



Phishing- Email Analysis

Introduction to Phishing

- ❖ **Phishing attack** is a type of attack aimed at stealing personal data of the user in general by clicking on malicious links to the users via email or running malicious files on their computer.
- ❖ **Phishing attacks** correspond to the "**Delivery**" phase in the **Cyber Kill Chain** model created to analyze cyber-attacks. The delivery stage is the step where the attacker transmits the previously prepared harmful content to the victim systems / people.

Phases of the Intrusion Kill Chain



The Phishing attack is the most common attack vector for initial access. Of course, the only purpose of the attack is not to steal the user's password information.

The purpose of such attacks is to exploit the human factor, the weakest link in the chain. Attackers use phishing attacks as the first step to infiltrate systems.

What is phishing email analysis?

Phishing email analysis involves studying the content of phishing emails to ascertain the techniques the attacker used.

What is a common indicator of a phishing email?

Common indicators of a phishing email include suspicious addresses, links, or domain names, threatening language or a sense of urgency, errors in the email, the inclusion of suspicious attachments, and emails requesting sensitive information.

Elements of a phishing email

All phishing emails include one of two components: a link or an attachment. Getting victims to click the link or open the attachment requires a sophisticated set of tools and techniques. Below are some of the most important elements of a phishing email:

Subject line

Perhaps the most critical element of a phishing email, the subject line is designed to entice, alarm, or frighten the victim into opening the email. Hackers who have done their research write highly targeted subject lines to entice victims into opening emails.

Email spoofing

Email spoofing involves creating an email address that looks like that of a trusted business. With display name spoofing, the hacker adds the desired display name in the sender field of the email. In other cases, a hacker will use an email address resembling a legitimate business email as the display name.

Brand impersonation

Hackers impersonate the brands you trust the most. When attacking businesses, hackers impersonate brands that a business has a relationship with, such as a bank or a software vendor. To create the illusion of legitimacy, phishers use real business and product logos and other visual elements of the brand's identity.

Phishing link

A link is typically placed in the body of the email, but it can also be placed inside an attachment or inside a legitimate hosted file on a service like OneDrive or SharePoint to avoid detection from email filters scanning for known phishing links. Victims are lured into clicking on the link by the email itself, which directs the user to visit a website to log into an account.

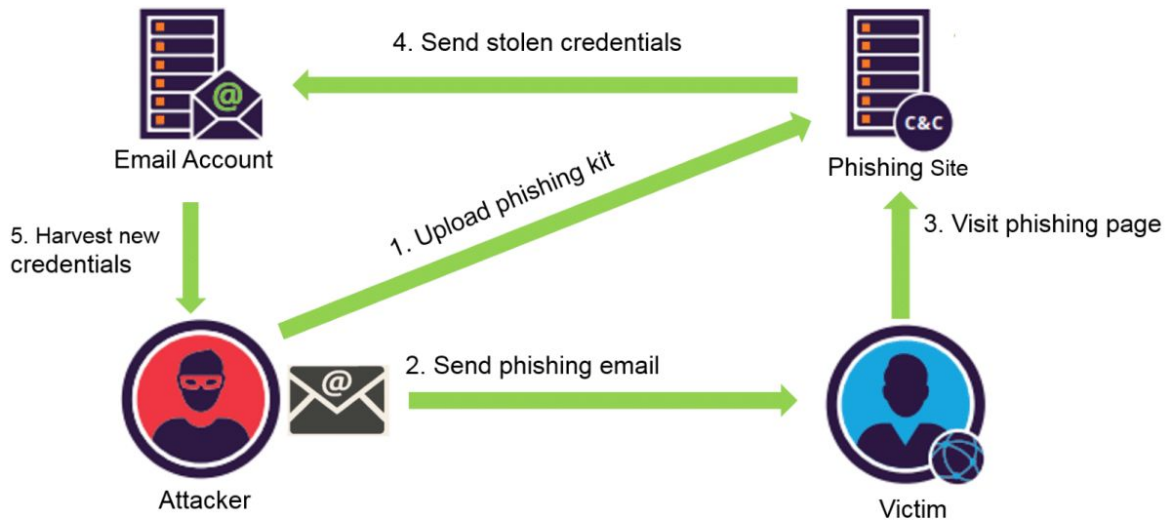
Attachment

Attachments are included either to conceal the phishing link from an email filter or to deliver malware/ransomware. Often in the form of a Word document, PDF, or .zip file, the attachment appears to be legitimate business correspondence, such as an invoice. The link might lead to a phishing website or result in an automatic download of malware or ransomware.

