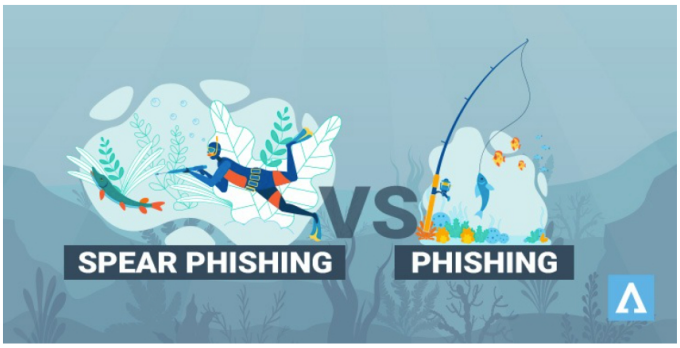

7
Jan

Phishing

Spear Phishing vs. Phishing: Everything You Need to Know

Spear phishing occurs when cyber criminals deploy targeted attacks against individuals and businesses alike via email. Using savvy tactics, hackers collect sensitive data about specific parties to construct messages that sound familiar and trustworthy.

As its name implies, spear phishing falls under the larger umbrella category of phishing attacks that victimize end users and organizations daily. What's the difference between the two kinds of scams? And how can individuals and enterprises alike safeguard their most important data from both types of threats?

This blog post will outline the significant differences between spear phishing and phishing, as well as some practical tips to protect your data from these kinds of cyber attacks.

Spear Phishing vs. Phishing: What's the Difference?

The biggest difference between spear phishing and phishing lies in the approach used by cyber criminals to carry out malicious activity.

Spear phishing is targeted and personalized to a specific individual, group, or organization. Conversely, regular phishing emails use a broad-strokes approach that involves sending bulk emails to massive lists of unsuspecting contacts. These phishing messages are often quickly crafted and don't usually include personal information about the recipient.

Because of their hyper-targeted nature, spear phishing can be even more dangerous than traditional phishing. The familiar tone and content of a spear phishing message make it more difficult for the average user to detect, heightening the threat level of this type of cyber attack.

Understanding And Avoiding Spear Phishing and Phishing Attacks

Since they aren't personal (and bad grammar can be a giveaway), bulk phishing messages are routinely identified by end users and quickly deleted. That said, it's also true that many less attentive individuals are still prone to clicking on phishing email attachments or links or not verifying a sender's address before replying.

For that reason, security awareness training and phishing simulations are essential to teach and reinforce key concepts related to detecting and avoiding phishing threats.

As a cyber threat, spear phishing is much more sophisticated and refined than the "spray and pray" technique of bulk email phishing. Cyber criminals succeed with this type of targeted attack because, at their core, spear phishing messages seem believable due to the inclusion of personalized information about the target, like contact details, hobbies, or interests.

In addition, spear phishing emails are more convincingly written than regular phishing emails. The message's content is positioned as coming from someone the recipient knows or trusts. As a result, the use of an urgent tone is much harder to resist, and the victim will be tempted to take action, whether that means preventing a large loss, legal charge, or account shutdown.

These well-written messages often include links to fake websites or attachments infected with malware, ransomware, or spyware. In some cases, there are no attachments or malicious links at all but contain instructions for the recipient to follow, making them even more challenging to spot with email security filters.

The Growing Threat of Spear Phishing Attacks

Spear phishing's detection difficulty level, coupled with the rise of remote workforces and weakened technical precautions, has led to it becoming a tool of choice for cyber criminals worldwide.

Recent data has painted spear phishing as a rapidly growing threat to individuals and organizations alike. In 2019, before the extra challenges brought about by the COVID-19 pandemic, 65% of attack groups were already using spear phishing as their primary infection vector.

On top of that, a whopping 95% of all enterprise network breaches are the result of successful spear phishing.

For the unsuspecting individual, a spear phishing attack may involve an email that appears to come

Search

Search...

