Hypertec
SOLUTIONS PARTNER

April 22, 2024 | by Arctic Wolf

Phishing: A Primer on How to Protect Your Organization

In April of 2024, the FBI released a warning that threat actors are sending SMS phishing, also known as smishing, messages to individuals pretending to be toll road operators messaging about unpaid toll fees. This kind of attack is a common one, and targets more than just individuals -- think the MGM resorts breach of 2023 that started with a phishing call to an IT professional and ended up costing the casino millions.

The tactic originated back in the 1990s and is still a popular avenue for hackers looking for quick financial gain or initial access into an organization.

According to the Arctic Wolf Labs 2024 Threats Report, user action represented 24.4% of engagements with Arctic Wolf Incident Response, and 9.5% of those engagements included phishing. According to the IBM X-Force Threat Intelligence Index 2024, phishing accounts for 30% of initial access vectors for threat actors.

It's clear that this tried-and-true method isn't going anywhere.

What is Phishing?

Phishing is a social engineering tactic that involves a threat actor sending an email to a user with fraudulent of malicious intent. Often, the email is disguised as a legitimate one and is intended to get the user to perform an action such as clicking on a link, handing over financial or sensitive information, or granting access to an asset or application.

At its most simple, phishing can look like the threat actor is using phishing to trick individuals to hand over small sums of money. However, phishing is increasingly becoming one stage in a more complex attack. Threat actors are utilizing it for initial access into an organization with the hope of launching malware or a full ransomware attack. The email used would be sophisticated and appear legitimate, and instead of financial gain, would seek credentials or access to vital applications within an organization.

How Does a Phishing Attack Work?

The crux of any phishing attack is the email itself, and there's a myriad of ways the message can look.

Phishing email examples include:

- A message that looks like it's from HR with a company-wide announcement
- A message seemingly from the IT department asking you to click on a link or provide access to an application
- A message with a link to an internal document attached
- A message that asks for personal information, such as a date of birth or a Social Security number

- A message that asks for credentials or asks you to authorize a multi-factor authentication (MFA) request

If a user falls for the email, or assumes it's legitimate, and takes the desired action, then the attack is successful, and the threat actor has gained what they were seeking.

Phishing tactics have grown in sophistication over the years. One of the first mass-emailed phishing campaigns disseminated the infamous ILOVEYOU virus in 2000. Looking back, it was quite basic by today's standards. All the incoming email message said was, "kindly check the attached LOVELETTER coming from me." Of course, it wasn't a love letter. The attachment was an executable — and maliciously coded — text file. Now, using generative artificial intelligence (AI) and other methods, threat actors can build incredibly realistic emails that are highly personalized or use information already available to them to trick unsuspecting users.

Tactics now used by cybercriminals include:

- Spoofing email addresses from known sources
- Sending well-crafted messages that appear completely legitimate
- Impersonating well-known brands that people trust
- Creating authentic-looking spoofed websites that don't raise any red flags

It's important to note that phishing, like other forms of social engineering, still relies on human behavior, and often, error. Threat actors are hoping that a user will be complacent, in a rush, or put in another heightened emotional state that will cause them to act without thinking through or double-checking the message.

Signs of a Phishing Email

While phishing emails have become harder to detect, they often contain certain traits that users should be on the lookout for.

Common indicators of a phishing attempt include:

1. The message is coming from an unknown sender

2. The message contains grammar or common language mistakes

3. The message is trying to employ a sense of urgency or create an emergency

4. The message contains suspicious links

5. The message supposedly comes from an internal source but uses an external email address or external links

6. The message contains unusual requests such as asking for credentials, access, or personal information

Hypertec
SOLUTIONS PARTNER

Most Common Kinds of Phishing Attacks

1. Email Phishing

Email phishing is a general term which describes any cyber attack that uses email as a method of contacting and possibly extorting victims. These attacks are typically mass-emailed campaigns that cast a wide net with phishing "lures" sent to a vast number of recipients. They will include a malicious link or attachment and try to get the person receiving the message to click on the link or open the attachment by expressing a sense of urgency, inciting fear or curiosity, or using some other enticing message. Attackers will craft their messages in a way to try to make you comfortable, so you'll let down your guard. That's why they often impersonate prominent, popular brands like Facebook and Microsoft, who make up 18% and 15% of all phishing URLs , respectively.

