SECURITY TASKFORCE

# When PHISHING hits your mail boxes.


## Phishing

Phishing is generally an attempt to gain the personal data by posing as a known authority; normally an online service or a bank.

Spear phishing has caused tremendous data loss for many organizations.

The main reason behind this is they seem to be completely **authentic and genuine** making it more difficult to understand the difference.

## Possible Remedies:

Ask your employees not to share the sensitive information as no company will ask for your personal data for official use.

Also implement an effective firewall, **spam filters** to prevent them from falling into the inbox.

# Understanding Phishing attacks

In Q1 2019, the Anti-Phishing system prevented 111,832,308 times and these number are based on detections by Kaspersky Lab's Anti-Phishing component.

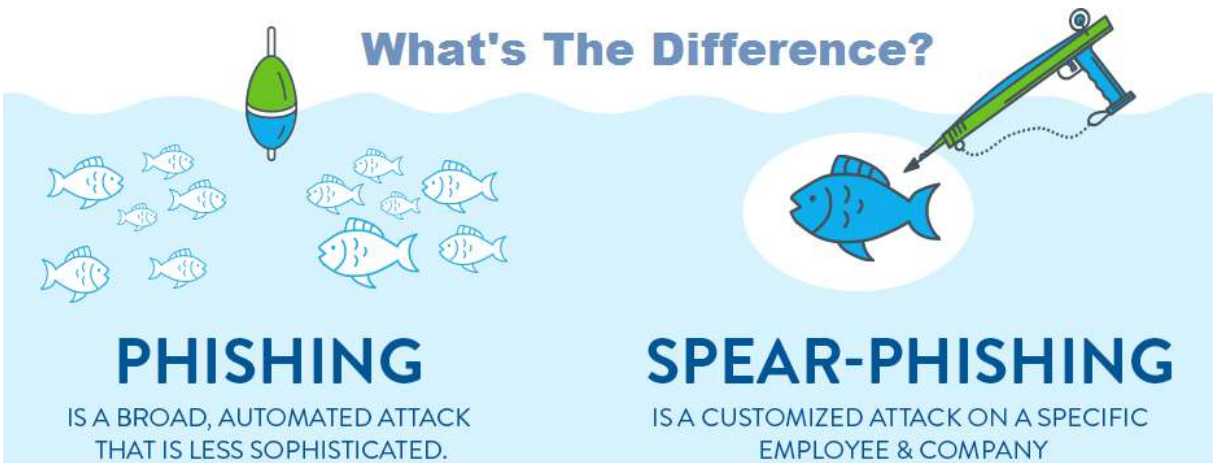
A phishing attack is a type of attack designed to steal user connections, credit card information, and other types of personal, commercial or financial information.

Coming from an apparent source of trust, for example by borrowing the identity of well-known and trusted websites, banking institutions or personal contacts, these attacks are becoming more and more advanced and, unfortunately, more effective.

By entering or using identifiers, clicking on links or replying to phishing emails with financial information, the information is sent directly to the malicious source.

It is not easy to avoid these attempted attacks. Awareness can be raised by implementing cyber-sensitivity programs to reduce the risk of being a victim of phishing attacks.

In addition, awareness or cyber threat assessments can be a good starting point to see how users in your organization are familiar with phishing attack tactics.



# What is Spear Phishing?

In general, phishing is the practice of sending fraudulent emails from what appears to be a trusted sender in your organization, like a family member, bank institution, or someone from your business that you frequent.

Phishing and spear phishing attacks both follow this practice, but the similarities end with the strategy they use to get your information.

Regular phishing attacks trawl the waters with a wide net, hoping to catch whoever falls for their scam. Spear phishing emails, on the other hand, target users that have specific access to the information hackers want. These users could be accounting employees, executives, or IT professionals.

Spear phishing emails are tailored to look, sound, and feel legitimate.

The messages they contain generally include a grab for confidential information, like a link you can follow to change your password, a downloadable attachment, or a request for sensitive employee data.

Regardless of what form it takes, if you follow the email's instructions, your computer and organization are immediately compromised.

## Spear Phishing Affects Everyone

The number of spear phishing attacks on organizations climbs every year. Cybersecurity growth has spiked to anticipate these security concerns, but that doesn't mean companies who follow best practices are protected from a potential attack.

Employees can fall victim to these scams without ever realizing something is amiss, and the repercussions of a single instance of infiltration? They're crippling.

Spear phishing attacks affect a multitude of industries. Top industries targeted by these attacks in 2019 include logistics, retail, public administration, finance, and services.

