected health information outside your organization? It could ruin your business.

Here are a few tips to avoid becoming the target of a whaling attack:

- **Focus on awareness.** Make sure everyone in your team, from the CEO on down, is trained to be skeptica about their email, especially ones that ask for sensitive information. Teach them to look closely at domain names to make sure they're exact matches for the ones they expect.
- **Limit your executives' exposure.** Review social media privacy settings with top executives to make sure their over-sharing doesn't endanger the whole company.
- **Bring in an expert.** Have a trusted IT provider assess your company's risk for whaling and recommend protective measures.
- **Invest in anti-whaling software.** Developers like Mimecast are making headway against whaling, using intelligent algorithms to search for suspicious patterns in email.

What do you do to protect your biotech firm from threats like whaling, phishing, and spear fishing? Share your tips in the comments section below.