How to Prevent Phishing Attacks

A Training Guide for All Employees

Provided by:

VERMONT CONNECTIONS

Table of Contents

Table of Contents

Introduction

Did you know your own colleagues are the weakest link in your business's security?

According to a Wombat Security report, **more than 75%** of information security professionals said their organizations identified phishing attacks in 2017.

This is a serious problem that affects businesses of all sizes, and it shows no signs of slowing down.

In this day and age, you cannot rely only on firewalls and passwords to keep your organization safe. Arming yourself with good information is the only way to keep hackers out and your data safe.

In the following pages we will show you:

- How cyber-thieves get you to open the virtual door
- The telltale signs that something is phishy
- What to do when you’ve found a potential threat

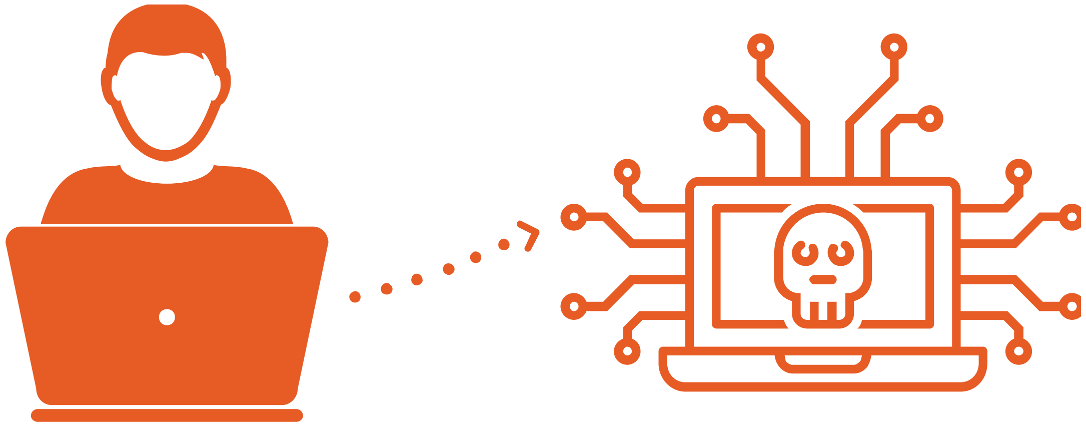
How Phishing Attacks Work

How Phishing Attacks Work

It’s a typical day at the office. Everyone is hard at work at their desks, not checking Facebook or shopping on Amazon (because you never do that, right?)

All of a sudden you get an email from your bank saying something to the effect of:
“Your last transfer is being held for security reasons. To release the funds, click on the link below and sign into your account.”

Concerned, you click on that link, and… just like that, you’ve opened the door for malicious software to infiltrate your business network and steal data.



How Phishing Attacks Work

Phishing emails are one of the most common and effective “social engineering” tactics hackers use to get access to private data.

Social engineering is a type of cyber-attack that involves convincing people to give something valuable to the attacker.

Although the tactics vary, thieves depend on getting people to trust them by posing as a business contact or a friend and stealing passwords, account information, or access to their computer or network.

How to Identify a Phishing Email

RULE #1: Always be vigilant. ⚠

A phishing attack will succeed only if a hacker finds you asleep at the wheel. But after today, that will never happen.

You’ll be able to spot one of these clowns from miles away.

Here’s how…

1. Check Your Emotions

Phishing emails are successful because they provoke urgency. They hit an emotional trigger that makes it hard for you not to respond. Here are some real life examples we've seen:

- An email posing as a message from Microsoft Outlook, claiming you have emails waiting to download into your inbox. Please sign in or your emails will be deleted in two days.
- A message from Netflix stating your credit card is expired and your account suspended. It asks you to click their link and update your information.
- An email from UPS or FedEx that asks you to update your company's address so they can ship an item to you.

If you get an email from a trusted business partner or friend that asks you to take fast action to get a reward or to avoid a negative consequence – this is the time to stop and look at things more closely.

2. Watch for Emails That Ask For Money or Personal Information

The three “Ps” of phishing scams include:

- **PAYMENTS**
- **PASSWORDS**
- **PERSONAL INFORMATION**

Any email that asks for any protected data from you should immediately throw up red flags.

Hackers carefully design their emails to look exactly the ones you would get from a trusted institution you love and depend on…like the IRS (Joke. Just checking to see if you are still paying attention).