Phishing page

A phishing page is a fraudulent webpage that impersonates a brand. Unsophisticated pages are easy to spot, but advanced phishers use real CSS from brand webpages to make their webpages identical to the real thing. Phishing pages impersonate login pages where victims enter their username and password to access their account. When they do so, their credentials are stolen.

Phishing attack flow



EXAMPLE OF PHISHING EMAIL

EXAMPLE OF PHISHING EMAIL

Fri 12/11/2015 10:33 AM

Urgency

Critical System Maintenance Team <noreply@csmt.com>

URGENT: Critical System Maintenance - Validate user account

To: [Redacted]

Follow up. Start by Friday, December 11, 2015. Due by Friday, December 11, 2015.
This message was sent with High importance.

Dear user,

We are about to carry out maintenance on our user interface. Upon the receipt of this notice, you are required to validate users can access the interface.

Failure to validate account functions within this time duration, will inactive all user accounts.

To validate the user interface, click on the web-link below or copy the link in your web-browser:

<http://reviewuserinterface.com/verify>

Yours in service,
Critical System Maintenance Team

Annotations:

- Not sent to you.
- Not addressed directly to you.
- Generic reference to unidentified system.
- Contains 'threat' if you don't act on email.
- Attempts to direct you to a link

Information Gathering

Spoofing

Attackers can send emails on behalf of someone else, as the emails do not necessarily have an authentication mechanism. Attackers can send mail on behalf of someone else using the technique called spoofing to make the user believe that the incoming email is reliable.

Several protocols have been created to prevent the Email Spoofing technique. With the help of **SPF, DKIM and DMARC** protocols, it can be understood whether the sender's address is fake or real. Some mail applications do these checks automatically. However, the use of these protocols is not mandatory and in some cases can cause problems.

- **Sender Policy Framework (SPF)**
- **DomainKeys Identified Mail (DKIM)**

To find out manually whether the mail is spoof or not, SMTP address of the mail should be learned first. **SPF, DKIM, DMARC and MX records** of the domain can be learned using tools such as Mxtoolbox. By comparing the information here, it can be learned whether the mail is spoof or not.

The screenshot shows the SuperTool Beta7 interface. At the top, there is a search bar with 'umuttosun.com' entered. Below the search bar, there is a dropdown menu with 'MX Lookup' selected. The main content area displays the results for 'mxumuttosun.com'. It includes a table with columns 'Pref', 'Hostname', and 'TTL'. The table shows one record with Pref '0' and Hostname 'umuttosun.com'. Below the table, there is a 'Test' section with a table showing the results of various tests. The tests include DMARC Record Published (failed), DMARC Policy Not Enabled (failed), and DNS Record Published (passed). The results section also shows 'No DMARC Record found', 'DMARC Quarantine/Reject policy not enabled', and 'DNS Record found'.

Pref	Hostname	TTL
0	umuttosun.com	4 hrs

Test	Result
DMARC Record Published	No DMARC Record found
DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled
DNS Record Published	DNS Record found

Since the IP addresses of the big institutions using their own mail servers will belong to them, it can be examined whether the SMTP address belongs to that institution by looking at the **whois** records of the SMTP IP address.

An important point here is that if the sender address is not spoof, we cannot say mail is safe. Harmful mails can be sent on behalf of trusted persons by hacking corporate / personal email addresses. This type of cyber attacks has already happened, so this possibility should always be considered.

E-mail Traffic Analysis

Many parameters are needed when analyzing a phishing attack. We can learn the size of the attack and the target audience in the search results to be made on the mail gateway according to the following parameters.

- **Sender Address**
- **SMTP IP Address**
- **Email Address Domain**
- **Subject (sender address and SMTP address may be constantly changing).**

In the search results, it is necessary to learn the recipient addresses and time information besides the mail numbers.

If harmful e-mails are constantly forwarded to the same users, their e-mail addresses may have leaked in some way and shared on sites such as [PasteBin](#).

Attackers can find email addresses with [theHarvester](#) tool on Kali Linux. It is recommended that such information should not be shared explicitly, as keeping personal mail addresses on websites would be a potential attack vector for attackers.

If mails are sent out of working hours, the attacker may be living on a different time-zone line. By gathering such information, we can begin to make sense of the attack.

What is an Email Header and How to Read Them?

