Biznado (Natalia Wocial Przemysław Adam Mączka) & Klocki (Aga Patro, Jakub Młocek)

PHISHING

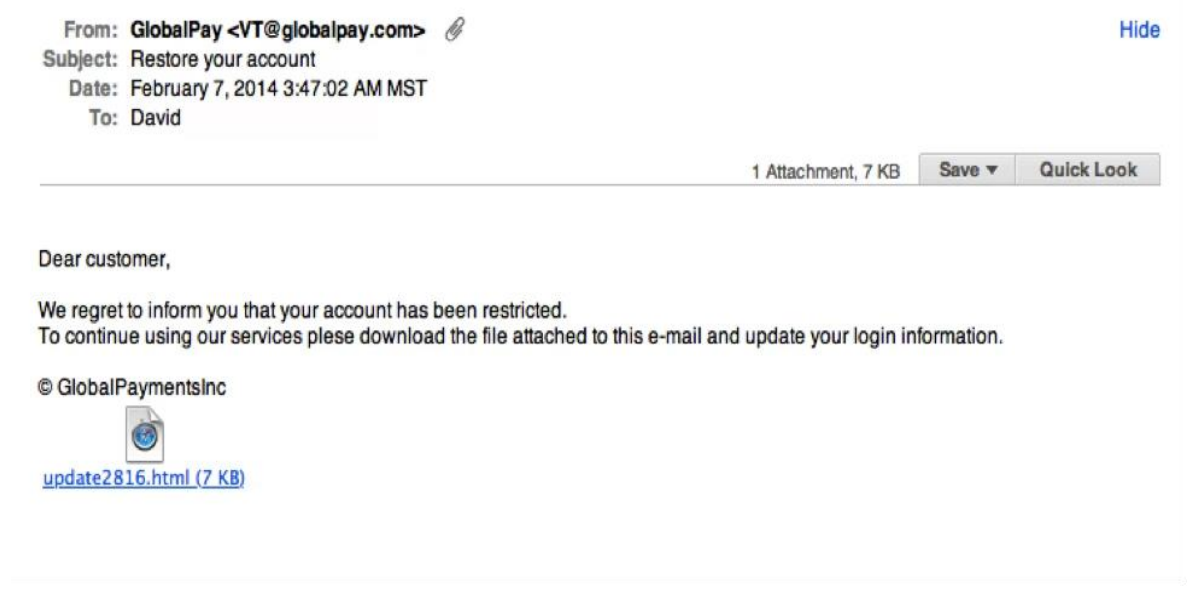
What is Phishing?

Phishing is one of the most popular types of attacks based on e-mail or SMS messages. It uses social engineering, a technique where online criminals try to trick network users into acting as they want to. Cybercriminals pretending to be, inter alia, courier companies, administration offices, telecommunications operators, or even our friends, try to obtain our login details, e.g. for bank accounts or the social media accounts we use, or business systems.

The name phishing evokes sound associations with fishing - that is, fishing. Criminals, just like anglers, use a properly prepared "bait". The most used technique is to send fake SMS and e-mails. Increasingly, fraudsters also operate via instant messaging and social networking.

Phishing messages are prepared by cybercriminals to make them appear genuine. They may try to trick you into revealing confidential information, contain a link to a website spreading malware (often criminals use similar website names to genuine ones), or have an infected attachment.

Example of phishing:

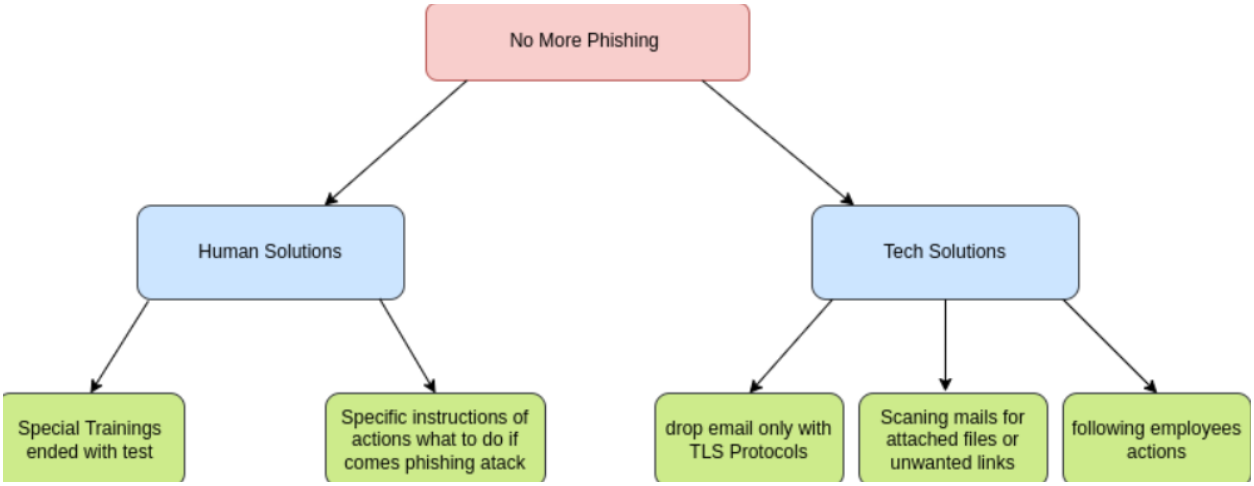


Types of Phishing:

