NoGo FallMaga

Phishing Handbook

tell two | cybersafe. FOUNDATION

Table of Contents

What is Phishing?

This is the practice of sending e-mails that appear to be from reputable sources with the goal of influencing or gaining personal information. The phishing email itself may be sent from a legitimate (although hacked or stolen) email address. Or it can be sent with a spoofed address, that is the sender's address looks legitimate, but it's actually from another address.

Phishing emails could have an attachment within the e-mail that loads malware (malicious software) onto your computer. It could also be a link to an illegitimate website. These websites can trick you into downloading malware or handing over your personal information.

Social Engineering

Phishing is a form of **Social Engineering** - psychological manipulation of people with the aim of getting them to reveal sensitive information or perform an action that is not in their best interest.

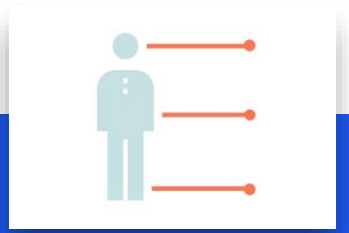
Information Targeted in Phishing Attempts

User Credentials

Usernames and passwords that can be used into personal and work accounts

Email Addresses

This could be for colleagues or family members that can be used to send more convincing phishing emails.



Personal Information

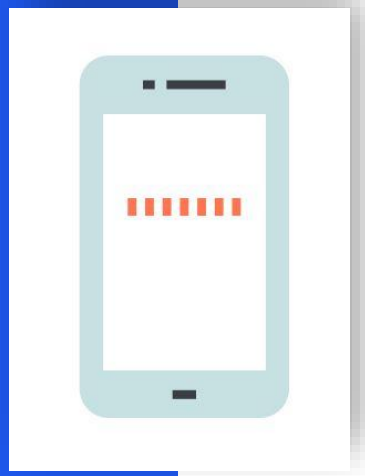
Such as names, physical addresses, birthdays, National Identification Number, etc. This can be used for fraud, identity theft or other social engineering scams.

Confidential Company Information

Such as details about research and development, trade secrets or other information that can give a competitive advantage.

Financial Data

Such as debit/credit card numbers, BVN, Bank account numbers, tax information that could be used to commit fraud and steal money.



Phone Numbers

That can be used to bypass two-factor authentication, as well as deliver SMS based phishing campaigns.

Types of Phishing

Phishing Emails can be grouped into two broad categories:

Non Targeted - These are phishing emails sent to a large number of recipients. The aim of they cybercriminals is to cast the net as wide as possible with the hope that some of the recipients will respond.

Targeted - These are phishing emails sent to a specific individual or group of people after research has been done to create a message that is personal, relevant and likely to evoke a reaction.

Non Targeted Phishing

Common non targeted phishing emails are advanced fee scams and emails impersonating IT Support/Service providers. The email shown is an advanced fee scam email.

Subject [redacted] 2021 Investment Opportunity
From The Atlantic Finance <office@ensspms.com>
To <connect@[redacted]org>
Reply-To The Atlantic Finance <marketing.erssystem@gmail.com>
Date 2021-05-21 11:52

Attn connect@[redacted]org
CEO / Manager

Greetings,

I am Mr. Robert Creighton Member Board of Directors of Atlantic Finance Company, USA I have a great Investment offer for you, a wealthy customer of ours who is from England died due to COVID19 leaving behind £75,000,000.00 GBP (Seventy Five Million GBP) which is approximately $115,000.000.00 USD (One Hundred and Fifteen Million USD) for Investment.

He had no next of kin to the inheritance and I am contacting you today because you can inherit this fortune through some legal processing means, because you share the same last name and with the help of the deceased personal lawyer he will prepare all necessary legal binding documents as next of kin, Power of Attorney that will enable this fortune mentioned released to you for investment if you accept this offer.

If you agree to this proposal the amount $58,000,000.00 USD (Fifty Eight Million USD) will be transferred to you for Investment via MTC103 wire transfer, So if you are interested, Kindly get back to me urgently so that I can furnish you with relevant details/documents for you to proceed with the legal binding documents for you to sign as next of kin.

This is a great opportunity of a lifetime and it is my pleasure to work with you so we can invest this fund properly. I will need acceptance letter from you or email with your company letter headed paper so that I will do a change of ownership of this investment fund to your company name after we both might seen face to face and agree and have sign (MOU) before we start this investment job and we need to agree on certain percentage before we start this transaction.