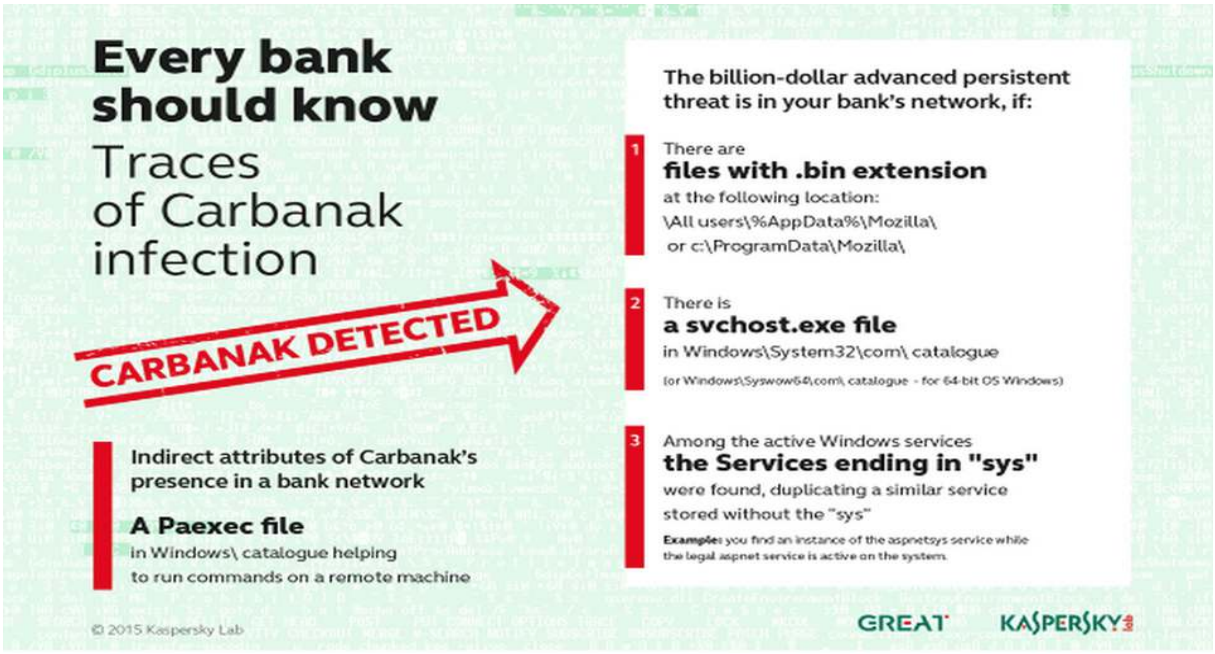
What's worse, a successful attack can cost a company, on average, $ millions. This is a huge amount of damage.

The Carbanak Breach impacted over multiples financial institutions and cost them around $ billions.

According to Kaspersky Lab, who investigated the breach:

*"The attackers used spear phishing emails [to infiltrate the bank's intranet], luring users to open them, infecting machines with malware. A backdoor was installed onto the victim's PC based on the Carberp malicious code, which, in turn gave the name to the campaign — Carbanak." Kaspersky Lab.*

Are you confident your business is secure enough to shut down potential phishing attacks? Think twice.




## How to Protect Yourself against Spear Phishing

If you're concerned about the danger of spear phishing attacks or looking for ways to make your environment more secure, we suggest you implement these seven steps in your company. They may help stop a potential attack before it can begin.


## 1. Keep your systems up-to-date with the latest security patches

Check your operating system frequently for the latest security patch releases. Insure to have

If you're running Windows, Microsoft is always updating and promoting their security patches, especially if they foresee a new security concern and want to fortify their users.

This is also true of unsupported versions, like Windows XP, Windows 7 or Windows 8 if there's enough risk to warrant an update.

Like Microsoft, Apple, Linux, AIX, and others operating systems also have security patches.

New ones are released as industries rise to meet and predict new phishing attacks, **so keep your systems** (both customer-facing and internal systems) **up-to-date and install new security patches** whenever possible to **avoid gaps in protection**.

## 2. Encrypt any sensitive company information you have

File encryption is a good way to protect sensitive company data from prying eyes. With the right tool or solution, the files you send to your systems, cloud environments, trading partners, and remote locations will be secure, making it difficult for outside parties to decrypt your data even if they get their hands on it.

What should you encrypt? Here are just a few examples that limit the amount of damage a spear phishing attack could do to your organization:

- Passwords and security questions
- Hard drives
- Cloud storage
- Internet activity (using a VPN or masked IP address)
- External storage (USB drives, external hard drives)
- Files (business contracts, audit reports, tax documents)

## 3. Use DMARC technology

You'd think, in this day and age, that emails received from an address you know would be trustworthy.

After all, you get emails from YourbestFriendatWorkr@company.com all the time, which means even the suspicious emails are safe to answer.
Right? Wrong.

Far too often, hackers are **able to spoof the FROM field** of an actual email address, such as JohnDoeCEO@company.com, and send a message with that address to company employees.

Because these spoofed emails look real and cause successful spear phishing attacks, DMARC (Domain-based Message Authentication, Reporting & Conformance) technology uses Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) to analyze incoming emails against its database.

If the email doesn't match the record for the sender, DMARC rejects it and submits a report to a specified security admin.