2. Spear Phishing

Spear phishing typically involves a greater degree of social engineering and more intensive research into the target. Such attacks focus on specific people, with attackers sending personalized emails that include valid information about the recipients to convince them of the sender's legitimacy. Cybercriminals may investigate social media for information or just use an educated guess. Although these attacks take more planning, they're also typically more successful, making them well worth the attacker's effort.

3. Baiting

Baiting is a phishing technique that uses an enticing offer or reward, such as a free movie download or giveaway prize. It can also involve physical media, like a USB drive, and arrives via physical mail. The drive may contain a file titled something like "HR highly confidential," counting on employees being curious enough that they can't resist peeking at its contents. Once they click on the file, however, malware is deployed which compromises their system.

4. Whaling

Whaling attacks target big wins scored through hooking executives and other high-value individuals. Attackers will increase their social engineering efforts and often research as much information as they can on the target, using that intelligence to gain trust. This may take place over months and involve repeated two-way communication.

5. Vishing

This attack type combines voice calls with phishing attacks, hence "vishing." During vishing attacks, cybercriminals impersonate people of authority — like a tech support person — to scare the target into acting. The caller tries to confuse and fluster the potential victim, making it a lot easier for the would-be victim to comply with the request. In the MGM Resorts breach of 2023, vishing was used to gain access to the resort's systems.

6. Smishing

Smishing uses text messages (SMS) to send its malicious link. Attackers may impersonate a legitimate company or a co-worker to entice the recipient to divulge sensitive information or download a malicious file. Smishing is also frequently used to get victims to approve MFA requests which may not be legitimate.

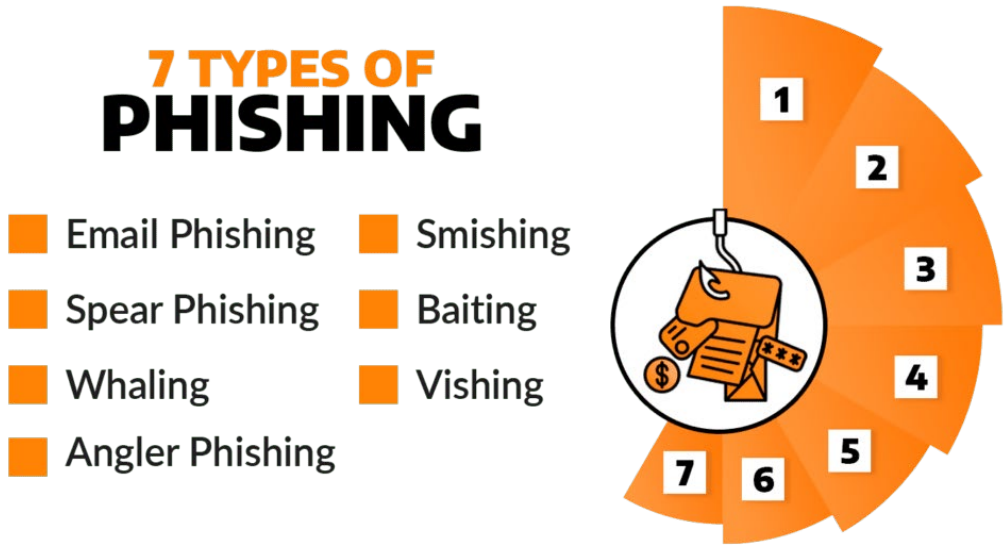
7. Angler Phishing

Angler phishing moves the tactic to social media. In one variation, the threat actor sends a shocking message and links to a person's contacts. When someone clicks on a link, it installs a browser extension that the scammer then uses to do things like change the privacy settings, steal data, and spread the infection through the victim's social media contacts.

In another variation of this tactic, the hacker may hijack a direct message conversation between a brand and a customer and redirect the customer to a fake, malicious page, where the customer is tricked into compromising their information.

Any of these kinds of phishing attacks, sometimes in tandem, can target users and get them to divulge important information, grant access, or accidentally install malware onto an endpoint. And while phishing may often be viewed by some as an obvious scam targeting a single individual for financial gain, it's important to note that it's now more often being used as one step in a series to launch a sophisticated attack against a full organization.