I look forward to your quick anticipation.

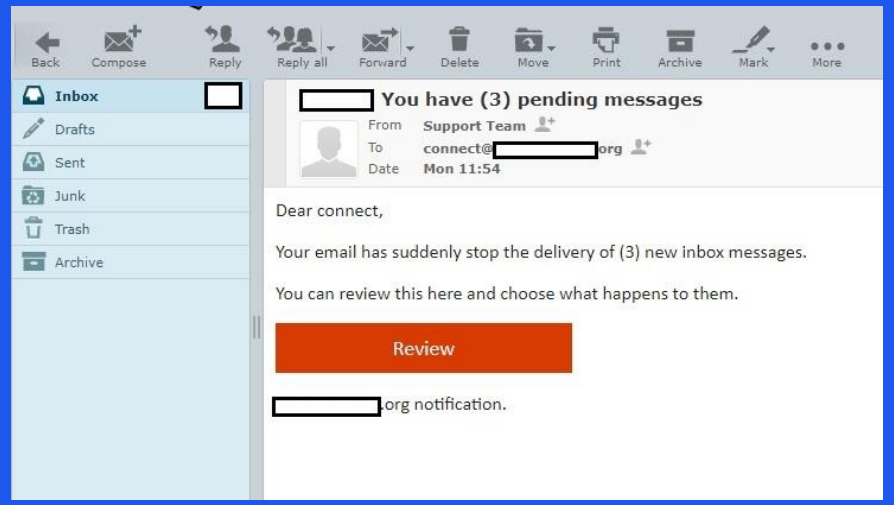
Telephone :- +1 970 724 4058
Email:- theatlanticfinance@gmail.com

Yours Faithfully,

Robert Creighton
Member Board of Director.
Atlantic Finance Company, USA.

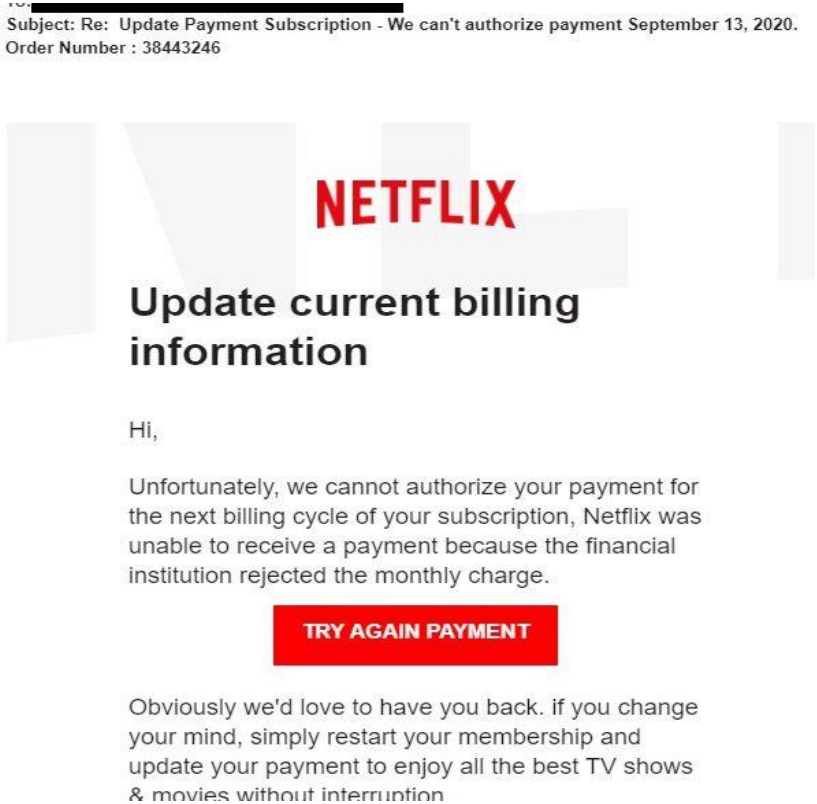
These type of scam emails typically involve promising the victim a share of a large sum of money for helping to hold, process or transfer it. The pretext is that someone wealthy had died of covid, and someone is needed to pose as a next of kin to claim the cash. As always, in the cause of trying to get the money, the need to pay several fees, whether to bribe someone, or for documents as to process the transfer will arise.