"A very important aspect in email security is making sure your email provider uses technology like DMARc".

It's the **only email authentication protocol** that ensures spoofed emails do not reach consumers and helps maintain company reputation.

Despite the obvious benefits of using email authentication technologies, DMARC and other protocols like it are not foolproof.

Many big companies like Microsoft, Google fell victim to a successful spear phishing attack in the past years when hackers sent emails containing

fraudulent Microsoft OneDrive links or Google Doc links to users. Million accounts were compromised.

While in Security Task Force, we still recommend implementing **DMARC/DKIM** into your email, consider it but one of many tools you should use to secure your data, users, and company.

It's just safer that way.

## 4. Implement multi-factor authentication wherever possible(Very important)

Many businesses have implemented multi-factor authentication (MFA) into their security routine. Some, like Microsoft, Google, allow their customers to turn on MFA as a precautionary measure.

So why not use MFA to protect your data?

Multi-factor authentication is a simple way to ensure anyone who accesses your private data is legitimate.

### How does it work?

It requires at least two pieces of identification, like a login and randomly generated token, that makes it infinitely harder for hackers to compromise your systems—even if they have half the information needed to get in.

If we lived in a perfect world, user passwords and security questions would always be secure.

But in reality, employees recycle passwords across multiple websites and overshare personal data on social media, compromising the integrity of their logins and security questions.

So really, implement MFA wherever you can—at work and in your personal life.  At the very last, it'll give you an extra layer of protection against spear phishing and other potential data breaches.

## 5. Make cybersecurity a company focus

Is cybersecurity a focus in your organization? It should be. When security is forefront in your mind and the minds of your employees, better decisions are made and more precautions are taken, enabling you to prevent spear phishing attacks before they become a concern.

Here are a few recommendations to get you started:

- Create a Global Cybersecurity Policy and data breach response plan for your organization.
- Document and send internal security procedures to your employees.
- Identify potential spear-phishing targets and brief them on the actions they should take if they receive a questionable email.
- Review employee roles and access regularly, including third party vendors, partners, and those in remote offices. Make adjustments as necessary remove unnecessary access privileges.
- Schedule quarterly meetings with IT security Officer and others cyber security key players to review the latest spear phishing attacks in your company or in the general industries.

## 6. Educate your employees and regularly test their knowledge

Over 90% of cyber-attacks are successful because of employee error. What's the common method used in these cyber-attacks to compromise data? You guessed it, spear phishing.

Spear phishing emails are rarely transparent. One believable email from a spoofed address is all it takes to gain access to employee credentials and, from there, sensitive company information. But the good news is, **human error is avoidable with some training and education**.

Talk to your employees about the reality of phishing attacks. Set aside 15 minutes at your next company meeting to educate them on what spear phishing attacks look like, what they do, and any steps they should take if they encounter one.

Document a quick guide to internet security and make it available on your network. Even quarterly quizzes with a fun prize for winners can be the motivation needed to build security knowledge.

The more opportunities your employees have to learn about spear phishing and other scams, the better prepared they'll be if they encounter something suspicious.

## 7. Confirm suspicious email activity before interacting with it

If you receive a suspicious email from someone you trust, but you're not sure if it truly came from them, stop by their office, pick up the phone, or send them a separate email.

The two minutes it takes to establish validity is absolutely worth it, no matter the outcome. Best case scenario?

The email is legitimate, and you have peace of mind. Worst case scenario?

It's a spear phishing email, but you still have peace of mind, and the person you spoke to can now warn others in the organization of a potential phishing attack.

Spear phishing attacks happen every day. But though they're a security concern, they don't have to be a problem if you plan ahead, prepare your organization for attacks, educate your employees, and encrypt your data.

## Best Practices

### Don't end up a victim of phishing:

- Use a phishing filter. Many web browsers have filters built in or offer them as plug-ins.
- Most companies, banks, organizations, government agencies, etc., do not request personal information or credentials via e-mail. When in doubt, give them a call (but don't use the phone number contained in the e-mail—that is fake as well).
- Never follow a link to what you think is a secure site from an e-mail. Always enter the URL contained in the email manually.
- Don't be fooled by the latest scams. If it looks too good, it isn't.
- Report suspected emails to suspect@safeonweb.be and contact your CSIRT or your national CERT if you have been hit by one those attacks.

### Watch for emails that:

- Insist on urgent action
- Have suspicious attachments
- Have unsolicited awards
- Have an unfamiliar or awkward greeting (Usually from Nigeria)
- Have an unusual or inconsistent email address, domain name, or link
- Request login credentials, payment Information or other sensitive information
- Contain spelling errors or grammatically wrong writing

To fight spear-phishing scams, employees need to be aware of the threats, such as the possibility of bogus emails landing in their inbox. Besides education, technology that focuses on email security is necessary.

Contact: info@security-taskforce.be Or just call: +32 496619154