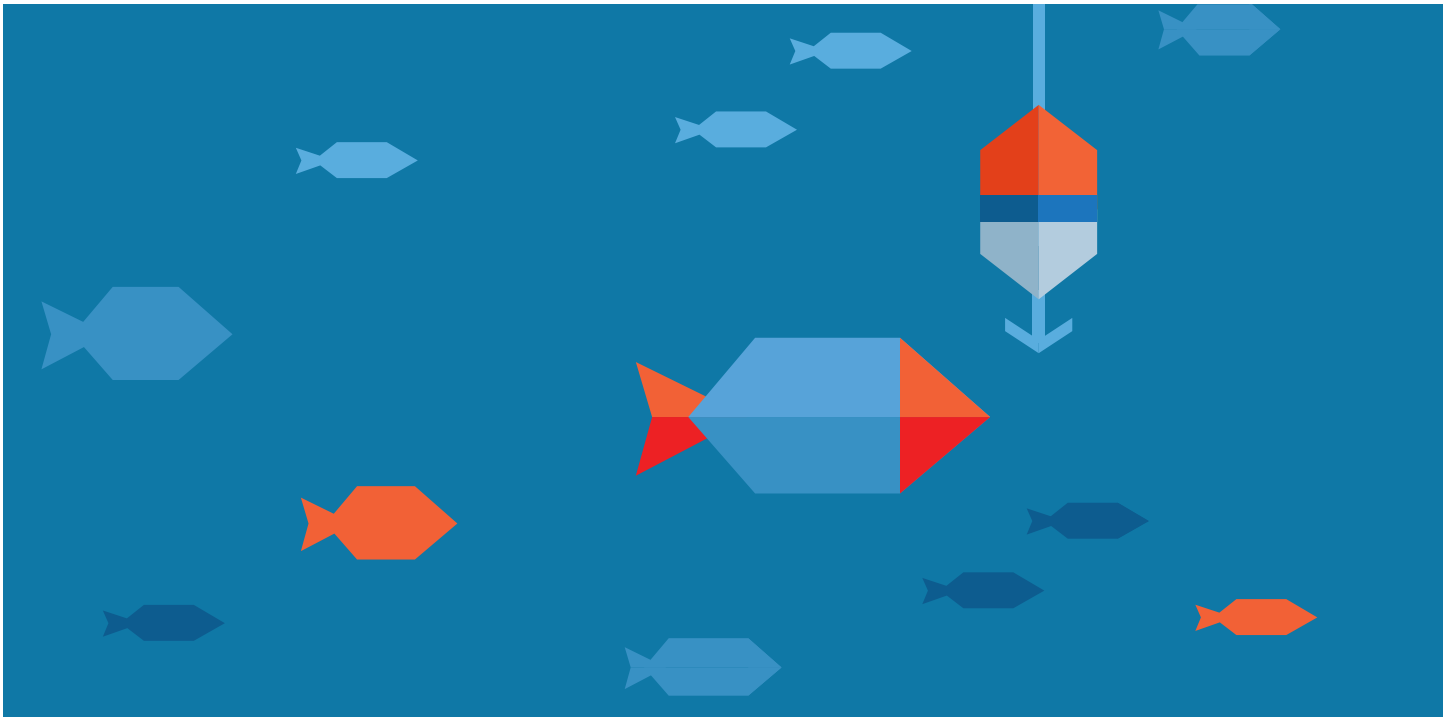

Don't Take the Bait

It's critical for firms to take steps to reduce phishing attacks.

MARK BREWER
Freelance Writer

A large global law firm with offices in more than 40 countries experienced a debilitating cyber attack in late June 2017. According to reports, the attack originated in the firm's Ukraine office, where an administrator clicked on a malicious link that brought the firm to its knees for at least three days.

While public evidence suggests that the attack did not result in the exposure of sensitive information, the firm sustained a significant business disruption and may have suffered reputational damage.

But how many law firms can withstand three days of technical chaos in a deadline-driven environment? An attack like this can deal a death blow unless the firm has considerable resources to remediate quickly and minimize disruption to operations.

THE RISKS ARE ENORMOUS

Malicious links are often packaged in phishing emails, which trick the reader into revealing login credentials or other confidential information, generally with the intent to create a misfortune the sender can profit from.

The risks are enormous. A successful phishing attack can cost firms precious cash in remediation or ransoms. Computer systems can be paralyzed for days or weeks. Secret,

"You need to have a solid perimeter and solid mitigation solutions and keep your systems up to date. The system you installed last year — unless it's a managed solution — is going to be out of date."

sensitive and personally identifiable information can be exposed — and the reputational risk can be severe.

Phishing attacks are soaring. According to the U.S. Office of the Director of National Intelligence, more than 100 million phishing emails are sent every day. About a third make it past default cybersecurity.