Another example of a non targeted phishing email is the IT support scam email. In this scenario the cybercriminal sends and email impersonating IT support claiming some problem has arisen and you're to perform an action to resolve it.



In the example above, the pretext is the non delivery of messages and the victim is told to click a link to review. The link might lead to a page that downloads malware on the victims device or is a clone of login page of a service in order to steal the victim's login credentials.

Another very popular non targeted phishing email is the service provider phishing email scam. In this scenario, the cybercriminal impersonates a service used by a lot of people. The aim is to steal login credentials or card details. Below is an example.



In the example above, the cybercriminal uses the company logo and a pretext of a failed subscription to try to get the victim to click a link. This link would lead to a look alike Netflix website where the victim would then be asked to input their card details so it can be stolen.

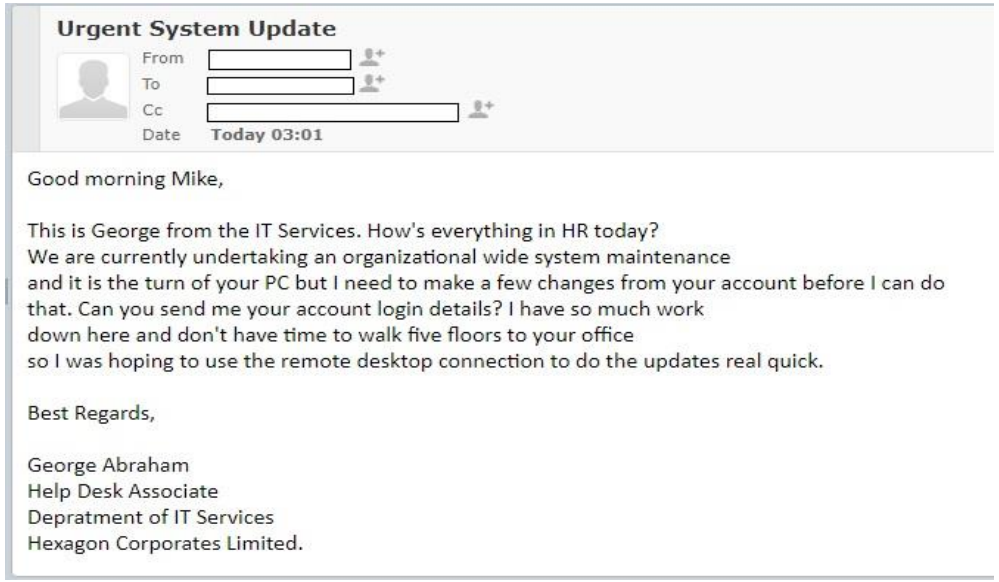
Targeted Phishing

Two popular targeted phishing methods are Spear Phishing and CEO fraud.

Spear Phishing

Spear phishing refers to phishing attacks that are designed and sent to target a specific person, business, or organization. If a criminal seeks to obtain credentials into a specific company's email system, for example, he or she may send emails crafted specifically for particular targeted individuals within the organization. Often, criminals who spear phish research their targets online and leverage overshared information on social media in order to craft legitimate-sounding emails.

Here's an example of a spear phishing email.