In this section, we will explain what the header information in an email is, what can be done with this information and how to access this information. It is important to follow this section carefully as we will explain how to perform the header analysis in the next section.

What is an Email Header?

"Header" is basically a section of the mail that contains information such as sender, recipient and date. In addition, there are fields such as "Return-Path", "Reply-To", and "Received". Below you can see the header details of a sample email.

```
Delivered-To: info@letsdefend.io
Received: by 2002:ab4:8fc7:0:0:0:0 with SMTP id cs7csp1721687ecb;
..... Mon, 21 Mar 2022 06:10:11 -0700 (PDT)
X-Received: by 2002:a05:620a:2416:b0:67d:7735:4bbf with SMTP id d22-20020a05620a241600b0067d77354bbfmr12659013qkn.501.1647868211414;
..... Mon, 21 Mar 2022 06:10:11 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1647868211; cv=none;
..... d=google.com; s=arc-20160816;
..... b=2xH9+3UjmlxSK/Y/LeaLuupLgQT9gWm71ZagKamcTCU/4Tp5WIYpwXZe7PKv4gz30h
..... 4jUc3QKlzm18KREmbs4RRQz8E7Varx+b2ZpejUitxWixYcoOWt25rWx1UnUU29vdT
..... OuGxWQYjqfJLoQeaDRSPoaFWKBrLbgfluZv7R5A9sYjVgf9jE/Jfy2HqBiHWvK/Z6v55
..... FH7TBavChCadh7ronXI4FfggfvGh7yEako6qHmnTWA3CsuseMKh18P4M2ZLNAMtx2t0
..... Ej5MiiMBBR/nJjetLwcuyNh37acMD7fuB4Atsu+4FS4sa8dFA9JSwR7wAUNT4Znh7bG
..... vlpq==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
..... h=mime-version:delivered-to:date:message-id:subject:to:from
..... :dkim-signature;
..... bh=HIAfOlDaK3JQlPh5fJuRxiIvU9cb88FSU4V8M1V9sI=;
..... b=DQbcXx7COpYCaegIw+c82nMDSTR6SGHNR4p+jqBAgtdIm3/TXsiJwKXJv/Yj6HRp9
..... YNm2RuORlLdajcHuklcl7wngpflP2678iuQsZvzPBFEbmgjRZbh/2OeIaNBpkEMzLaDo
..... 4a6MNUZl/DJmLVQokqQ7s5hYePucKTGhpziJQDC/7aubWiaXuOzwXvNt9V2GsHoxvRr
..... dph2LsXWADYDc6sAGCtWR7wIve4zoDBw/evWoH/g55aChuX8KGB7OPuP3G12fo0F296
..... EAVSovT/zvPl0/MN6oaSOWIYoYshyKm36ceOtbFZLqDYhxsID+NeXEk8seecPz14LGg
..... lNEg==
ARC-Authentication-Results: i=1; mx.google.com;
..... dkim=pass header.i=@letsdefend.io header.s=google header.b=hRMogQ3u;
..... spf=pass (google.com: domain of ogunal@letsdefend.io designates 209.85.220.41 as permitted sender) smtp.mailfrom=ogunal@letsdefend.io
Return-Path: <ogunal@letsdefend.io>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
..... by mx.google.com with SMTPS id d7-20020ac8544700000b002de980041b8sor9866778qtq.15.2022.03.21.06.10.11
..... for <info@letsdefend.io>
..... (Google Transport Security);
..... Mon, 21 Mar 2022 06:10:11 -0700 (PDT)
Received-SPF: pass (google.com: domain of ogunal@letsdefend.io designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
..... dkim=pass header.i=@letsdefend.io header.s=google header.b=hRMogQ3u;
..... spf=pass (google.com: domain of ogunal@letsdefend.io designates 209.85.220.41 as permitted sender) smtp.mailfrom=ogunal@letsdefend.io
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
..... d=letsdefend.io; s=google;
..... h=from:to:subject:message-id:date:delivered-to:mime-version;
..... bh=HIAfOlDaK3JQlPh5fJuRxiIvU9cb88FSU4V8M1V9sI=;
..... b=hRMogQ3uKl9FSba7f/JLWB2QkC0Rr8IR6YqQBj1HTp9egr9Vwpc6qHPYHskxOdgT0
..... 7vwxxkHhRBLJWgJqXeVv+MNBXKLK52fiLw3B3esnnMdrmyysJLuRuvyRV2LakLqY9gCc
..... lW0yolWFT/990p5h4GqMJOPSYQLPbZTWJEWc2UdfChte4YHuxB1PUVZ26lwhpbqNdxGy
..... jCKBbl14DN0AM3olu5tu6hVZr6kgreS7TTrShGz/73bTM0JnoExH/XU+V8RmYP60ei3Av
```

What does the Email Header do?