Categories

Compliance and Governance (9)
Cyber Security Awareness (298)
Data Privacy Awareness (57)
Events (11)
GDPR (9)
News (25)
Phishing (91)

Recent Posts

What is Baiting in Cyber Security?
7 Smishing Examples and How to Protect Yourself
What is Swatting? What to Look for and How to Defend Yourself
The 2023 Gone Phishing Tournament Results: Everything You Need to Know
Protect your loved ones from phishing, social engineering and other cyber attacks

Tags

byod CISO Communication tools Covid-19 Scams credential stuffing attacks Cyber Security Awareness cyber security professional Data breaches Data Privacy End user engagement gartner magic quadrant GDPR Training governance Human Risk Information security awareness Information security program Ilse Iapointe malware National Cyber Security Awareness Month NCSAM Password phishing Phishing scams phishing simulation ransomware Remote working Security Awareness Framework Security Awareness Training social engineering Social Networks Work from home

from the person's bank or a reputable business such as Amazon. The message may appear to be a shipping notice or transaction confirmation request that entices the reader to click a malicious link or respond with confidential personal information.

Cyber criminals also attack businesses in this fashion, often targeting a couple of employees at a given company. A legitimate-looking email may be sent to those users, appearing to come from their manager or a company executive, directing them to transfer money, reveal a password, or provide confidential company information.

In both cases, a spear phishing email typically has an air of urgency. It gives victims the impression that they will bear the brunt of severe consequences if immediate action isn't taken.

7 Ways to Protect Your Organization Against Spear Phishing

While the danger of spear phishing is real and complex, there are several ways organizations can easily limit the risk associated with this cyber threat.

1. **Educate, educate, educate.** Avoiding the negative impacts of a successful phishing attack starts with effective education. Educate employees about spear phishing and take advantage of free phishing simulation tools to help them consistently identify threats.
2. **Use proven security awareness training programs.** Go beyond freely available tools and use proven security awareness training and phishing simulation solutions to keep spear phishing and related threats top-of-mind across the workplace. Also, ensure that your training is accessible to all users and be consumed in various formats (in other words, long, boring training videos don't have to be your only option).
3. **Monitor and measure results.** Empower and remind the security leaders and your organization's program ambassadors to monitor employee spear phishing awareness with phishing simulation tools. Make sure your programs are supporting long-term cyber security goals and adjust where necessary.
4. **Spread the right word.** Launch an organizational awareness campaign that provides ongoing communication about cyber security, spear phishing, and social engineering. This includes establishing strong password policies and reminding employees about the risks that can come in the format of attachments, emails, and URLs.
5. **Limit access to sensitive information.** In today's BYOD (bring your own device) era, it's essential to establish network access rules that limit the use of personal devices and the sharing of information outside of your corporate network.
6. **Keep software updated and current.** Ensure that all applications, internal software, network tools, and operating systems are up-to-date and secure. Install malware protection and anti-spam software.
7. **Create a security-centric culture.** Incorporate policies and procedures, best practices, executive security awareness, change management, and support into your corporate culture.

At the end of the day, while there are fundamental differences between spear phishing and regular phishing, the solution to both shares some common elements.

Security awareness training programs that give employees the knowledge and skills they need to protect personal and organizational data are an absolute must, particularly as cyber threats become more and more complex.

However, phishing simulations are a vital component of any successful security awareness initiative. These practical exercises are crucial because they allow users to safely navigate scenarios they may encounter in the real world.

Ultimately, implementing the right type of security awareness training—one supported by phishing simulations—helps any individual or organization build an effective defense against spear phishing. However, it's important to know what that right type of training program is regarding your unique cyber security needs and goals.

Share:

Newer
What is the Dark Web: Learn How to Keep Your Information and Identity Protected

Older
How To Build a Strong Security Awareness Program in 2021

Phishing Simulation
Cyber Games

GET STARTED

Free Demo
Request a Quote
Phishing Simulation Trial

STAY CONNECTED

Customer Support
Cybersafe and Sound Newsletter

Email must be formatted correctly.

SUBMIT

SIGNING UP FOR NEWSLETTERS INDICATES YOU AGREE WITH OUR PRIVACY POLICY.

IF YOU DECIDE THAT YOU NO LONGER WANT TO RECEIVE OUR NEWSLETTERS, YOU CAN UNSUBSCRIBE BY CLICKING THE "UNSUBSCRIBE" LINK, LOCATED AT THE BOTTOM OF EACH NEWSLETTER.

FORTRA
Terranova Security