This evolution is seen in the rise of phishing-as-a-service (PaaS). Like ransomware-as-a-service (RaaS), PaaS outsources the more technical aspects of phishing, which threat actors selling via "phishing kits" on the dark web. This allows more amateur hackers to enter the field and expands the volume of phishing that can occur.



Hypertec
SOLUTIONS PARTNER

Why is Phishing So Commonly Employed?

Phishing is not only at the top of inboxes, but also at the top of minds of enterprise executives across the globe. According to a survey by Arctic Wolf, **89% of respondents** have been targeted by malicious messages in the last twelve months — 59% of those were suspected phishing emails and 41% were impersonation emails or text messages. That's a high number, and it grows when considering that the most common security incident of the last year for organizations was **business email compromise (BEC)**, an attack that often begins with a phishing attack to gain credentials or access to specific email accounts.

When questioning executives about attack concerns, ransomware (43%) and business email compromise (38%) were number two and three on the list. The common thread? Both attacks can begin with phishing. Those attacks can be costly, too. According to the IBM Cost of a Data Breach Report 2023, phishing was the most common attack vector and the second most expensive at $4.76M. And there's a simple reason for this frequency: phishing works.

Cybercriminals count on flaws in human nature for phishing attack success. They know that if they get lucky, their message will arrive at a time when a user is focused on other things, in a hurry, on the move, or otherwise not paying close enough attention. To improve their already reasonable odds in getting recipients to do the wrong thing, threat actors use additional strategies that ratchet up the tension or provide credibility to the situation.

By employing these strategies, threat actors have found a high success rate with phishing, and outside of immediate financial gain, these attacks create more opportunities for threat actors. They can gain information to distribute malware, launch a BEC attack, launch a ransomware attack, or even attack connected organizations.

Cybercriminals have an abundance of nefarious motives behind their actions. They employ phishing attacks to gain access to systems and data, and then use that access or information to:

- **Sell your data.** Attackers monetize stolen data by selling it on the dark web to other bad actors, who perpetrate new scams.
- **Try your data on alternate sites.** Knowing that many people recycle their passwords, scammers will try the credentials harvested in one attack to gain access to other online accounts.
- **Leapfrog through all your contacts and impersonate you.** By accessing your email, they launch attacks on the people in your contact list, infecting their systems or attempting to scam them.
- **Lie in wait to deploy ransomware or wreak havoc.** Phishing is often just one step in a multiphase attack. Cyber attackers often wait patiently for the opportune moment to achieve their actual goal.
- **Use your information as their first step to launch an inside attack.** If they get in with compromised credentials, they're more likely to fly under the radar because security solutions like firewalls don't typically flag logins that are using legitimate usernames and passwords. This gives the attackers the opportunity to further penetrate systems undetected — and any systems to which you connect.

Hypertec
SOLUTIONS PARTNER

How To Prevent Phishing Attacks

As phishing shows, the human element is a major part of an organization's attack surface, and reducing human risk is the main way to prevent social engineering attacks like phishing. But any strong cybersecurity strategy should be multi-pronged and comprehensive, looking at everything from human risk to email security to access controls.

Phishing attack prevention should include:

1. Security awareness training that works to reduce human risk while educating employees on what to look out for so they can identify and stop phishing attempts they may receive in their inbox.

2. Regular phishing simulations that test your human attack surface and educate users on what real phishing threats could look like.

3. Email security that not only filters out spam and flags suspicious emails but has a way for employees to flag and report potential phishing emails.

4. Organization-wide access controls such as MFA. If an employee falls for a phishing attack and gives away credentials, a simple access control can stop the threat actor from proceeding with their attack.

5. 24×7 monitoring of endpoint, network, cloud, and identity sources to ensure that if a phishing attack is initially successful, it can be detected and responded to swiftly, preventing a larger attack or data breach.

Want to learn more or need help?

> Contact Sales by email or call **1.866.787.0420**

> About Hypertec Solutions Partner

Blog by Arctic Wolf

Arctic Wolf provides your team with 24x7 coverage, security operations expertise, and strategically tailored security recommendations to continuously improve your overall posture.