A. Enables Shipper and Recipient Identification

- Thanks to the "From" and "To" fields in the header, it is determined from whom an email will go to whom. If we look at the email above that you downloaded in "eml" format, we see that it was sent from the address ogunal@letsdefend.io to info@letsdefend.io

```
From: Omer Gunal <ogunal@letsdefend.io>
To: Letsdefend IO <info@letsdefend.io>
Subject: Example subject
```


B. Spam Blocker

- It is possible to detect spam emails using **Header analysis** and other various methods. This protects people from receiving SPAM emails.

C. Allows Tracking an Email's Route

- **It is important to check the route it follows to see if an email came from the right address.** If we look at the sample email above, we see that it came from the ogunal@letsdefend.io address, but did it actually come from the **letsdefend.io** domain or from a different fake server that mimics the same name? We can use the header information to answer this question.

Important Email Header Fields

From

- ❖ The "From" field in the internet header indicates the name and email address of the sender.

To

- ❖ This field in the mail header contains the email's receiver's details.
- ❖ It includes their name and their email address. Fields like CC (carbon copy) and BCC (blind carbon copy) also fall under this category as they all include details of your recipients.
- ❖ If you want to find out more about carbon copy and blind carbon copy, check out how to use CC and BCC.

Date

- ❖ This is the timestamp that shows when the email was sent.
- ❖ In Gmail, it usually follows the format of "day dd month yyyy hh:mm:ss".
- ❖ So if an email had been sent on the 16th of November, 2021, at 4:57:23 PM, it would show as Wed, 16 Nov 2021 16:57:23.

Subject

- ❖ The subject mentions the topic of the email. It summarizes the content of the entire message body.

Return-Path

- ❖ This mail header field is also known as Reply-To. If you reply to an email, it will go to the address mentioned in the Return-Path field.

Domain Key and DKIM Signatures

- ❖ The Domain Key and Domain Key Identified Mail (DKIM) are email signatures that help email service providers identify and authenticate your emails, similar to SPF signatures.

Message-ID

- ❖ The Message ID header field is a unique combination of letters and numbers that identifies each mail. No two emails will have the same Message ID.

MIME-Version

- ❖ Multipurpose Internet Mail Extensions (MIME) is an internet standard of encoding. It converts non-text content like images, videos, and other attachments into text so they can be attached to an email and sent through SMTP (Simple Mail Transfer Protocol).

Received

- ❖ The received field lists each mail server that went through an email before arriving in the recipient's inbox. It's listed in reverse chronological order — where the mail server on the top is the last server the email message went through, and the bottom is where the email originated.

X-Spam Status

- ❖ The X-Spam Status shows you the spam score of an email message.
- ❖ First, it'll highlight if a message is classified as spam.
- ❖ Then, the spam score of the email is shown, as well as the threshold for the spam for the email.
- ❖ An email can meet either the spam threshold of an inbox or exceed it. If it's too spammy and exceeds the threshold, it will automatically be classified as spam and sent to the spam folder.

Reference of Field Definitions: gmass.co

How to Access Your Email Header?

