HOW TO SPOT AND PREVENT PHISHING ATTACKS

PRESENTED BY

Ntiva

Your Success. Secured.

WHAT IS PHISHING?

Phishing is a type of online scam where cyber criminals send deceptive emails that appear to be coming from a legitimate organization or person, to unsuspecting recipients.

Their intent is to trick the email recipient into clicking on a link or downloading an attachment, in order to:

- **Steal sensitive information such as credentials, social security numbers, etc.**
- **Embed malicious code (malware) into computers and networks**
- **Get the recipient to wire funds, pay bogus invoices and other financial schemes**

It is estimated that more than 90 percent of security incidents today start with a phishing attack, and that the average user now receives at least 16 phishing attempts per month!

This has become a very serious issue for organizations across the globe. Barely a week goes by when we don't hear of a major security breach that has occurred due to phishing in a well-known company or institution.

But don't be fooled – companies of every size and type are just as vulnerable.

WHY PHISHING WORKS

In short – **human error**.

An unopened phishing email that sits in your inbox is harmless.

To unleash its destructive capabilities, you must either click on a link or download an attachment.

Not too long ago, phishing emails were easy to spot. They were typically bulk spam emails, badly worded and full of grammatical errors.

Today, phishing emails are way more sophisticated and sometimes it's extremely difficult to spot them.

Phishing and other cybercrimes are no longer performed by a couple of guys in a basement – this is BIG business and is run by experienced teams who make billions of dollars.

THE TWO MAIN GOALS OF PHISHING

Generally, a phishing campaign tries to get the victim to do one of two things:

1. Hand over sensitive information.

These messages trick the user into revealing important data, such as a user name and password so the attacker can breach a system or an account. A classic example is an email that is tailored to look like a message from a major bank. The victim clicks on a link and is taken to a malicious site that looks like the bank – and then hopefully enters their username and password. The attacker can now access the account.

2. Download malware.

This type of phishing email aims to get the victim to infect their own computer, and often the entire company network, with malware. Once a recipient clicks on a link, the malware gains access to the device and locks down (encrypts) your files, databases and or applications.

The most common form of malware is ransomware, where the attacker demands a ransom in exchange for releasing, or de-encrypting, your data.

THE THREE MOST COMMON TYPES OF PHISHING ATTACKS

Although there are many different types of phishing attacks, below are three of the most common phishing techniques that you are likely to encounter.

1. Deceptive Phishing

In this ploy, the attacker impersonates a legitimate company in an attempt to steal personal data or login credentials or get the recipient to take action on a fake claim (such as buying gift cards or paying bogus invoices.)

This method often involves a “spray and pray” technique, sending mass emails to as many addresses as they can obtain. These emails are often written with a sense of urgency, informing the recipient they must respond immediately.

A good example of this is an email that appears to come from your bank, or a large vendor such as PayPal or Amazon. Recipients are instructed to click on a link in order to rectify a discrepancy with their account or similar request.

In actuality, the link redirects to a website that is designed to impersonate the vendor’s login page. The website collects the login credentials from the victim when they try to log in and sends the data to the attackers, who now have complete access to the account.

THE THREE MOST COMMON TYPES OF PHISHING ATTACKS

2. Spear Phishing

The goal with spear phishing is the same as deceptive phishing: trick the victim into clicking on a malicious URL or attachment so the user will hand over their personal data, install malware, or take action on a fake claim.

The difference here is that opposed to the bulk emails mentioned above, malicious emails come from what appears to be a trusted source, such as a colleague or your boss, and are often sent to specific individuals within an organization.

In spear phishing, this does not mean that the hacker has necessarily hacked the company email. It is often a case of "spoofing" the email address.

These email campaigns are hyper-personalized in order to make the victim believe they have a relationship with the sender, making them more likely to fall for the ruse.

A good example is an email that appears to come from your boss, asking you for login credentials, to wire funds to a certain account, or perhaps purchase an item. If you're under pressure, juggling multiple tasks or a junior employee, it can be tempting to respond to the request immediately, especially if the sender is your boss or your CEO.

3. Business Email Compromise

This form of phishing is when the attacker obtains access to the business email account of an employee, typically a high-ranking executive such as the CEO.

Once they have access to the executive's email account, they can send emails to employees using the correct email address, making it really difficult to spot the trick.

Even if the victim takes the time to look at the sender's email address very carefully, it will look legitimate.

So how do we figure out what is real and what is not? Read on!

