MetaCompliance®

FIND THE PHISH: HOW ANTI-PHISHING TRAINING SOFTWARE CAN GET YOU OFF THE HOOK

PREV PAGE

NEXT PAGE

How Anti-Phishing Training Software Can Get You Off the Hook

Table of Contents

PREV PAGE

NEXT PAGE

How Anti-Phishing Training Software Can Get You Off the Hook

Introduction:

Email is critical to nearly every business in today's interconnected world. It is how employees update directors on their day-to-day tasks, how account managers communicate with clients and submit invoices, and how supply chain logistics personnel pass on intellectual property, sensitive plans, and/or confidential designs that help ensure a business advantage. In more ways than one, email holds a business together.

Unfortunately, attackers understand how important email is to businesses, and they know how it makes companies vulnerable. Furthermore, they realize they can exploit that fallibility to breach not only a target company but also larger customers with which it does business. All it takes is one successful phish, and they're in.

No organization is safe from a phishing attack. That is why every business, from the SMB to the large enterprise, has an incentive to invest in anti-phishing training software. The vigilance of their employees and the security of their customers, both large and small, depend upon it.

PREV PAGE

NEXT PAGE

How Anti-Phishing Training Software Can Get You Off the Hook

What Is a Phishing Email?

In its report The Evolution of Phishing Attacks: 2011-2013, Kaspersky Lab defines a phishing email as an attack by which malicious actors use social engineering techniques to lure users into visiting a fake website where they can collect information about them.

Here it is important to differentiate hacking from social engineering. The former relies on the technical expertise of the actor to exploit vulnerabilities they find in a target system's technology. Hacking attempts require little to no input from any person besides the hacker, who can develop scripts and other programs to automate the cracking process.

By contrast, social engineering requires little to no technical expertise. It hinges instead on an actor's ability to trick a target user into performing some action that they ordinarily would not perform. As such, in phishing attacks, not to mention other schemes based on social engineering techniques, an attacker exploits another person's human weakness.

Daniel Magana, IT Security Analyst at Tripwire, has identified three parts to every phishing attack. These are as follows:

1. Request for personal information
2. Bad/Forged links
3. Sense of urgency or fear

As an example, an attacker crafts a phishing email warning the recipient that their bank account is about to be closed (urgency). The email provides a URL that the user can click on to prevent their account from deactivating (links). The URL leads to a fake sign-in page that looks similar to the actual login page of the bank where the recipient has an account. When the user enters their username and password, the information is sent to the attacker, thereby giving them full access to the victim's bank records (request for personal information).

Technically, phishing pages can prompt users for as much information at the attacker wants. But they must do so carefully, as asking for too much data or unusual pieces of information could make victims suspicious.

A Phish and Its Plentiful Purposes

Tricking people into handing over their login credentials and other personal information can serve a number of purposes.

First, a phishing attack might be an end in itself. Once a bad actor has successfully obtained access to a victim's information, they may use it to their benefit--and to a victim's detriment. For instance, an attacker could abuse a user's social media login credentials to write a number of disparaging posts that damage their personal brand or their company's reputation. If the information is financial in nature, the actor could empty the victim's bank account or abuse a compromised payment card to make fraudulent purchases.

Second, a phisher could sell the information. This is especially true in attack campaigns that ask users about their medical history, pieces of data which are worth 10 times more than your credit card details on underground web markets. Buyers can in turn use that information to fraudulently bill victims for medical procedures they never received, target them with scam emails offering fake pharmaceutical drugs at "cheap" prices, and much more.

Third, a phishing attack could conceal an even greater threat. More and more phishers are no longer interested in collecting users' credentials outright. Instead they attempt to lure users into visiting a website or clicking on an attachment that, in turn, downloads malware onto the victim's machine. Once the malware is downloaded, attackers can log all keystrokes and attempt to expose additional data sources. If they find themselves in an organization's IT systems, they could also attempt to hack their way laterally across the corporate network, compromising additional machines and processes as they go.

