PHISHING AND SPEARPHISHING: AN IT PRO'S GUIDE

By James Sanders

TechRepublic

INTRODUCTION

While security professionals focus largely on identifying and patching vulnerabilities in software, the weakest security link is typically end users. Phishing is a social engineering method to fraudulently obtain information by disguising communication as being from a trusted source; the information can then be used to access devices or networks. Spearphishing is a targeted phishing attack that relies on the use of personal information to make the attack look more trustworthy. This guide offers an introduction to the social engineering attack.

WHAT IS THE DIFFERENCE BETWEEN PHISHING AND SPEARPHISHING?

Phishing is a social engineering method to fraudulently obtain information, which can then be used to access devices or networks. This type of attack uses technology to disguise communication or web pages as being from a trusted source. Fundamentally, phishing attacks rely on confidence tricks as much as technological trickery to achieve its aims.

In contrast, spearphishing is a phishing attack targeted to a specific individual or company. These attacks usually rely on tailored methods and resources, such as attempting to clone the login interface for corporate intranets, as well as using personal information gathered in advance (perhaps from a prior breach) about targets to increase the likelihood of success. Spearphishing attacks conducted against senior executives are referred to as whaling.

The whaling formula is also reversed as "CEO fraud," in which phishing emails are disguised as originating from the CEO. According to Colin Bastable, CEO of security training company Lucy Security, "These socially engineered attacks are devastating because the spoof emails have all the appearances of being real, and the victims voluntarily hand over the money. Why would the insurance company cover the loss? Targets are identified, groomed, and then deceived by quite sophisticated email techniques into wiring funds to 'burner' bank accounts, often in Asia, which are then emptied. Thinking that the email request comes from the CEO, the victim willingly sends the money. SMBs are particularly vulnerable, as they have short lines of communication, with fewer checks and balances, between finance staff and the CEO."

Additional resources

- The challenges with preventing phishing attacks: An insider's perspective (TechRepublic)
- What is phishing? Everything you need to know to protect yourself from scam emails and more (ZDNet)
- This phishing scam group built a list of 50,000 execs to target (ZDNet)
- Video: How to solve the human challenges of cybersecurity (TechRepublic)
- Why we might see more spam and phishing post-GDPR (TechRepublic)

WHAT TYPES OF PHISHING ATTACKS EXIST?

Malicious actors typically employ a variety of phishing techniques in their attacks:

Deceptive linking

The most frequently used—and most reliable strategy for attackers—is to disguise a malicious link as pointing to a legitimate or trusted source. These types of phishing attacks can take any number of forms, such as exploiting misspelled URLs, creating a subdomain for a malicious website, or using confusingly similar domains.

For examples of those three strategies, consider the following: The letter I is very close to L on standard QWERTY keyboards, which would make "googie" a plausible stand-in for "google." For subdomains, an attacker controlling example.com could create subdomains for that domain (e.g., "www.paypal.example.com,") for which the start of that URL appears legitimate. For confusingly similar domains, the domain "accounts-google.com" was registered as a clone of "accounts.google.com" in a phishing attack during the 2016 US presidential election.

International Domain Names (IDNs) can also be used to create confusingly similar looking domain names by allowing the use of non-ASCII characters. Visual similarities between characters in different scripts, called homoglyphs, can be used to create domain names with visually indiscernible differences, fooling users into believing that one domain is actually another.

Website cloning, forgery, and covert redirecting

Websites vulnerable to cross-site scripting (XSS) attacks can be used by malicious actors to inject their own content onto the actual website of the service being attacked. XSS can be used to harvest data entered on a compromised website (including username/password fields) for the attackers to use at a later date.

Some phishing attacks use XSS to create pop-ups, which originate from a vulnerable website but load a page controlled by the attackers. Often, this type of covert redirect loads a login form to harvest login credentials. As a result of the prevalence of this type of attack, most browsers now display the address bar in pop-up windows.

Voice and text phishing

Malicious actors also rely on phone calls and text messages to harvest account information, with texts sent to banking customers claiming their account access is disabled and prompting users to call a phone number or use a website set up by attackers, from which account information can be harvested.

Additional resources

- Phishing warning: If you work in this one industry you're more likely to be a target (ZDNet)
- How one hacked laptop led to an entire network being compromised (ZDNet)
- Why botnets, ransomware, and phishing attacks are the biggest cyberthreats to your business (TechRepublic)
- Hackers target Japanese academics with phishing campaign to steal research data (TechRepublic)
- Cybersecurity and cyberwar: More must-read coverage (TechRepublic on Flipboard)

WHY SHOULD I BE CONCERNED ABOUT PHISHING?

Fundamentally, phishing affects everyone. Malicious actors usually cast a wide net when using phishing attacks, hoping to catch any arbitrary victim to gain access to personal banking information or a port of entry into a corporate network, from which attackers can potentially retrieve sensitive information. Even with policies ensuring segmented access to information, this may still put information about employees, clients, and customers at risk.