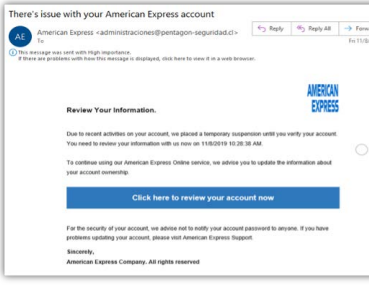
THREE REAL PHISHING EXAMPLES

A picture is worth a thousand words, so let's look at some real phishing examples.

1. When the sender's email address is "fishy."

If you look closely at the email image shown, you'll notice several things wrong.

First, the name and email don't match. Considering the domain name of American Express is americanexpress.com, we can tell that this is not a legitimate email.



Second, "American Express Company" in the salutation is not the name of the company. Big red flag.

Third, the sense of urgency in the subject line of the email is a clear indication that this might be a phishing email.

Fourth, if you were to hover over the provided link, you would notice it does not take you to the URL of the legitimate American Express website.

If a request comes out of the blue from a large institution, a partner, or anyone that you do business with, and it seems unusual– pick up the phone and call before responding!

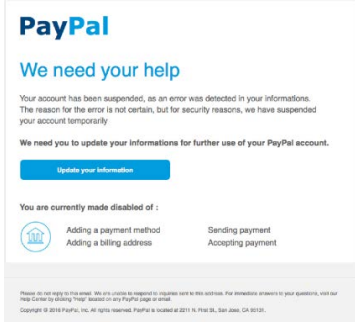
THREE REAL PHISHING EXAMPLES

2. When the sender uses a generic salutation.

If PayPal or your bank or other provider sends you an email that doesn't mention you by name – beware.

In the PayPal email, we only see "We need your help."

It's really unlikely a large organization would not use your first and last name in any official correspondence.
We can also notice grammatical errors.

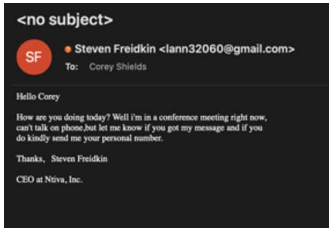


It's unfortunate that we need to check out almost every email we receive for legitimacy, but it pays to be suspicious BEFORE you click!

3. When you recognize the sender - but not the request.

This is an example of a phishing email Ntiva employees received which appeared to be from our CEO Steven Freidkin.

For starters, the email address is completely bogus. But suppose in your rush to respond to your CEO you did not notice the bogus email address or – the email address was actually correct (as in Business Email Compromise.)



The fact is that this request is extremely odd. It's highly unlikely Steven would be asking one of our marketing managers for his personal number, or to purchase 200 Apple iTunes cards, or to wire money immediately...the list goes on.

Again – pick up the phone or send a fresh email to confirm if the request is legitimate!

WHAT CAN EMPLOYEES DO TO PREVENT PHISHING ATTACKS?

Here are some top tips to help you recognize and prevent phishing attacks:

- Never click on links or download attachments from an unknown sender. Just don't.
- If you think you recognize the sender, but the request seems odd or out of place – pick up the phone or send a fresh email to confirm.
- Hover over links before you click. Use your mouse to hover over a link (Do not click! Just hover!) in Outlook or a web browser. A small window will pop up to show you where the link really goes.
- Unfortunately, even hovering over a link to determine the URL is not always completely safe. If you really want to verify a link, try a tool such as Google Safe Browsing or **this nifty tool from trendmicro** that will show if the link is legitimate.
- Do not respond to high pressure emails that request password changes or personal information – again, pick up the phone or send a fresh email if you are concerned.

WHAT CAN BUSINESSES DO TO PREVENT PHISHING ATTACKS?

Here are some of our best recommendations, but be sure to consult with a **qualified cybersecurity consultant** to nail down exactly what your business needs to do to remain safe.

1. Educate employees and conduct **training sessions** with phishing scenarios.

2. Keep all systems current with the latest security patches and updates.

3. Implement a security policy to address password expiration and complexity.

4. Implement **Multi-Factor Authentication** to protect access to online applications and to the environment (such as a VPN).

5. Deploy a web content filtering solution to block malicious websites.

6. Deploy an email spam filtering solution to minimize the amount of phishing emails coming through.

7. Deploy an **Endpoint Detection & Response (EDR)** solution on every system to prevent malware from spreading into the environment.

That last recommendation – EDR – is now even more important since many of our workers are remote, and may well stay remote. Most of us are no longer behind the firewall in the office!

SUMMARY

Every single business is exposed to phishing attacks on a daily basis.

But if you know what to look out for and have the right tools in place, you can secure your data under lock and key and keep your business safe from harm.

If you would like to see how Ntiva can help you identify and prevent cybersecurity breaches and attacks, **give us a call or send us an email** and we'll be happy to help.

Ntiva

Your Success. Secured.