Gmail

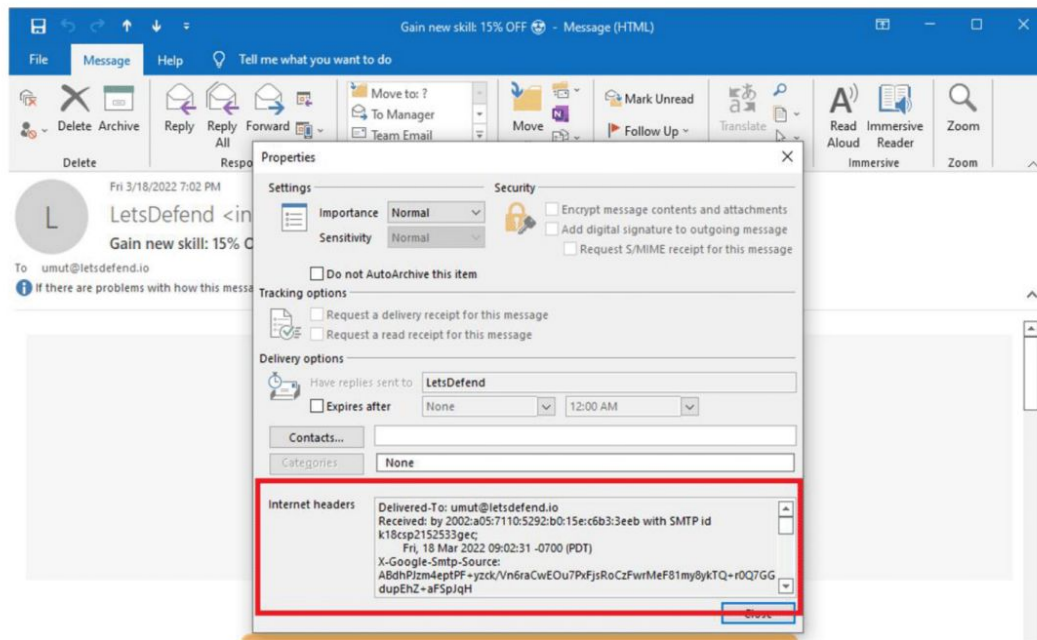
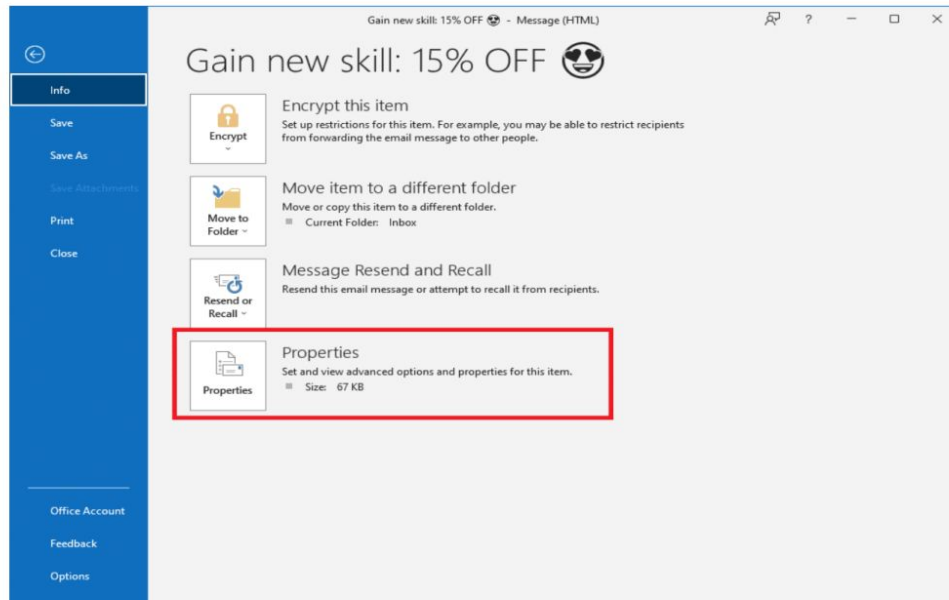
- 1- Open the relevant e-mail
- 2- Click on the 3 points at the top right "..."
- 3- Click on the "Download message" button.



4- Downloaded ".Open the file with the extension ".eml" with any notebook application

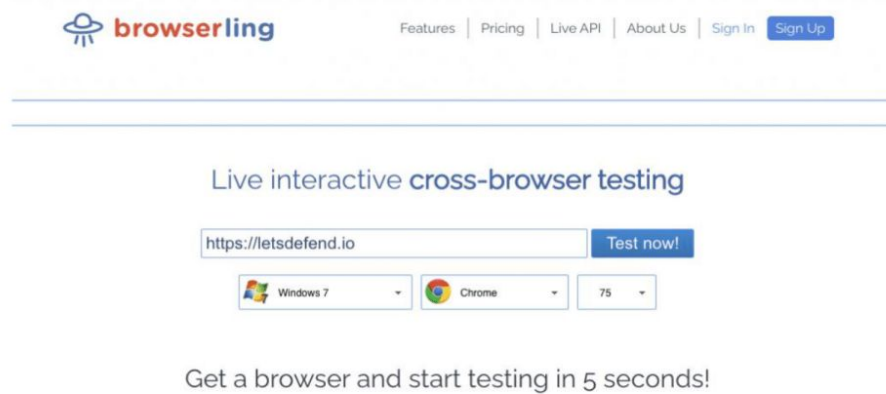
Outlook

- 1- Open the relevant e-mail
- 2- File -> Info -> Properties -> Internet headers



Dynamic Analysis

URLs and files can be found in the mail. These files and URL addresses need to be examined. You don't want your data to be stolen by hackers by running these files on your personal computer. For this reason, the websites and files in the mail should be run in sandbox environments and the changes made on the system should be examined, and it should be checked whether they are harmful or not.



