Forage

THE BEST RUN SAP®

SAP CYBERSECURITY VIRTUAL INTERNSHIP PROGRAM

Task 2 - Gone Phishing.

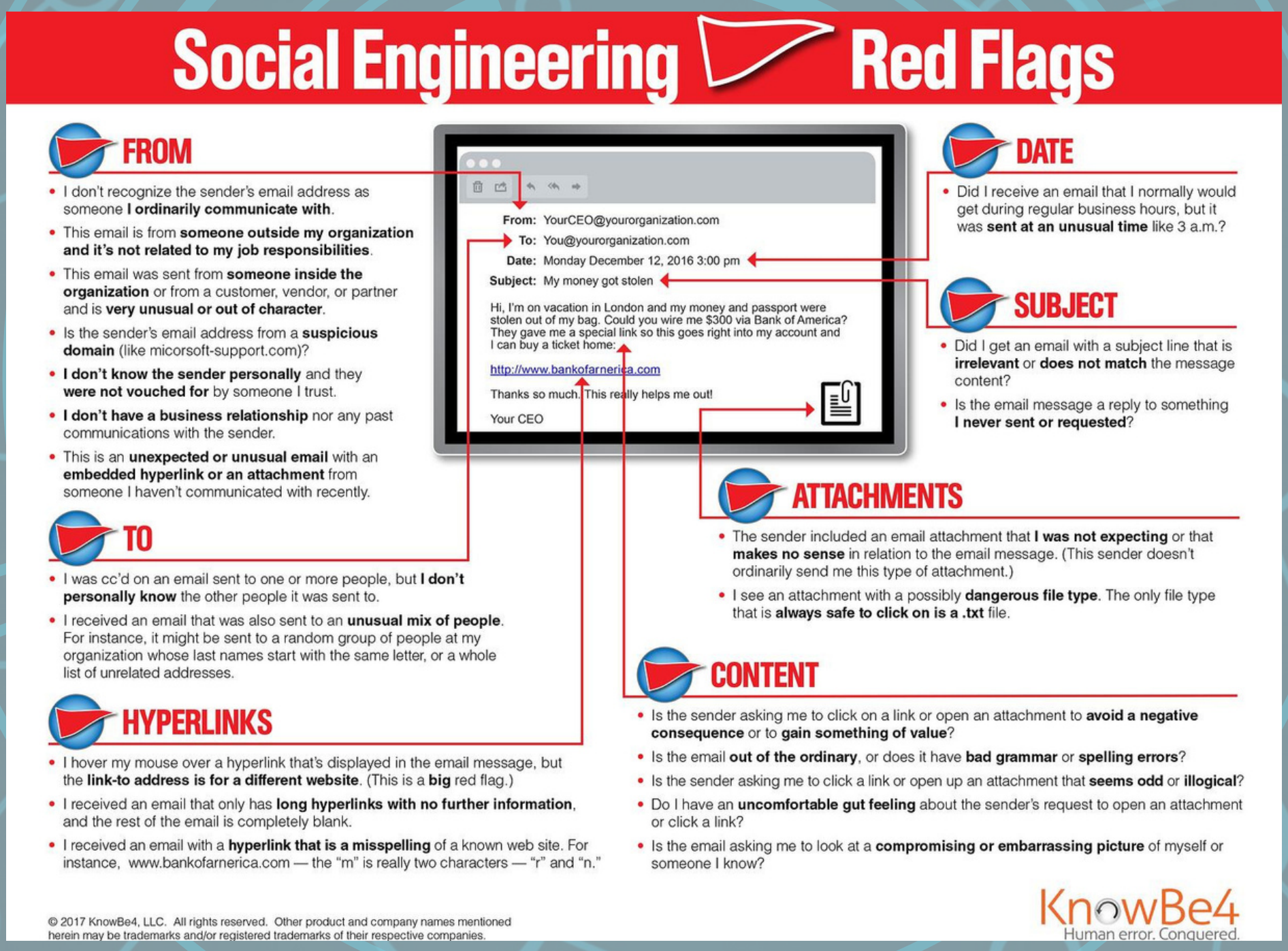
Identify and mitigate phishing attempts for your client!