Attackers can clearly do a lot with a phishing email. This flexibility helps to explain why different groups, from taxpayers to Russian banks, from government employees to WhatsApp users, have all been targeted in separate attack campaigns.

PREV PAGE

NEXT PAGE

How Anti-Phishing Training Software Can Get You Off the Hook

Target and the Big Catch

Phishing emails endanger all businesses, but they do so unequally. The threat level of a phishing campaign depends upon a number of factors. These include a company's sector, its size, and the services of other businesses on which it depends.

With that in mind, large enterprises might ultimately be the most vulnerable to phishing campaigns. These types of organizations maintain business partnerships with a variety of vendors/third parties that might have access to their customers' networks depending on the services they provide. If that is the case, attackers could focus their energy on phishing the smaller companies as a means of breaching their larger customers.

The best example of this type of phishing attack is the Target breach. In 2013, attackers compromised the financial information of some 40 million credit and debit card holders, not to mention another 30 million customers' personal information, after they uploaded malware to the retailer's point-of-sale (PoS) systems. They did not breach Target's network, however. They logged on with a verified set of credentials they obtained from Fazio Mechanical Services, a company that specializes in providing refrigeration and HVAC systems for companies like Target. It is believed the attackers gained access to an authorized set of credentials via a phishing email, which they then abused to expose the payment card details at one of the largest retailers in the United States.

After accounting for the coverage offered under its data breach insurance policy, the 2013 breach cost Target approximately $162 million. These damages are considerably less than the retailer's initial estimates. However, rebuilding one's reputation and customer loyalty after a data breach can take years. No company wants to endure that lengthy recovery process.

PREV PAGE

NEXT PAGE

How Anti-Phishing Training Software Can Get You Off the Hook

Empowering the User

A company's susceptibility to phishing attacks boils down to its employees' security awareness. It's not that you can protect against every phishing email that gets through your defenses. It's more that you need to build up your organizational "smarts" so that your staff can avoid the more obvious phishing scams and think twice before opening a suspicions email.

Unfortunately, the reality is that many workers still cannot spot a phish.

To illustrate, in the 2016 Verizon Data Breach Investigations Report, researchers observed that nearly a third (30 percent) of people opened phishing messages across all industries. Additionally, more than a tenth of users (12 percent) clicked on attachments sent to them from suspicious sources.

These click ratios in part reflect the evolution of phishing attacks. Better graphics, professional email templates, and the use of proper English all make a phishing scam appear more genuine and therefore harder to spot. Many phishing attempts also incorporate trending topics, such as the disappearance of Malaysia Airlines flight MH370 and the Zika virus, to prey on people's curiosity and trick them into clicking before they have time to think.

Given how sophisticated phishing attacks have become, it is up to employers to ensure their employees have the necessary security awareness training to resist email scams. That is why anti-phishing training software such as MetaPhish is so useful. Employers need a solution that can test employees' susceptibility to inbound phishing attacks on an ongoing basis. Designing one's own phishing simulations could take up a lot of time and resources. By contrast, MetaPhish comes already equipped with a range of email templates, each of which can be matched to domain names relevant to an organization.

The solution also records whenever an employee clicks on a phishing link. Companies can therefore pair this knowledge with other user awareness content such as a good quality phishing eLearning course to provide employees with the right knowledge before each simulation. In this regard, MetaPhish not only teaches anti-phishing skills; it helps to build a dynamic security culture that is well versed in phishers' latest tricks.

PREV PAGE

NEXT PAGE

How Anti-Phishing Training Software Can Get You Off the Hook

Conclusion

Phishing emails threaten every organization, and unfortunately, it takes just one employee to expose an entire enterprise to malware or to a breach. That is why your employees' ability to spot a phishing scam is so important. And it all starts with improved user awareness.

PREV PAGE

FIND THE PHISH. Learn how MetaCompliance's solutions can enhance your employees' anti-phishing training and see how vulnerable your organisation is to a phishing attack?

NEXT PAGE