But clever criminals are staying a step ahead of prevention efforts. And law firms are juicy targets, housing a treasure trove of sensitive information while being perceived as lagging in security. Why target a major corporation when their law firm is easier to breach?

"Phishing has been going on a long time, but firms haven't prepared for it as much as they need to," says Eli Nussbaum, Managing Director at Keno Kozie Associates, a Chicago-based law firm technology consultancy. "Every day, a firm gets hit and they're learning the lesson. Eventually all firms will learn, but today, we're in a learning curve. The more I learn about security, it becomes a function of when, not if, it will happen. You need to be prepared for it."

LAW FIRMS ARE AT A DISADVANTAGE

Phishing scams continue for one good reason: They're successful enough for criminals to make huge profits. As protection evolves, so does the threat. "The bad guys are constantly evolving their attacks and are moving more quickly. They are even automating the process of stealing login credentials to start the process of getting into your email system in real time," says Nussbaum.

Phishing works by sidestepping protection technologies. With 100 million attacks daily, firms are statistically at a disadvantage. And it only takes one successful breach to open a big can of worms.

TAKING THE BAIT: WHAT MODERN PHISHING LOOKS LIKE

Phishing is not new, and many firm employees may think they understand it well enough to not take the bait. The reality is that nearly anyone, under the right circumstances, can be tricked. According to Verizon's 2017 data breach report, about one-third of phishing emails are opened.

All phishing runs on one simple idea — to trick the user into a response. Phishing is now more likely to be shaped by "social engineering," which is an approach that plays on people's good nature and business need to be helpful and responsive in order to trick them into bypassing normal security procedures. It's a practice designed to deceive the most vigilant users with emails that are generally urgent in nature, requesting immediate information or action. The idea is to get the user to act now and think later.

The most successful attacks look like emails the recipient is expecting. This type of attack, known as spear phishing, blends in with email traffic. They tend to send legitimate-looking emails that appear to come from partners or clients, often with detailed instructions to wire a large sum of money.

Cybercriminals can pull this off because they're already in the target firm's email system reviewing privileged conversations and looking for a ripe opportunity to make a play.

"With the right technology in place, firms can further advance their cause by having and enforcing data retention and destruction policies to prevent the stockpiling of sensitive information that is not being used."

KEEP YOUR PROTECTION SOFTWARE UPDATED

Cyberattacks are perceived as requiring a cyber solution. Certainly, technology plays a necessary role in protection. "You need to have a solid perimeter and solid mitigation solutions and keep your systems up to date. The system you installed last year — unless it's a managed solution — is going to be out of date," Nussbaum says.

Antivirus and antimalware tools are a must. Advanced malware protection that uses artificial intelligence to keep up with threats can help narrow the gap between known and

"Phishing should be discussed frequently. People don't learn unless they're reminded. Rinse and repeat. Don't let them get too far away from it before you remind them again because they will forget. You constantly need to keep it top of mind."

emerging threats. But these tools are only as good as the last update or, for advanced tools, the latest attack.

With the right technology in place, firms can further advance their cause by having and enforcing data retention and destruction policies to prevent the stockpiling of sensitive information that is not being used. Also important are clear procedures for handling requests for sensitive information or large financial transactions.

BUILDING AWARENESS IS KEY

But experts say that user education is the most important part of reducing phishing attacks in law firms. Nussbaum suggests starting with annual training for user awareness. If firm employees and partners know what a risky email looks like, they will be less likely to take the bait and suffer the embarrassment of being the gateway to a breach. Many companies offer online training programs.

Secondly, Nussbaum says, "Phishing should be discussed frequently. People don't learn unless they're reminded. Rinse and repeat. Don't let them get too far away from it before you remind them again because they will forget. You constantly need to keep it top of mind."

One technique for staying top of mind is simulated phishing campaigns. Sometimes called ethical phishing, these campaigns send random test emails to users to see who clicks through. Small campaigns can be run throughout the year, with the simulated emails becoming progressively advanced. You can also run a phishing campaign before an educational effort to get a baseline on how susceptible your firm is to an attack.

Several companies offer simulated phishing campaigns, including KnowBe4 and Trend Micro. Simulated phishing campaigns are relatively inexpensive, costing tens of dollars per user per year.

A more involved technique is tabletop exercises where key firm security stakeholders run a simulated attack to go through the response process. This helps prevent attacks because the simulation can reveal obvious gaps in technology and processes, as well as aiding in preparing a successful response to an attack.

Firms can't avoid phishing attacks. But given the risks, they can take concrete steps with technology, processes and user awareness to mitigate that risk. Even with the best protection, a firm can still fall victim. Being prepared with a sound response to an attack will ease the impact on the firm's ability to continue doing business — and help preserve the firm's reputation. ■

ABOUT THE AUTHOR

Mark Brewer is a freelance writer who helps decision makers understand technology, trends and ideas to make them more effective in their work.

mark@markbrewerwriter.com

markbrewerwriter.com