How to Keep Employees Safe from Phishing Scams
INTRODUCTION

What is Phishing?
Phishing is a social engineering technique cybercriminals use to trick an unsuspecting victim into:

- Clicking a link that installs malicious software
- Giving up sensitive, and sometimes personal, information

Since 2015, cybercriminals and hackers have relied on these types of scams as their primary exploit for bypassing cybersecurity. These techniques, rather than relying on coding prowess or technical knowledge, use deception and human gullibility to penetrate otherwise secure networks.

While cybercriminals and hackers use many kinds of scams and attacks—such as denial-of-service (DoS) and ransomware—to steal information, phishing is perhaps the most prevalent. And with the right strategies in place, it’s also one of the most preventable.

The Prevalence of Phishing Attacks
In its 2016 Data Breach Investigations Report, Verizon reported that 30 percent of phishing emails were opened by the target, who did so within an average of one minute and 40 seconds. Of even greater concern, 12 percent of users clicked on the malicious attachment or link that the email contained, doing so within three minutes and 45 seconds on average.

Additionally, in its 2017 Data Breach Investigations Report, Verizon looked at how many users fell victim to phishing more than once within a year’s time and discovered that in a typical company, with 30 or more employees, about 15 percent of users who fell victim once would also fall victim a second time.

Corporate email users are frequently the target of these schemes, and in the second quarter of 2016, the Anti-Phishing Working Group tracked over 400 brands that were targeted for phishing schemes each month. During this same time period, software security firm Kaspersky Lab reported that 8.7 percent of its user base received a phishing email of some kind.

In this whitepaper, we are going review the main types of phishing scams cybercriminals use, outline tips for recognizing a phishing email, and look at strategies your organization can implement to keep employees from falling victim to these scams.
# 5 Types of Phishing Schemes

## 1. Deceptive Phishing

The most common type, deceptive or “traditional” phishing, is primarily done through email. The messages routinely rely on a sense of urgency, highlighting the consequences of inaction, such as a suspended account or deleted information.

Previously, the links contained in these emails focused on directing users to phony sites that were intended on capturing user information—particularly usernames and passwords. However, more frequently these messages contain either attachments or links intended to install persistent malware or ransomware.

## 2. Spear Phishing

These types of schemes are more customized and personalized to the target user. The sender may rely on profile data from social media platforms, such as LinkedIn, to obtain the target’s name, position, responsibilities, or other pertinent information.

With more data available, these scams can more easily create a false sense of connection, such as a message pretending to be sent from a business partner or subsidiary.

## 3. Whaling

Much like spear phishing schemes, these scams are highly targeted; however, the focus is on CEOs and other senior executives. High-ranking personnel are sometimes more susceptible to these efforts as they routinely do not participate in security awareness training with other employees.

If the first phase of a whaling attempt is successful, scammers will take advantage of the executive’s credentials to engage in larger fraud, such as authorizing wire transfers from the compromised email account.

## 4. Angler Phishing

With so many users active on social media platforms, criminals have begun to create fake customer service accounts for popular brands, such as national banks or retailers, using these accounts to direct consumers to phishing websites or to gain access to personal information.

Given that communication on these platforms is nowhere near as secure or monitored as email, fraudsters can bypass most security tools with this strategy.

## 5. Pharming

These efforts are not targeted at your business directly, instead they attack the domain name systems (DNS) that comprise the backbone of the internet. Via one of these attacks, the scammers can redirect legitimate web traffic to a malicious website that displays the appropriate website address.
HOW TO IDENTIFY A PHISHING ATTEMPT

To help protect against phishing attacks, it’s important that employees know what to look for when they receive a suspicious or unsolicited email. A phishing attempt will typically...

Be Poorly Written

Most communication that comes from a government office or professional business will have passed through the hands of an editor or legal department, where someone would have reviewed spelling and grammar.

By contrast, most phishing attempts originate from overseas, where English is not the primary language, so frequent spelling and grammar mistakes within an email—particularly one requesting information or financial payments—should be suspect.

Ask for Personal Information

If a message asks you to provide your personal identification information or general account information, you should be suspect. Any partner, supplier, or vendor that interacts with your business should already have any needed information (including account and routing numbers) on file. Similarly, no legitimate business or IT department will need your employees to send their login and password information in an email or social media message.