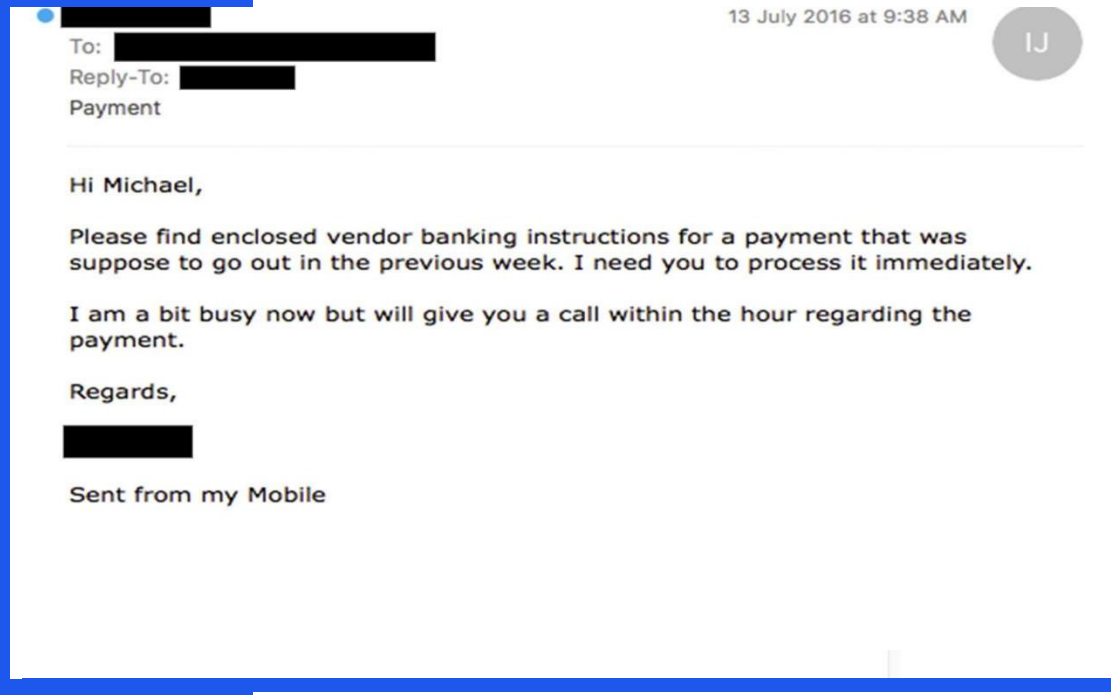


In the above example, the cybercriminal has done his homework. He found someone in the IT department to impersonate and knows the name of someone in HR to target. Also he uses details such as the distance from the IT department to HR to build trust and make the email look more legitimate-sounding.

CEO Fraud

This is when a cybercriminal impersonates a top executive of a company (usually a CEO, CFO, COO) and asks a lower lever employee (usually in Finance or Accounting) of the company to perform an action such as sending money to an account.

This form of phishing often nets significant returns and has the downside of making the employee who falls for it look incompetent and in some occasions may cost the employee their job.


[redacted]
13 July 2016 at 9:38 AM
IJ
To: [redacted]
Reply-To: [redacted]
Payment

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

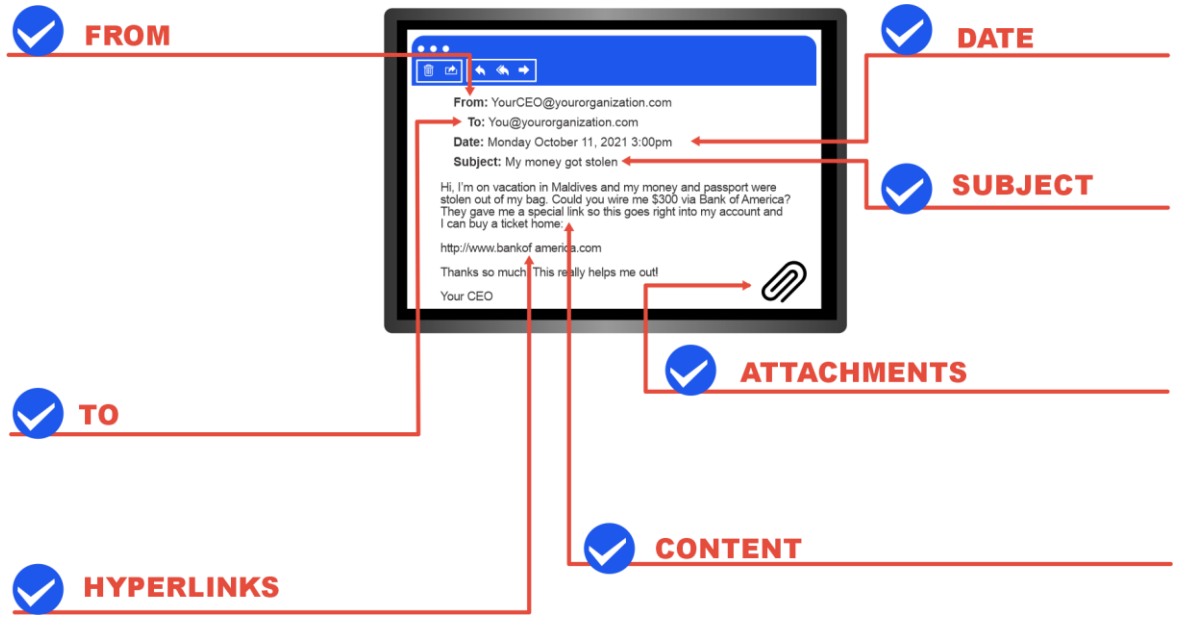
Regards,

[redacted]

Sent from my Mobile

The Anatomy of a Phishing Email

Having been acquainted with phishing and its various forms, we will now concentrate on the various parts of an email that can serve as indicators, so as to be better equipped to spot phishing emails.