If you want to quickly check the web addresses in the mail, you can see the content of the website using online web browsers such as [Browserling](#). The good thing about such services is that you will not be affected by a possible zero-day vulnerability that affects browsers, since you do not go to the web page on your own computer.

The disadvantage of using web browsers such as [Browserling](#) is that if the malicious file is downloaded on the site, you cannot run this file. For this reason, your analysis will be interrupted.

Sandbox Environment for Email Header Analysis

You can examine suspicious files and websites in sandbox environments. When you examine the files in these environments, you remove the risk of infecting your computer with malware. Many sandbox services / products are available. These products / services are available for paid and free use. You can choose one / more of these services according to your needs.

A few commonly used sandboxes:

- ❖ VMRay
- ❖ Cuckoo Sandbox
- ❖ JoeSandbox
- ❖ AnyRun
- ❖ Hybrid Analysis(Falcon Sandbox)

NOTE

- ❖ Malware can wait for a certain period of time without any action to make detection difficult. You must wait for the malware to work before you decide that the examined file is not harmful.
- ❖ The fact that there are no urls and files in the mail does not mean that this is not harmful. The attacker can also send it as a picture so as not to get caught up in the analysis products

Additional Techniques

Another technique that attackers use is to perform phishing attacks using normally legal sites. Some of them are as follows.

A. Using services that offer Cloud Storage services such as Google and Microsoft

Attackers try to click on Google / Microsoft drive addresses that seem harmless to the user by uploading harmful files onto the drive.

B. Using services that allow creating free subdomains such as Microsoft, Wordpress, Blogspot, Wix

Attackers try to deceive security products and analysts by creating a free subdomain from these services. Since whois information cannot be searched as a subdomain, it can be seen that these addresses were taken in the past and belongs to institutions such as Microsoft, WordPress.

C. Form applications

Services are available that allow free form creation. Attackers use these services instead of creating a fishing site themselves. Since the domain is harmless under normal conditions, it can pass on to the user without getting stuck on antivirus software. Google Form is an example of these services. When looking at whois information, the domain can be seen to be Google, so the attacker can mislead analysts.

Hand-on Practice Lab with SOC Alerts on LetsDefend Platform

- 93 - SOC146 - Phishing Mail Detected - Excel 4.0 Macros
- 82 - SOC140 - Phishing Mail Detected - Suspicious Task Scheduler
- 45 - SOC114 - Malicious Attachment Detected - Phishing Alert
- 52 - SOC120 - Phishing Mail Detected - Internal to Internal
- 86 - SOC141 - Phishing URL Detected

Social Engineering Red Flags



FROM

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



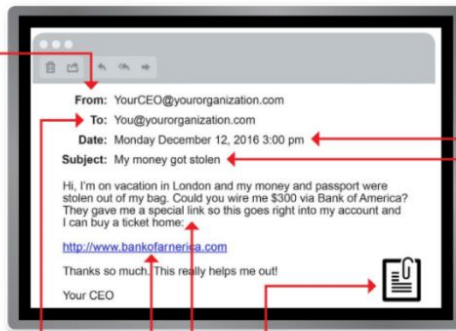
TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.



HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofamerica.com — the "m" is really two characters — "r" and "n."



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?



SUBJECT

- Did I get an email with a subject line that is **irrelevant or does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?



ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt file**.



CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar or spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd or illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

DEFENSIVE PROTECTIVE MEASURES

Some defensive layers to take into consideration to assist in preventing email phishing attacks and credential stealing from phishing attacks would be:

- **Email scanning and filtering**
- **Email security gateways**
- **DNS authentication (DMARC, DKIM, and SPF)**
- **Anti-malware and anti-spam**
- **Multi-factor authentication (MFA)**
- **Phishing security awareness**

No matter how robust the email defensive layers are, phishing emails will find their way into a user's mailbox. In the end, the user is the last measure in these defensive protection layers, and they are only as strong as the effectiveness of the phishing security awareness training provided by the organization.
