PHISHING PREVENTION EBOOK:
WHAT TO KNOW ABOUT UPGRADING YOUR STRATEGY

TABLE OF CONTENTS

Introduction

Phishing represents a continuous threat to enterprises worldwide, and phishing attacks are growing increasingly sophisticated. Once phishing emails slide past security safeguards, nearly a third of phishing emails are opened.[1] In turn, the probability of someone clicking on malicious content and precipitating a cyber security incident is quite high.

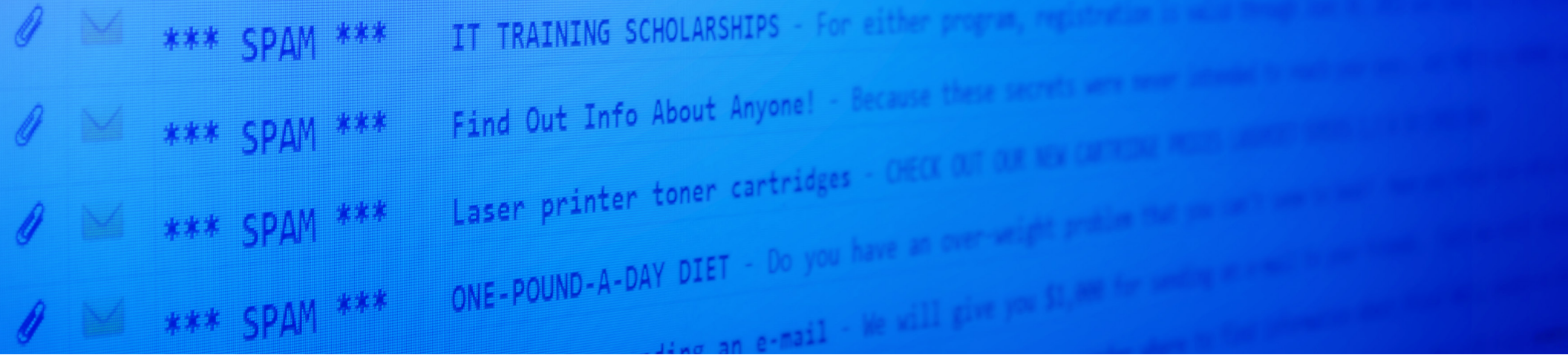
Phishing attacks prey on human behavior, as they aim to take advantage of altruism, fear, uncertainty and other human emotions. Improving phishing prevention can add value to your organization and can prevent value from being lost. In terms of direct value losses, phishing attacks can cost organizations millions of dollars. The latest reports state that the average remediation expenses surpass the $4.5 million mark.[2] And, of course, indirect costs can also take a toll.

In this eBook, get an array of powerful offensive and defensive tactics designed to help decision makers and IT leaders mitigate phishing threats.

---

[1] Slack: Phishing Attacks Go Beyond Just Emails, Clearedin, Ranjeet Vidwans
https://www.clearedin.com/blog/slack-phishing-attacks-go-beyond-emails#:~:text=But%20Slack%20upped%20their%20security,associate%20phishing%20with%20email%20only.

[2] Cyberattacks 2021: Phishing, Ransomware & Data Breach Statistics..., Spanning, Jan 18, 2022
https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/#:~:text=As%20per%20IBM's%20report%2C%20the,increased%20by%2011.9%25%20since%202015.



The Most Common Phishing Scams

Before diving into solutions, it helps to better understand the nature of the issue. These problematic phishing threats commonly send organizations reeling.

1

Brand Phishing

This type of phishing threat occurs when a cyber attacker impersonates a legitimate organization in order to steal usernames, passwords, addresses and other sensitive information.

2

CEO Fraud

This type of phishing scam occurs when attackers impersonate the CEO of a company in order to pressure employees into transferring money into an attacker-owned bank account, or into providing sensitive information.

3

Whaling

This attack type is similar to CEO fraud in that the attackers target executives within a company and aim to persuade them to unwittingly transfer funds, provide login credentials, or otherwise authorize access to systems.

4 Malware-Based Phishing

A suspicious email attachment or downloadable file is a sign of malware-based phishing. Once malicious content is clicked on, it downloads malware (computer viruses, worms, ransomware or other malicious programs).

5 Smishing

Smishing, or text message-based attacks, commonly aim to coerce individuals into clicking on malicious links associated with sales, discounts or bank accounts. Once a link is clicked, malicious code may download or a page requesting personal information may appear.

6 Domain spoofing

In this type of phishing attack, cyber criminals impersonate the domain of a legitimate brand in order to fool users into making fraudulent purchases. Domain spoofing is dangerous on two levels in that it can lead to loss of consumer trust in a brand, and it can lead to personal losses on the part of the targeted individuals.