Subject

The thing to look out for in the subject of an email is if it matches the content of an email. Also, you should check to see if it is a response to something you sent. If the content of the email is about something else other than the stated subject, and it arrives out of the blue, then you should be very suspicious.

From

The is the field for the email address of the sender. Below are a list of things you should be on the look out for:

- Do you recognize the sender's email address as someone you communicate with?
- If it's your work email, is the email from someone outside your organization and not related to your work activities?
- If it's from someone you know (family, boss, colleague, vendor, customer), is the email very unusual and out of character?
- Is the senders email address from a suspicious domain? E.g. bank.axing.nfb.com

Something else to keep in mind is that even if all the conditions above are satisfied, the email address could be spoofed. Email spoofing is when the sender's address is forged.

To

This is the field for the recipient(s) email address. Typical red flags are:

- You were copied on an email sent to one or more people but you don't personally know the other people.
- You received an email sent to an usual group of people. For instance, a random group of people in your organization whose names begin with the same letter or a list of unrelated addresses.
- The email address on the To field isn't yours, meaning you were blind copied.

Date

This is the day and time the email was received. A typical red flag is receiving an email at an usual time, for instance receiving an email from a vendor that usually sends emails during business hours at 2 AM.

Hyperlink

These are the clickable links in an email. The typical red flags are:

- You hover over the link with your mouse and the destination domain displayed is different from domain of the link
- You receive an email with a very long hyperlink such that you cannot see the full domain
- You receive an email with a hyperlink that is a misspelling of a known brand e.g. rnicrosoft.com instead of microsoft.com - "r" and "n" are used together to look like "m."

Content

This is the body of the email which comprises the message. Typical red flags are:

- You receive an email with bad grammar and spelling errors
- You receive an email that conveys fear and urgency - you're asked to perform an action such as clicking a link or downloading an attachment before a certain time or else a negative consequence would occur.
- You receive an email promising a reward for taking an action

Attachments

A popular use of email is to distribute files, this done by attaching it to the email and sending. Unfortunately cybercriminals has been exploiting this to send people malware as attachments. Here are the typical red flags:

- The sender of an email includes an attachment you were not expecting
- The attachment ends with an extension such as ".exe" ".dmg" ".html" or others you don't recognize

Generic Greeting

If an email is supposedly from a company of individual you have an established relationship with then they should address you by name. A general salutation like "Dear Customer" as we have in our example above is a huge red flag. Note that for spear phishing emails, the cybercriminals might not use a generic greeting because they would have done their research
about you.

Protecting Against Phishing

Be cautious about clicking links in emails

Always bear in mind that a web address may not be what it appears to be in an email. Instead of clicking a link in an email to take you to where you can login, it is better you open a web browser and type in the domain yourself.

Be cautious about downloading attachments in emails

A good rule of thumb is never to open any attachment you didn't explicitly ask for, If in doubt, contact the sender first (via phone or some other means) to confirm the authenticity of the email.

Beware of urgent requests, gifts or money orders.

Messages that appear to be urgent requests for either immediate payment, updates to your account, password changes, etc, play on the reactive emotional response of a user to get information from them quickly. Also, watch out for messages offering gift cards or saying you've won a prize. This is baiting, and the aim is to use the promised item to trick you into clicking a link or taking some other action.

When in doubt, contact the sender

If you're able to, verify that the sender actually sent you the message in question by asking them in person or over a different messaging service, or call them

Use Two-Factor Authentication

Make sure you're using two-factor authentication on your email as well as all other online accounts.

Keep Devices and Software up to date

Software and devices may send updates from time to time. Make sure all such updates are downloaded and installed.

Use an email security solution

Consider using an email security solution that can scan inbound emails and also stop spam and phishing scams from hitting your inbox.