Don’t be the Phish: One Click Could Destroy Your Business

Howard Green

Email is now the weapon of choice for cyber criminals--and we’re all prize targets. Let’s face it, most of us have been the “phish” on the email hook, baited by cybercrooks who’ve found ways to lure us into dangerous waters.

Far too many of us have clicked on links we shouldn’t have. As a result, bank accounts have been emptied and companies left widely exposed by electronic thieves, leading to debilitating financial losses. There’s also reputational damage. Experts say one in three consumers no longer does business with a company that’s had a security breach.

According to Michael Hiskey, Chief Strategy Officer at Avanan, a cloud security company that concluded its clients’ biggest cyberthreats arrive in employees’ inboxes, more than ninety percent of security breaches start with an email. That includes the headliners you hear about on the news. “The number one problem that results in breach is email-based phishing attacks”, says Hiskey’s colleague, VP Don Byrne. Hiskey adds that email, the all-too familiar way we communicate, “is a front door to your infrastructure”. What’s often viewed as a minor annoyance is suddenly deadly serious.

At its most basic, phishing means you get an email from someone impersonating someone they’re not. Sleepwalking through your unread messages, you fall for the scam and whatever its urgent instructions are--i.e. click on this link. By doing so, you might have been duped into paying a fake invoice--or perhaps worse, you unleashed toxic software known as malware on to your network granting open access to a thief. Once in, the perpetrator will work unseen, undetected, sometimes over a period of weeks to access your system administrator passwords, download email, determine critical servers, key files, client data, designs and more; akin to grabbing the combination to your safe deposit box, or that of your employer.

Often, thieves are lurking behind the spoofed logo of a well-known, trusted brand, like Amazon, PayPal, FedEx or a bank. In cases of so-called ‘spear-phishing’, they could be posing as your supervisor or boss. Of course, you always do what the boss says--and that email sure looks like it came from his office. It even sounds like him! Unfortunately, that command from on high you see in your inbox is not really from the C-Suite. But it’s too late, you’ve been played. Preying on your fears, the phisher just tricked you into giving him the equivalent of your crown jewels such as online banking information.

This kind of crime is now more prevalent because of cloud-based computing. “The fact that email has moved to the cloud has changed the game considerably,” says Hiskey. Your data isn’t simply stored in a server in the privacy of your basement anymore. It’s sitting in the cloud, maybe in Dropbox, where any number of cyber anglers can insert their hooks. What’s more, Avanan says cyberthieves are often more knowledgeable than your company’s system administrator (and better paid), not to mention the fact that the entry code for so many things is now tied to your email address, something we all have. Your inbox is the proverbial weak link in the chain.

According to research conducted by Avanan, which specializes in protecting against phishing, one in every ninety-nine emails is a phishing attack. In a five-day work week, that amounts to almost one a day, per employee. What’s more, one in every twenty-five branded emails (the ones that look like they come from your bank) is phishing. These figures are based on the 55 million emails Avanan sifted through over a four-month period in 2018, determining which ones got caught by the cyber netting already put in place by cloud providers Microsoft and Google.

Of course, the cyberthieves are always one step ahead. There’s not just phishing, via email. Now there’s smishing, via texts. And vishing, via phone calls. Plus, angler-phishing, via social media. Practically every day, there’s a new fraudulent scheme; a so-called “zero day” attack, courtesy of ever-creative cyber villains. According to Starport’s co-founder and chief technology officer Brian Everest, these have “never been seen in the wild”, meaning they’re even new to cybersecurity experts.

Old fashioned grifters pointed snub-nosed revolvers at bank tellers or knew how to crack a safe. While crooks of the past also conned people, today’s robbers are full-fledged social engineers, using psychology to profit from our ever-so-human weaknesses.

"How can I design an attack in a way that feels natural to the person being attacked?" a hacker might ask himself. Hiskey says hackers "are evolving by getting way more patient," and are able to hide their tracks eerily well. Far too often, they get past the default online protection already constructed by Office 365 (in 30 percent of the cases, according to Avanan research). Hackers also target people at vulnerable times; on weekends, holidays, during natural disasters and periods when their guard is down. Take "Flo in accounting", for example, who clicks on a random email on her iPhone on a Saturday morning and logs in with her credentials (email and password), which opens the door and eventually allows the whole company's infrastructure to be exposed, copied and used against it.

Aside from financial services companies, the automotive and manufacturing sectors are high-value phishing targets for corporate espionage, often pinpointed by nation states looking for trade secrets. Universities are also particularly vulnerable. Email addresses ending in ".edu" are especially valuable because of their implied credibility and potentially lead to a trove of intellectual property.

Avanan's patented advantage, Hiskey says, is its invisibility, sitting behind existing security--it's there without you and the thieves knowing it. Most importantly, the company secures the cloud from within, capturing your email before it lands in your inbox, creating a perimeter of security so phishing emails never arrive. The software also scans all internal email before a criminal takes over an employee's email account. For the rare, nefarious email that slips through the protective sheath, Avanan's software then searches for it and destroys it along with any copies.

Meanwhile, in keeping with our times, artificial intelligence has become a crucial component of the company's toolbox. Avanan's software learns from past breaches and new threats, then uses that data to predict what might happen next. At present, there are some 300-plus phishing indicators (and growing) in emails, not apparent to users but visible to the company's software. It scrutinizes those hundreds of elements, scoring each email as either phishing, suspicious or clean.
According to the 2019 Verizon Data Breach

Investigations Report, C-Level executives were many times more likely to be targeted because they are higher impact, meaning closer to key information and money. The report also underlines the risk posed by mobile users who are more likely to click on phishing emails and therefore more susceptible to successful attacks.

Employers everywhere are now trying to educate their workers in cyber hygiene, because all it takes is one ill-advised click to corrupt an organization's network, and in a worst-case scenario, destroy the business. On average, it takes one minute and forty-seconds--the amount of time to read a phishing email. Then it's about another two minutes to make the fateful mistake of clicking on that dreaded link thereby allowing a nasty digital infection to spread throughout your company's computer system.

User education, while worthwhile, isn't enough. Tone comes from the top, as they say. Lots of executives don't want the hassle associated with protection, which by definition makes system access more difficult. Starport's co-founder and president David Poulson says many business leaders still see cybersecurity as an obstacle--a bother--even after they've been hacked. Astonishingly, some want their spam filters disabled so they don't miss emails, including ones that have been quarantined as high risk.

"We're trying to change the all-to-often laissez-faire attitudes of senior officials towards what should be seen as suspicious email," Poulson says. "We're trying to help people, at all levels, to protect against their biggest off-balance-sheet risk, the threat of cyber theft".

The mid-sized company--five-hundred or fewer employees--is particularly vulnerable because it doesn't view itself as a target. And Avanan executives argue that if companies are using the ever more popular Slack, they have crossed "the next frontier of phishing attacks." Cyber risk brings to mind the fate of Titanic. A sufficient number of lifeboats was viewed by the ship's owners as excessive, unnecessary ballast that would slow down the world's greatest ship and newest technology of the era. More than a century later, icebergs still pose threats to ships. But after such a preventable tragedy, vessels now carry lifeboats for everyone on board. In designing a shield against cyber theft, it's worth assessing whether your cloud infrastructure has the modern-day equivalent of enough lifeboats.

Howard Green is a Toronto based broadcaster, author and business journalist. He can be reached at: howardgreen.com