7 Wi-Fi compromise

In some attacks, criminals leverage fake Wi-Fi hotspots. When individuals use these hotspots, they unintentionally give device access to attackers.

8 Vishing

Scams that rely on telephone/cell phone calls now involve impersonation of major brands. In these scams, a fake a "customer service" representative can pretend to help individuals solve tech problems, only to trick them into downloading malware.

While these attack types may or may not be new to you, the ones on the following page are likely to put your phishing expertise to the test.

Phishing scams newly seen in 2022

1 Ice Phishing

The term "ice phishing" is relatively little-known. For those who may be unfamiliar, it refers to duplicitous activities designed to coerce users into signing transactions that permit token use by cyber attackers. Delegating approval of token use is a common type of transaction related to **smart contracts**, especially those used in DeFi.

In an "ice phishing" attack, threat actors simply need to modify the contract spender's address; switching it over to the attacker's address. This technique remains effective due to the fact that current user interfaces do not reveal all pertinent information that may point towards contract tampering.

After the ice phishing contract/approval has been signed, the attackers can access any corresponding financial resources. Current ice phishers habitually accumulate approvals over time and then drain all financial resources at once.

2 Browser in the Browser Phishing

When a person uses SSO to sign in, the person ordinarily sees a pop-up window that helps with the completion of the authentication process. In a BitB attack, cyber criminals replicate this entire process using a mix of HTML and CSS code in order to create a phony browser window. Once a victim lands on the attacker-owned website, the victim will feel "at-ease" (since it looks normal) and will type credentials into the domain, falling for the attack.

3 Aging Accounts Report Scam

In this scam, attackers send employees (usually in the accounts receivable department) an email that claims to be from a company executive. The body of the email explains that the executive is interested in conducting research related to outstanding receivables, and asks for the latest "AR aging" report, which should include a list of all customers who owe money and the amount past due. Afterwards, the cyber criminal creates and registers a look-a-like domain name, and they reach out to everyone on the list asking for payment.

4 Scams from Your Own Phone Number

Recently, wireless carrier customers reported receiving scam texts that ostensibly derived from their own phone numbers. Research shows that these attacks do not indicate the hijacking of a phone number or lack of account security. Rather, recipients should simply ignore the link, as forwarding it to the standard SPAM (7726) number may result in account difficulties.

5 Wrong Number Scams

Cyber criminals are now sending people personal-sounding text messages, with the goal of having the recipient reply with the words "wrong number". Once the reply text is sent, the scammer knows that the phone number is legitimate. Next, a cyber criminal will attempt to engage in further conversation.

Phishing Prevention Best Practices

The following phishing prevention best practices can empower organizational IT leaders.

Blocking Spam

More than 320 billion spam messages make their way around the globe everyday. Spam filters are often "working overtime" to prevent these messages from making their way into employee inboxes. However, many pieces of spam manage to slip through, and they can contain malicious content. While there isn't a silver bullet when it comes to stopping spam, apply anti-spam technologies that analyze known and emerging distribution patterns and that can block the latest threats.

Security Policies

As noted earlier in this eBook, Business Email Compromise (BEC) is a tactic commonly used by cyber criminals and it involves the impersonation of a business's CEO, CFO, CTO or another trustworthy individual. Upon impersonating the high-level employee, the BEC scammer makes believable requests to other employees, asking them to transfer funds, change billing details...etc.

Sidestep BEC scams by decentralizing your business's approval process. In small to mid-sized companies, the approval process is often highly concentrated, and there are not many who are authorized to give a green light for projects and requests. If at least two individuals are required to approve something, BEC scams will be more easily identifiable.

Review Password Policies

Cyber criminals are often after user credentials. Because people commonly recycle passwords across business accounts, a stolen password (combined with "password spraying") can lead to widespread account access, and can allow hackers to disappear with extensive volumes of data. Consider requiring business passwords of a certain character count, remind teams to avoid sharing passwords, and implement technology that can catch corporate password reuse.

4 Authentication Systems

You can set up authentication systems to identify certain IP addresses, countries and devices as red flags. For example, if you know that your organization does not have any employees in Croatia, you can set filters to flag any requests coming from the country.

With certain technologies, you can also configure systems to provide alerts concerning "impossible travel" or an access request that arrives from a location that would have been impossible to arrive in quickly, based on a users' last known location.

5 Endpoint Security

In addition to email security, endpoint security can help scan incoming messages for malware.

6 Real-Time Notifications

Consider implementing tools that allow for real-time security notifications. If your software only checks links against phishing databases every 24 hours, chances are that your tools have missed quite a few threats. Instant feedback can help security admins and individual users alike, and can facilitate the optimization of day-to-day threat prevention strategies.