- **Spear phishing** - an attack targeting a specific group or type of people, e.g. company system administrators.
- **Whaling** - CEOs, CFOs, and all other directors in an industry or specific company target this type of attack. The whaling email message may say that the company in question has legal issues and you need to click a link for more information. This link takes the victim to a page where all-important company details, such as tax ID and bank account numbers, must be entered in order for the site to work.

- **Smishing** - a type of attack that uses text messaging or SMS. A popular smishing technique is to send an SMS message containing a click link or a callback number to a mobile phone.
- **Vishing** - this type of attack is carried out over a voice connection. A typical vishing attack is a call from someone who claims to be a Microsoft representative. It informs you that a virus has been detected on the user's computer. He is prompted for credit card details so that the hacker can install an updated version of the antivirus program on his computer. From now on, the hacker has the victim's credit card details and probably tricked them into installing a virus on their computer.
- **Phishing e-mail** - The most common type of phishing that has been around since the 90s. Hackers send their messages to any e-mail addresses they can get hold on. The content of the message most often informs you that your account has been hacked and you should react quickly by clicking on the link provided.
- **Search engine phishing** - Also known as SEO poisoning or SEO Trojan, these are hackers' actions aimed at getting a high position in the search engine results of an Internet search engine. When user clicks on such a link, they will be redirected to a specially crafted website. With its help, criminals can collect data related to the interaction or trick it into providing sensitive information. Hackers can impersonate any website, but the most common sites for hackers are banks, money transfer services, social media, and online stores.

Our team proposes two solutions for the problem of phishing. The first one is Human solutions and the second consists of securities based on technology.



1. Human Solutions

How to protect your business against phishing?

Since the problem of phishing is mainly related to negligence on the part of employees and less related to IT security oversight, the solution to the problem will be based primarily on making staff aware of the problem. Below we will propose both It and human solutions approaches to the problem.

Good employee habits

The main issue when it comes to protecting against phishing is the use of caution by users. Workers must be aware of the dangers of ill-considered:

- opening links in e-mails
- opening attachments in e-mails
- accessing questionable websites

For this purpose, it is worth organizing training on phishing in your company. So that employees know what to do when they get a suspicious message. Not to let them click without thinking about the links they get in e-mails. Employees should have it in their heads that before they click on anything, it is worth considering twice whether it is sometimes a "trap". Good habits of employees will definitely allow Eklamot to be protected against the loss of important information.

Effective phishing training – what should it consist of?

1. Familiarize employees with the term phishing, with a focus on demonstrating why it is dangerous for both the company and private Internet users – it is important that the presentation includes examples of future attacks and information on how much the company has suffered as a result.
2. To provide training participants with knowledge of the detection of phishing messages by handing out cards with printed phishing notes.
3. Demonstrate the different types of phishing using examples of e-mails sent by cybercriminals using this form of phishing, and instruct staff on what to do in the event of a particular type of phishing.
4. Conduct an exercise to identify types of phishing and propose measures necessary to ensure that staff understands the information provided and internalizes their knowledge of the area.
5. Simulation of a phishing attack in which emails are sent to employees to get important information from them. Thanks to the simulation, employees can safely familiarize themselves with the sequence of these types of attacks – it is important that the simulation takes place approximately 2-3 weeks after the training to verify the knowledge of the employees.
6. *It may be helpful to list notes in the public area of your company about phishing information that you have raised during the training.

How to recognize an e-mail phishing?

- Many phishing messages have incorrect grammar, punctuation, and spelling, or there are no Polish diacritics, e.g. "ą" "ę".
- Confirm that the e-mail comes from the organization that the sender refers to. Often the sender's e-mail address is completely unreliable, or it is not the same, for example, as the signature under the content of the e-mail.
- The assessment of the overall quality of the e-mail may come from the organization/company from which the e-mail should come, e.g. logos used, footers with the sender's data, etc.