Here are the different types of phishing emails you might see:

- **Mass Phishing** – These emails are sent to thousands of users at once, so they aren't personalized. One example is a message that tells you someone just bought an airline ticket using your credit card and to open the attached document to dispute the charges.
- **Spear Phishing** – These attacks are personalized and specific, often posing as someone you know. Instead of saying "Dear Customer" they will be addressed to your name.
- **Business Email Compromise** – In these cases, the attack is sent through a compromised email address in your organization, which makes them harder to spot.

If you get an email that asks you to voluntarily give up personal information, don't comply to their request! At this stage, you should inspect the email for other signs of tomfoolery.

3. Check the Email Address

It’s important to understand the difference between a display name and the email address. This is where a lot of people get tripped up.

A display name is what most people see first when they open an email, and that name tells them whether or not it’s someone they trust. But here’s the rub:

Display names are easy to fake. Email addresses are not.

If you open an email and see anything that makes you suspicious, check the email address. Is the sender from “support@amazon.com” (likely legit) or does it say “amazon1@gmail.com?”

This tells you the address is likely fraudulent.

Another sign, much easier to spot, is when the address has illegible gibberish in it.

If you recognize one of these issues in the address, chances are good you’ve seen the hook before biting the worm.

4. The Tone of the Email or Spelling Seems Strange

A phishing email usually looks a little bit strange to the trained eye. For instance, you know what your friends and family sound like when you read their messages. These subtle nuances are very hard for hackers to imitate, so the rule of thumb is when something sounds wrong, it’s because it usually is.

Emails that are masked to sound like third-party businesses, like your bank or favorite online retail store, can be a little harder to detect, but if the content of the email throws up a red flag (by trying to generate an emotional response) you might also find the writing sounds a little wooden, like it was written by someone who doesn’t speak native English. You might also see odd grammatical and spelling errors. This is a clear sign of a phishing scam.

5. The Greeting Sounds Different

Even though some hackers have gotten more sophisticated and started using contact tokens in their email templates, many of them still use generic greetings like, “Dear Sir” or “Dear Madam.”

A legit business will use a personalized greeting every time, so if you see a complete absence of that you might reply with “Dear Phishing Scammer.”

What Do You Do When You’ve Identified a Phishing Threat?

What Do You Do When You've Identified a Phishing Threat?

When you come across an email that looks suspect, the most obvious thing to remember is to not click on any attachment or link in it.

Close the email, and notify your systems administrator right away.

If your company works with a Managed Services provider, they have likely set up a shared mailbox specifically for "suspicious email reporting." Add the email to the mailbox and contact your MSP right away.

Spread the word fast. It's safe to assume you aren't the only one in the organization who got this email, and one of your co-workers might slip up and click on something they shouldn't.

What Happens If You Accidentally Click On a Malicious Link?

If you click on a link or attachment before realizing it’s likely malicious, here are some steps that will help you mitigate the damage:

1. **Disconnect your device from the network immediately**
2. **Back up all your files on a server or external hard drive before restoring your computer**
3. **Change your login credentials**
4. **Put your credit card companies on high alert for potential fraud**
5. **Run an anti-virus program and scan your system for malware**

Conclusion

That’s it!

You’re now prepared to stop a phishing attack dead in its tracks.

Please add your signature for the form below and return to Human Resources, confirming that you have read this training guide and understand the material.

Thank you for helping us keep our company safe and secure!

Please sign this page and return to Human Resources:. If you have any questions about the material, please speak with your hiring manager.

By signing, I certify that I have read this training guide, and understand my role in preventing cyber-security attacks on our company resources.

Signature	Email	Date

About Vermont Connections

Vermont Connections is a managed IT solutions provider located in St. Albans, VT, specializing in helping companies achieve greater productivity, security, and efficiency across their organizations.

OUR SERVICES INCLUDE:

- Help Desk & Co-Managed IT Support
- Managed Security, Backup & Disaster Recovery, and Compliance
- Cloud Migrations
- Planning & Consulting
- Office Phone Systems

We believe every healthy IT environment begins with a well-informed staff, and this training manual is just one example of the resources we provide to the business community.

Visit our website to learn more about ways to improve security, increase efficiency, and reduce unneeded expenses: www.VermontConnections.com.

Thanks for reading!

David Mahoney, President & Founder