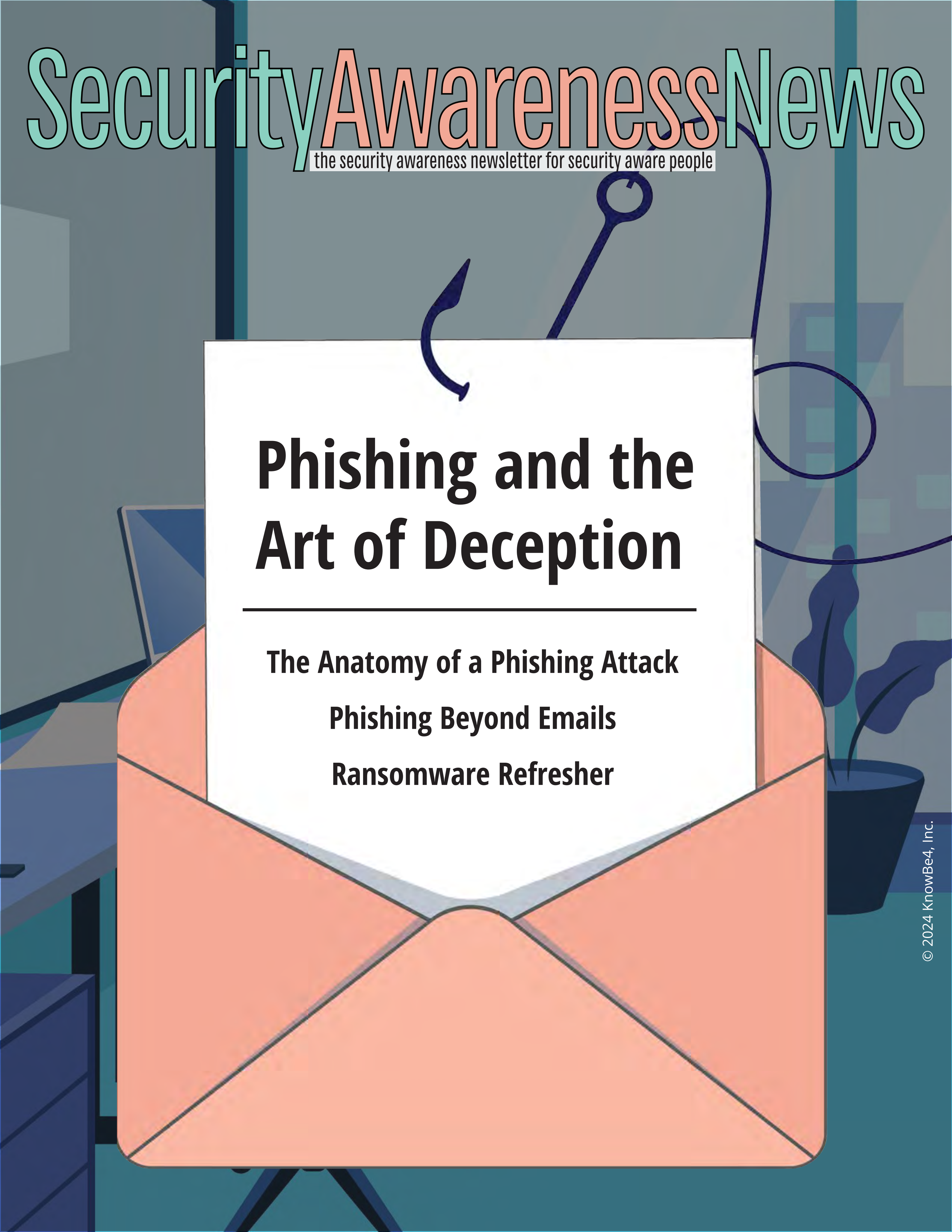
SecurityAwarenessNews

the security awareness newsletter for security aware people



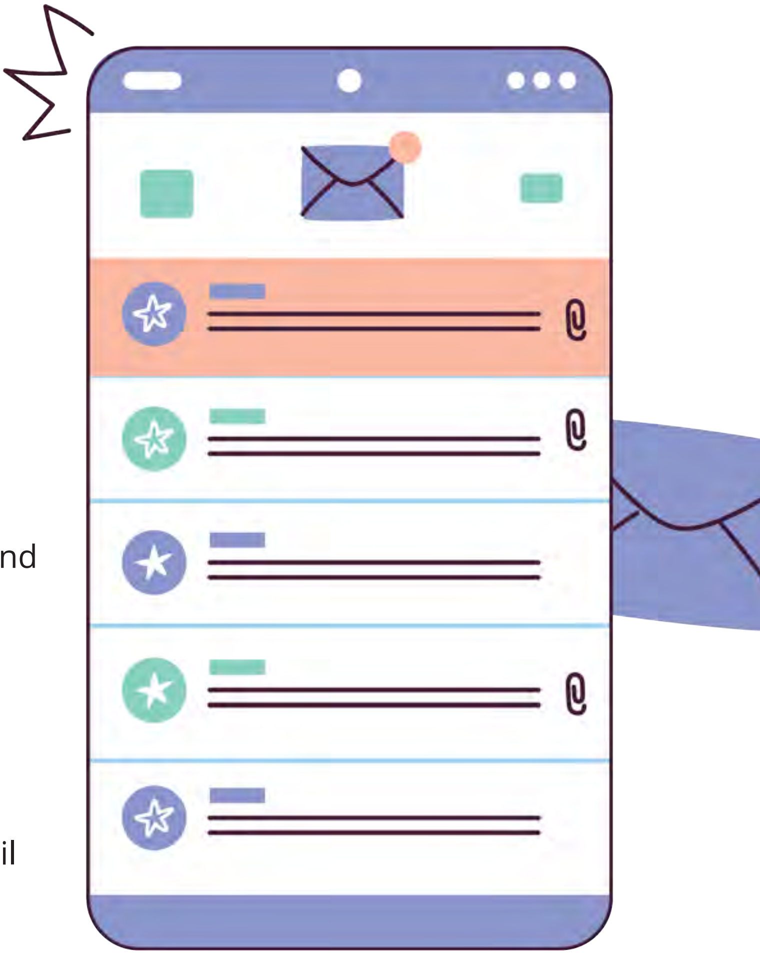
Phishing and the Art of Deception

The Anatomy of a Phishing Attack

Phishing Beyond Emails

Ransomware Refresher

The Anatomy of a Phishing Attack

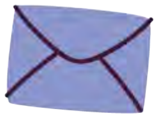


Phishing is the general term given to scams that attempt to lure people into doing something they shouldn't. Cybercriminals use phishing to steal sensitive information, defraud people of money, and spread malware (malicious software).

Let's break down a typical phishing email from the attacker's perspective to better understand the deceptive techniques common in these scams.

Step One: Develop Intrigue

One of the most crucial steps to any phishing email is convincing the target to actually open the email. That's why many attacks begin with an intriguing subject line. Something like "Alert! Your Bank Account has Been Locked!" is usually enough to complete this step.



Step Two: Establish Legitimacy

It's important that the target thinks they're dealing with someone they know. To accomplish this, attackers will create fraudulent email addresses that look trustworthy but have slight alterations. For example, they can simply change a letter in a bank's email address and hope the target doesn't notice.

Step Three: Push Urgency

Attackers want the target to act fast, without thinking. For that reason, phishing emails often feature messages designed to create a sense of urgency. In the bank account example, the email might claim the recipient's funds will remain locked until they can confirm their password and update it.

Step Four: Evoke Response

This step is the call to action. It's where the attacker will ask for confidential information like passwords or urge someone to open a malicious link or attachment. No matter the scenario, this is the moment the attacker hopes their message convinces the target to make a bad decision.

Phishing Beyond Emails

It's easy to understand why email is the primary delivery method for phishing attacks. Emails are easy to create, have a wide reach, and make it simple for attackers to disguise themselves. Phishing, however, is not limited to just email.

Four Ways You Might Encounter Phishing Beyond Emails

Over the Phone

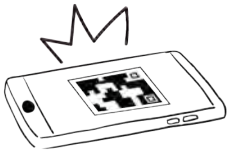
Phishing over the phone usually involves a made-up scenario with the caller pretending to be someone else. For example, they may introduce themselves as a member of your organization's IT department who needs to run an important security update. They need your username and password to install the update on your computer.

Through Text Messaging

Attacks via text messages use many of the same techniques as phishing emails. They often feature urgent or threatening language that begs you to open a malicious link. The personal nature of this attack makes it especially dangerous. People tend to trust messages that come to their phone numbers.