Pablo Gagliardi

THE BEST RUN SAP®

Forage

Social Engineering Red Flags review.



How to identify phishing scams?

Here are some common red flags to look out for:

1. The sender's email address is unfamiliar or suspicious-looking.
2. The message contains urgent or threatening language to create a sense of panic.
3. The message asks you to provide personal or sensitive information, such as passwords or financial details.
4. The message includes a link to a website that looks similar to a legitimate site but has a slightly different URL.
5. The message contains spelling and grammar errors or appears unprofessional.

If you receive an email that exhibits any of these red flags, it's best to avoid responding or clicking on any links and instead report it to the relevant authorities or contact the company directly to verify the message's legitimacy.

THE BEST RUN SAP®

Forage

NIST tips and tactics for dealing with ransomware review.

https://www.nist.gov/news-events/news/2021/05/nist-releases-tips-and-tactics-dealing-ransomware

NIST National Institute of Standards and Technology U.S. Department of Commerce

NEWS (https://www.nist.gov/news-events/news)

NIST Releases Tips and Tactics for Dealing With Ransomware

May 13, 2021

Used in cyberattacks that can paralyze organizations, ransomware is malicious software that encrypts a computer system's data and demands payment to restore access. To help organizations protect against ransomware attacks and recover from them if they happen, the National Institute of Standards and Technology (NIST) has published an infographic (https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST_Ransomware_Tips_and_Tactics_Infographic.pdf) offering a

The"NIST Releases Tips and Tactics for Dealing With Ransomware." provides an overview of the threat of ransomware attacks and offers recommendations for mitigating the risks.

The document is well-organized and easy to read. It starts with an introduction that explains the basics of ransomware and how it works. It then proceeds to describe the tactics that attackers use to deliver ransomware, such as phishing emails, exploit kits, and remote desktop protocol (RDP) attacks.