- Is the email address with your first and last name, or does it refer to a "valued customer" "friend" or "colleague"? Not having an exact address could indicate phishing.
- Does the e-mail contain a hidden threat that requires immediate action? Be suspicious of words such as "send this data within 24 hours" or "you have been a victim of a crime, click here immediately".
- Look carefully at the sender's name to see if it looks real or just mimics someone you know.
- If the message sounds too good to be true, it usually is. It is unlikely that someone is willing to donate money or to give access to an unavailable part of the Internet.
- Your bank or any other institution should never ask for your data in an e-mail form.
- Public administration offices never ask via SMS or e-mails for an additional payment for a vaccine or paying your taxes.
- You should check any questionable commands or questions in the e-mail, for example by calling the bank asking if such a message was sent.
- Pay attention to links that are also passed between friends, does the link lead to the right page? Increasingly, criminals by gaining illegal control over social media accounts are impersonating friends and family.
- Be careful of shortened links, if you are unsure where the link will lead, just hover over the link (not clicking) and the full link address will be displayed at the bottom of the browser.

Simulation of a phishing attack

An interesting solution, recommended and used by IT security specialists, is to conduct a fake phishing attack. Such an attack may involve, for example, sending e-mails to employees, the purpose of which is to obtain important information from them. Thanks to the simulation, employees can safely familiarize themselves with the scheme of operation of this type of attack. They will see it live, without the unpleasant consequences of losing confidential information. On the other hand, people responsible for IT security in the company received, thanks to the simulation, a lot of useful information on the behavior of users, and thus - an excellent training material for the future. If employees do not pass the test, appropriate steps should be taken to train them.

We could use the service of hoxhunt which proposes offers for such a mock exam and are specialists in this field

2. Tech Solutions

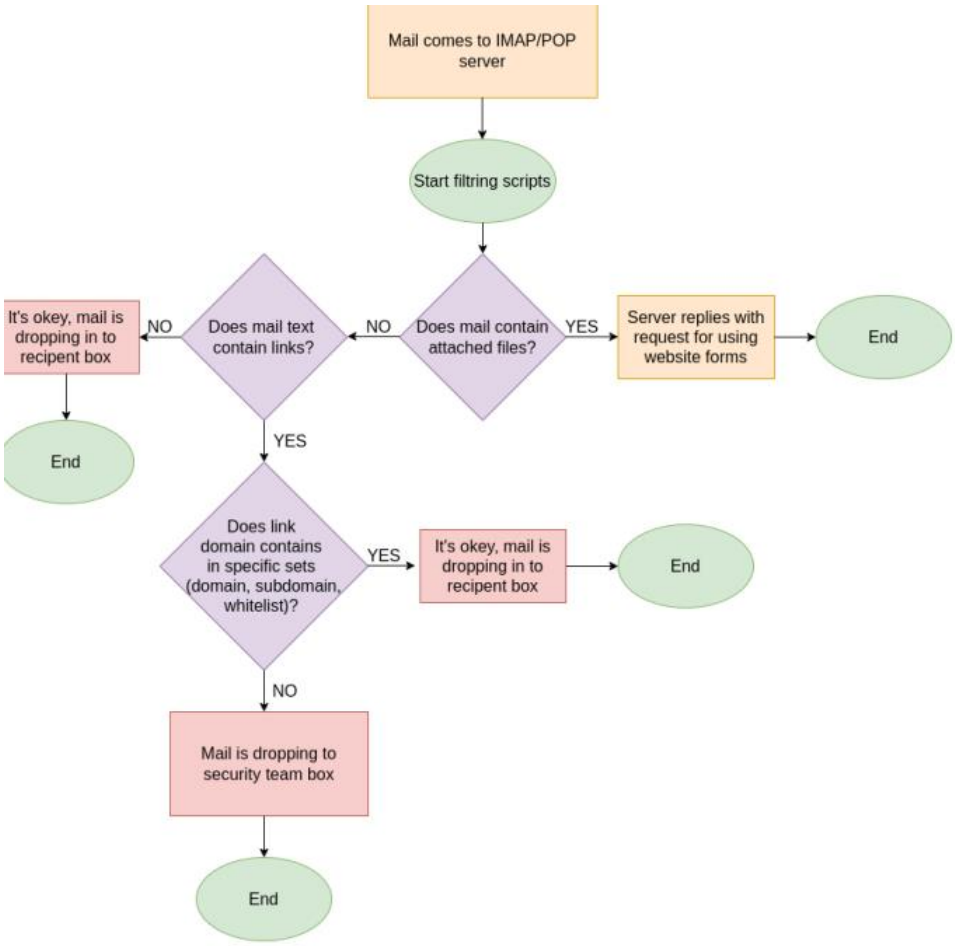
As every mail of every employee is a property of the Company, we can and should scan every mail that comes in. So here are some things that we would like to implement:

TLS Protocol

Only mails with TLS protocol should be allowed to be dropped in server

Mail-filtering script

Our company should create a "whitelist" which contains allowed domains that our employees can visit by clicking the link. We should create a script that will scan every email and look for links. This script should be running on the server before it comes to the receiver mailbox. If a link is from the company domain, subdomain, or whitelist it's okay. But if it does not contain in any of these 3 sets, we do not send this mail to the receiver, and we can send this to a special box that is handled by the specific person who will look at this mail closer.