Contain a Mismatched Web Address

A common technique scammers use is to embed a web link in an email that appears to be legitimate but that actually leads to a harmful site. For example, the text of the link will read: legitcompany.com. However, when you click the link, it will direct you to scammersparadise.com instead.

An easy way to tell if a URL is legitimate is to hover your mouse over the link without clicking it. Most email programs will notify you either via a popup or at the bottom of the screen what the actual target of the URL is. If these do not match, you likely have a phishing email.

Use Misleading URLs

Another trick hackers commonly use to take advantage of how little attention most people pay to URLs is to insert additional information. For example, login.legitcompany.com is a URL that takes you to the real company that your business works with. However, login.legitcompany.com.scammersparadise.com directs you to a fake site that’s intended to steal your login information.

The key is to successfully identifying the scam is to look at the text immediately to the left of the “.com” (or .org, .edu, etc.). That text will disclose the site that the link actually leads to.
Critical thought is one of the primary enemies of a social engineering attack, so most criminals will place strict time limits in their phishing messages.

Have a Sense of Urgency
Critical thought is one of the primary enemies of a social engineering attack, so most criminals will place strict time limits in their phishing messages. The missive will either threaten a penalty—such as shutting down an account or levying a fine—or offer a limited time reward that the recipient needs to act on immediately before you have time to think.

BEST PRACTICES FOR BLOCKING PHISHING ATTACKS

Employ Technology
Your first line of defense should be an email filtering system that accounts for known tricks, like email spoofing. Consider two-factor authentication procedures for high-target systems, and segment your network to limit further access if an account or user has been compromised. Actively monitor your network for signs of suspicious activity or data exfiltration to cut down response times.

Offer Security Awareness Training
No matter how complicated your email monitoring systems may be, your business will still be vulnerable to phishing attacks because hackers do not target your IT systems—they target your employees.

Phishing scams rely on strategies to trick your employees into trusting fraudulent sources, and the only true means to combat these attacks is to create a savvy, well-educated workforce. To do this, you need to provide all your employees, even key executives, with regular security awareness training. You should also provide staff with a mechanism for reporting suspicious emails, and make sure that they know how to escalate a potential threat. Of the 636,000 phishing emails identified in the 2016 Verizon study mentioned earlier, only an approximate 3 percent of recipients alerted management of a potential phishing attempt.

Create Policy
As previously mentioned, executives are frequently the targets of phishing schemes, and if the account of one of these key decision makers can be compromised by scammers, your business could quickly become the victim of full-blown fraud.
To limit the damage caused by a successful phishing attempt, put in place stringent policies that limit how payments and other financial transfers are authorized, particularly for new vendors or other recipients.

Consider requiring additional confirmation beyond a simple email, such as a corresponding phone call from the responsible party. With such a strategy in place, criminals won’t be able to convince your accounting department to send them extravagant payments, even if they are sending “legitimate” emails from the compromised account of the CEO.

**Test for Weakness**

Send “false phishing” emails to staff—including senior leadership—to identify how effective existing training programs are and if any potential gaps exist in employee understanding.

When you combine false phishing tests with your training program, you can provide your employees with a lasting, real-world example that will likely reinforce cybersecurity concepts better than any learning session will on its own.

**CONCLUSION**

When it comes to gaining access to your company’s data, a simple phishing email may be the most effective attack. Cybercriminals are constantly thinking up new techniques to fool your monitoring software and employees. In response, your business needs to be equally diligent in preparing your staff to identify potential security risks, whether through email or some other avenue.

Unsurprisingly, education is key, and a sound training program coupled with effective communication policies can empower your workforce to play a critical role in company cybersecurity.
ABOUT WORKPLACE ANSWERS, AN EVERFI COMPANY

Since 1997, Workplace Answers (WPA) has helped companies across the globe foster ethical, inclusive and secure workplaces with online compliance training. With the launch of Campus Answers to serve the higher education market, and the acquisition of Click 4 Compliance to provide the most comprehensive and engaging online compliance training library to companies across the globe, Workplace Answers has expanded its training offerings to reach new audiences.

In 2017, EVERFI announced its acquisition of Workplace Answers to become the world’s largest company committed to empowering learners at every stage of their lives, from the classroom to the boardroom. As part of the EVERFI Network, Workplace Answers has the opportunity to continue its legacy of solving compliance challenges with the best-in-class online compliance training, subject matter expertise, and client support—now with even more reach.

REFERENCES