On Social Media

Scammers use social media to steal personal information or defraud people of money. One common way this happens is through impersonation of someone you know. The attacker creates a profile with that person's name and photos and then sends you a friend request. If you accept the request, it gives the scammer full access to your profile, including all of your contacts.



Via QR Codes

In recent years, attackers have embraced the convenience of QR codes (short for quick-response codes). They'll create malicious codes and place them in public areas or deliver them via email and other communications. Scanning a malicious QR code can have similar consequences to clicking a malicious link.

If you ever encounter a phishing attack or anything else suspicious, report it immediately. And remember to always follow organizational policies, which are designed to keep people, data, and devices safe.

Ransomware Refresher

Ransomware attacks are one of the most common and devastating cyberthreats targeting organizations in nearly every industry. Here are a few things everyone should know about ransomware.

What is ransomware?

Ransomware is a type of malicious software (malware) designed to block access to a computer system or files until a large sum of money is paid to the attackers. The malware can spread across networks and prevent organizations from accessing vital resources, bringing entire operations to a halt.

How does it spread?

The most common way ransomware spreads is through phishing. Phishing emails use deceptive techniques to convince people to open a malicious link or attachment. When someone falls for it, ransomware can infect their device and then spread to other devices on the network.

Ransomware can also spread through USB flash drives or cables, outdated software and firmware, and malicious advertisements on infected websites.

What is double extortion?

Many ransomware attacks now feature a double-extortion technique. Instead of simply locking data and asking for money, the malware first extracts the data and sends it to the attackers. They then threaten to leak or sell it, putting more pressure on the victim to pay.

How do organizations recover after an infection?

There are generally three ways to recover from a ransomware infection:

- Attempt to restore systems or data from backups
- Work with security experts to remove the malware
- Pay the ransom fee (never recommended)

What can you do to prevent it?

Given that phishing is the primary method for spreading ransomware, it should remain your primary concern. You can identify many phishing attacks by staying alert for common warning signs such as threatening language, urgent requests, and unrealistic promises or scenarios.