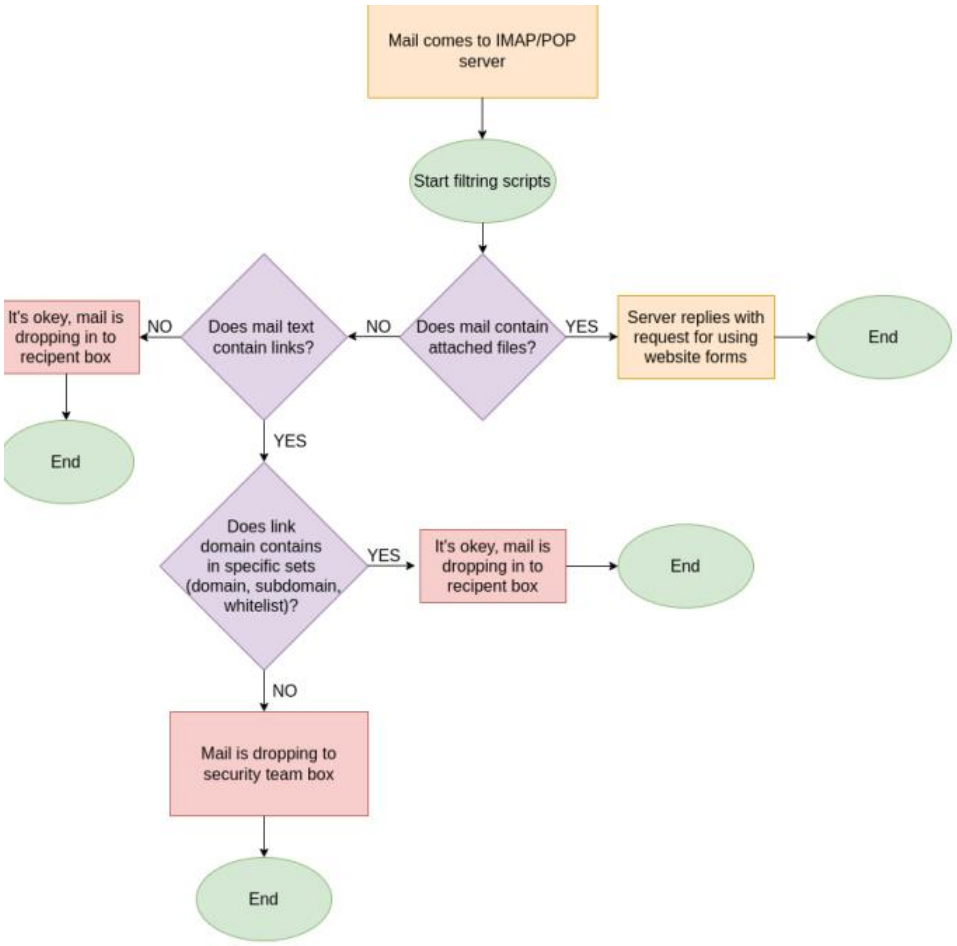


Enable receiving an attached file in mail

Hackers can hide malicious programs in files. As we want to avoid downloading these files to our environment, we decided to allow opening these files only on the website (as long as we do not click "download" viruses cannot install on our machine). To make that we decide to add special forms to our website, which should contain a lot of different cases), where clients or someone could add their file. To prevent receiving mails with attached files, we propose to: create another script, than would also scan emails from the server level (before being dropped into the receiver inbox) for attached files. If some file is attached, our server should reply to this mail with the message "please use the website form to contact us" Example: (for a good customer who only wants to return his product) We have a John, who bought shoes. But he has some complaints about them. He sent an email with attached photos of his faulty product. Our server got this email and scanned it. The script is found attached file. Now

server replies to John "please use website form". So John choose the website form for returning the case and attached this file there. Everyone is happy. Now let's consider a bad customer Tom, who does not want to return his product, but who wants to give the company malicious programs. The situation is identical to John's, but the virus cannot install itself on the employee machine and infect the company environment. The company is safe, and Tom is sad.

Presentation of how the whole system of checking mails should like:



User activity monitoring

Sometimes educating employees is not enough. It may be necessary to introduce special anti-phishing devices.

It seems a good idea to monitor the activity of computer users and record it in the form of video files. It is important that monitoring would be performed in real-time. Thanks to this, the person responsible for IT security will be able to control employees' lives, which gives the possibility of immediate reaction to a detected threat. When you see an employee doing something suspicious, you can block them, for example, preventing them from further activity on the computer.

Videos with user activity are also a great training material that can be presented to employees subject to "how not to do".