Security monitoring solutions are designed primarily to alert users or IT professionals to the existence of a virus based on data such as hashes of known payloads or programmatic behaviors of viruses. This model of security software adapts poorly to phishing attacks that rely extensively on social engineering methods to convince users to take action immediately without analyzing a situation. Because of this, the best defense against phishing is security training for end users.

Filters have been developed in an attempt to identify phishing attacks in emails, though some phishing emails use images of text in place of written text to evade these mail filters. Likewise, phishing websites frequently rely on code obfuscation techniques to prevent security software from detecting malicious activity. Often, phishing attacks rely on AES-256 or Base64 encoding inside JavaScript, or custom encoding strategies, making it difficult to analyze the underlying source code. (The use of code obfuscation itself can't be flagged as malicious intent.)

Researchers at Proofpoint recently disclosed a phishing toolkit that obfuscates data by use of a substitution cipher that relies on a custom font to decode. This toolkit uses a customized version of the Arial font with individual letters transposed. When a phishing page is loaded, the content looks normal. When a user or program attempts to read the source, the text on the page appears jumbled.

Additional resources

- How one man's phishing scam cost two major US tech companies $100M (TechRepublic)
- Phishing attacks: Why is email still such an easy target for hackers? (ZDNet)
- Don't skimp on IT security training: 27% of employees fall prey to phishing attacks (TechRepublic)
- Individualism may make you better at catching a phish: Research (ZDNet)
- Google: Our hunt for hackers reveals phishing is far deadlier than data breaches (ZDNet)

HOW LONG HAS PHISHING BEEN A THREAT?

The concept of phishing was first discussed in 1987 in a paper presented at Interex titled "System Security: A Hacker's Perspective." From an etymology standpoint, the first recorded appearance of the word "phishing" was in a hacking tool called AOHell, in 1996.

The earliest known phishing attempts targeting financial services were in 2001 and were against the "digital gold currency" service E-gold. By October 2003, attackers had targeted Bank of America, CitiBank, PayPal, Lloyd's of London, and Barclays.

According to the Anti-Phishing Working Group, the number of unique phishing reports the organization received in 2005 totaled 173,063, with that number expanding to an all-time high of 1,413,978 in 2015. Since then, phishing attacks have modestly decreased in frequency, with 1,122,156 received in 2017.

Additional resources

- The biggest phishing attacks of 2018 and how companies can prevent it in 2019 (TechRepublic)
- Video: why hackers use phishing attacks on political campaigns (CBS News)
- Attackers are using cloud services to mask attack origin and build false trust (TechRepublic)
- Why organizations aren't succeeding in threat hunting strategies (TechRepublic)

HOW CAN I PROTECT MY ORGANIZATION AGAINST PHISHING ATTACKS?

There are a variety of strategies to safeguard against phishing attacks, though multiple strategies should be used together to avoid a single point of failure.

Because phishing attacks are fundamentally a technological means to a social engineering exploit, user training is the most important strategy for your organization. Training users to spot identifying characteristics of

phishing emails, and running simulated phishing attempts to target the efficacy of that training, will do more to ensure security integrity than software solutions can.

Establishing policies to protect against employees unwittingly transferring funds or providing data access for non-legitimate purposes is similarly important. Bastable noted, "All security starts with a policy—businesses should have an agreed policy for such situations, and they should train their staff accordingly. CEOs should hire strong people who are willing to stick to the policy under pressure. Of course, defying the CEO is a great way to get fired in American business, and the cybercrooks rely on this."

For technological solutions, changing the default behavior in email clients such as Microsoft Outlook can improve security. Third-party scanning tools can reduce the efficacy of phishing attacks or prevent them from reaching users' inboxes.

Modern browsers also include Safe Browsing filter services, which are enabled by default. The services detect phishing attacks and prevent users from falling victim.

Additional resources

- 3 ways to protect your employees' inboxes from phishing threats (TechRepublic)
- 10 tips to combat phishing via social media platforms (TechRepublic)
- The top 11 phishing email subject lines SMBs should look out for (TechRepublic)
- How to set up a rule in Microsoft Exchange to send an alert of a phishing attack (TechRepublic)
- Here are the 'most clicked' phishing email templates that trick victims (TechRepublic)
- Cheat sheet: How to become a cybersecurity pro (TechRepublic)

CREDITS

Senior Director, B2B Editorial
Jason Hiner

Editor in Chief, UK
Steve Ranger

Senior Managing Editor
Bill Detwiler

Associate Managing Editor
Mary Weilage

Senior Editor
Alison DeNisco Rayome

Editor, Australia
Chris Duckett

Senior Features Editor
Jody Gilbert

Senior Writer
Teena Maddox

Chief Reporter
Nick Heath

Staff Writer
Macy Bayern

Associate Editor
Melanie Wachsman

Multimedia Producer
Derek Poore

Cover image:
iStock/faithiecannoise

TechRepublic

ABOUT TECHREPUBLIC

TechRepublic is a digital publication and online community that empowers the people of business and technology. It provides analysis, tips, best practices, and case studies aimed at helping leaders make better decisions about technology.

DISCLAIMER

The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.