7 Protection for All Devices

Hand-held devices often fly-under-the-radar when it comes to cyber security. But your phishing protection solution and/or email security solution should enable you to protect corporate-owned devices. In some cases, you may be able to offer protection to employees who use personal devices for work purposes.

8 Email Security

You need email security. Implement email security solutions that can easily layer into existing cyber security solutions, and that can detect the most sophisticated of cyber attacks. This type of software is designed to prevent malicious emails from hitting end-users' inboxes. In addition, consider a solution that can provide sandboxing capabilities; the practice of quarantining suspicious URLs and other potentially malicious content.

9 Employee Vigilance

Employees can be your best defense or your weakest link. Ensure that employees have the knowledge and tools to prevent phishing across electronic environments. Hold security awareness education and information sessions on a regular basis. Be sure to communicate your message in a dynamic and interesting way that's relevant to end-users. The end-goal is employee behavior modification.

Expert Interview Highlights: Patrik Honegger

This is an excerpt from a recent CyberTalk.org interview with a Customer Success Manager from Check Point Software.

What is the role of automation in preventing and defending against phishing threats?

An extensive degree of automation is a must when it comes to preventing phishing threats. Given the high number phishing attempts, it's simply not practicable to do manual interactions. These should be reserved for flagged attempts, if needed. Modern automation technologies enable organizations to elevate their security standards and to achieve better security outcomes.

In relation to phishing, how can organizations cut through reporting noise?

Although you can have multiple layers of advanced protection, there is no such thing as 100 percent prevention. You need to automate as much as possible and own tools with advanced built-in technologies, intuitive consoles and reporting features. With simplified dashboards and enough insights, administrators can quickly cut through the noise, identify systematic email security risks and if necessary, remediate them instantly. Look for: Actionable analytics, a threat feed overview, and granular analyses capabilities.

How can security professionals save time as they work to prevent/defend against phishers?

- Ensure that your executive board fully supports your holistic view (security controls), and that all areas of threats are addressed, and are part of your prevention mindset!
- Run the prevention approach and fully automate as much as possible, using standard and customized tools. Automation for timely remediation is a key factor in the prevention architecture nowadays.

To see the full interview, click here.

Case Study: Regional Credit Union

One of the largest financial cooperatives in the United States was spending up to 20 hours per week remediating cyber security issues and fending off cyber threats, including vicious phishing attacks.

In one instance, a bank vendor experienced a compromise, leading to a particularly aggressive spear phishing campaign directed towards the bank's underwriters. The threat actor referenced underwriters by name and routinely included malicious Word files in emails, which appeared to come from legitimate, known sources.

"Looking at that email...even I couldn't tell anything was wrong with it," said the Information Security Manager. The phishers were that expert in obfuscating their intentions.

When users received clean and empty attachments, they asked about the originals. A quick look at the emulation results indicated critical severity with a high level of confidence.

The Bank's Technological Solution

"Without...technology in place, the user's computer would most likely have been impacted and infected by the virus that came through," stated the Information Security Manager.

The bank upgraded its cyber security architecture and cyber security posture. Now, the bank's IT teams benefit from comprehensive reports and actionable analytics.

Says the Information Security manager, "[Because of our security upgrades] We're far less likely to get hit with email-born attacks. It helps everybody... sleep a little better at night..."

The solution that the bank went with? Sandblast, by Check Point Software.

> "I would say [Sandblast] has already paid for itself in the year that we've had it, just the time it saves us having to remediate actions, having to do investigations, and its ability to prevent something worse than that happening. You can't put a price on that,"
>
> – Manager of Information Security, Regional Credit Union

In Conclusion

Attending to the best practices and expert insights in this eBook can help you select the right offensive and defensive moves to counter phishers. In addition, be sure to select a phishing solution that can offer:

- Monitoring, logging, reporting and event analysis to correlate data and provide attack information.
- Actionable analytics, a threat feed overview, and granular analyses capabilities.
- Click-time URL protection that examines and blocks suspicious links in real-time, which removes the risk of URLs that are weaponized after the email has been sent.
- Zero-day phishing protection that identifies and blocks new and known phishing sites through analysis of page characteristics and URL components.
- Reduced risk from incoming emails through the inspection of message components — attachments, links and text — before they enter mailboxes.

Check Point's phishing prevention solutions eliminate phishing threats without disrupting workflows or productivity.

For more information about protecting your institution from ever-evolving phishing emails, reach out to your Check Point security representative.

Lastly, be sure to visit the executive-level thought leadership site, CyberTalk.org, for the latest phishing prevention information.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com

© 2022 Check Point Software Technologies Ltd. All rights reserved.