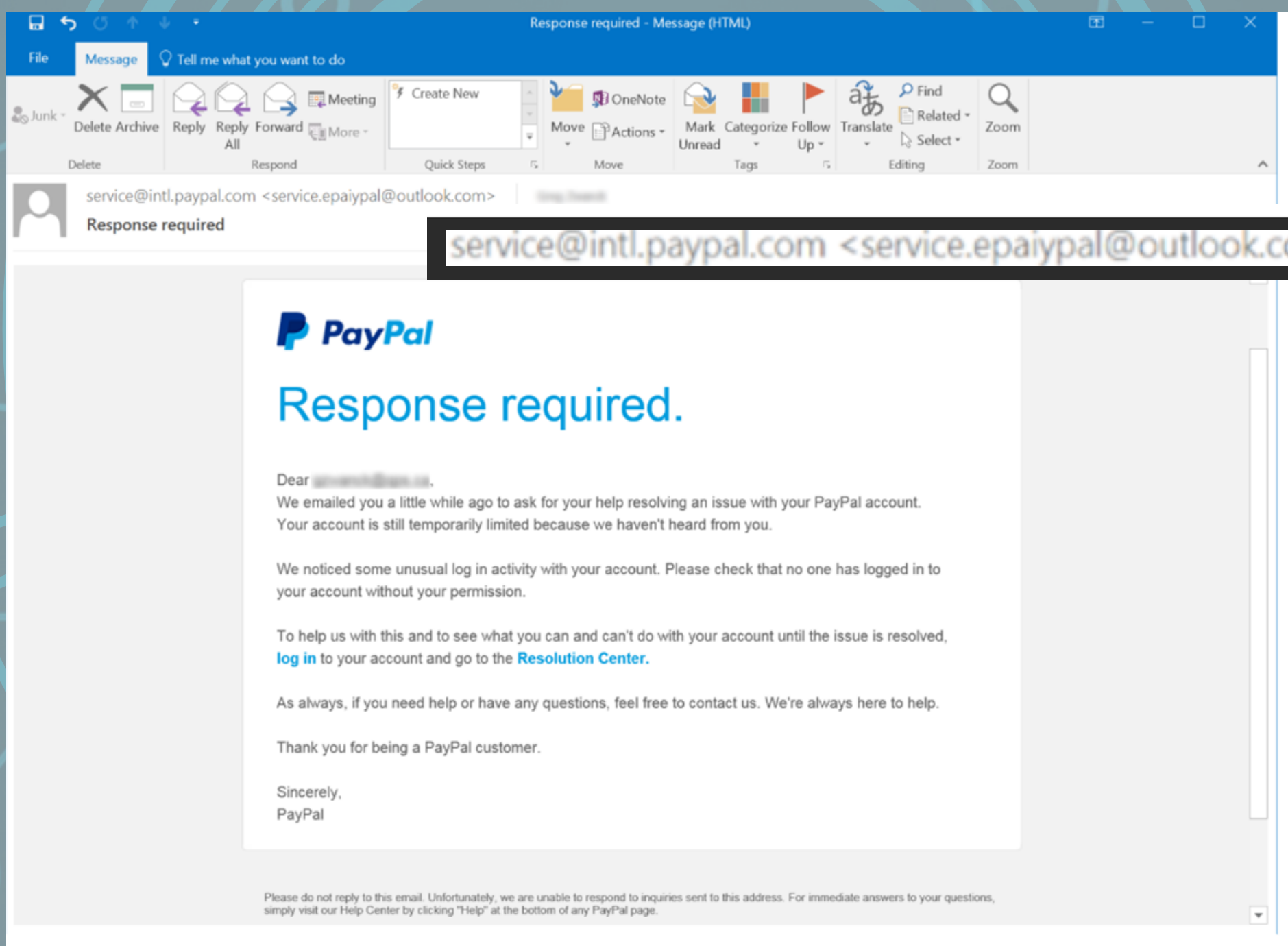
The document provides detailed recommendations for preventing ransomware attacks, such as keeping your software up to date, using strong passwords, and backing up your data regularly. It also provides guidance on how to respond to a ransomware attack if it occurs, such as isolating infected systems, contacting law enforcement, and not paying the ransom.

Overall, the document provides valuable information for individuals and organizations looking to protect themselves from ransomware attacks. The recommendations are based on best practices and guidelines from the National Institute of Standards and Technology (NIST), which is a reputable source for cybersecurity advice.

THE BEST RUN SAP®

Forage

Email 1 review



The sender is using an unofficial PayPal domain email address. If you look closely, you may notice some misspelled words like epaiypal.

We can assume that this email is probably malicious, trying to convince you to provide your account details like username and password and then your account will be stolen.

Email 2 review

Cathy Frisbie <CFrisbie@clientsdomains.com> 12:10 PM (0 minutes ago)
to CarlEYoung

Hey Carl! I found that file you are looking for. Check out the urgent news sent by our CEO. Click this link to read it!

This is time sensitive and not reading this can result in being suspended from the company without pay!

Your Friend,

Frisbie

Reply Reply all Forward

In this particular email, there are some hints that the email might be malicious, such as the following:

clientdomains != clientsdomain:
As we can see in the previous task document "Organization Password Policy", enterprise emails use the @clientdomains domain, and we can see that the sender of this email is @clientsdomains which has an extra "s".

Sense of urgency and threats of suspension without pay:
This is very common in phishing emails, they try to convince you that you need to take urgent action to avoid bad consequences.
That way, people tend to think less about the risk they're taking and make the wrong move by clicking on links.

Email 3 review

HR employee verification Inbox ×

Gloria Hicks <GloriaHicks@clientsdomains.com> 1:07 PM (0 minutes ago)
to ErikaNRansdell

Hey Erika, This is Gloria from the HR department. As part of our HR auditing process, it is important to verify your social security number and date of birth. Please fill and submit the information by clicking the below link.

Submit your social security number and date of birth here

Please reply in the next 10 minutes to avoid having your company account suspended.

Best Regards,

HR Department

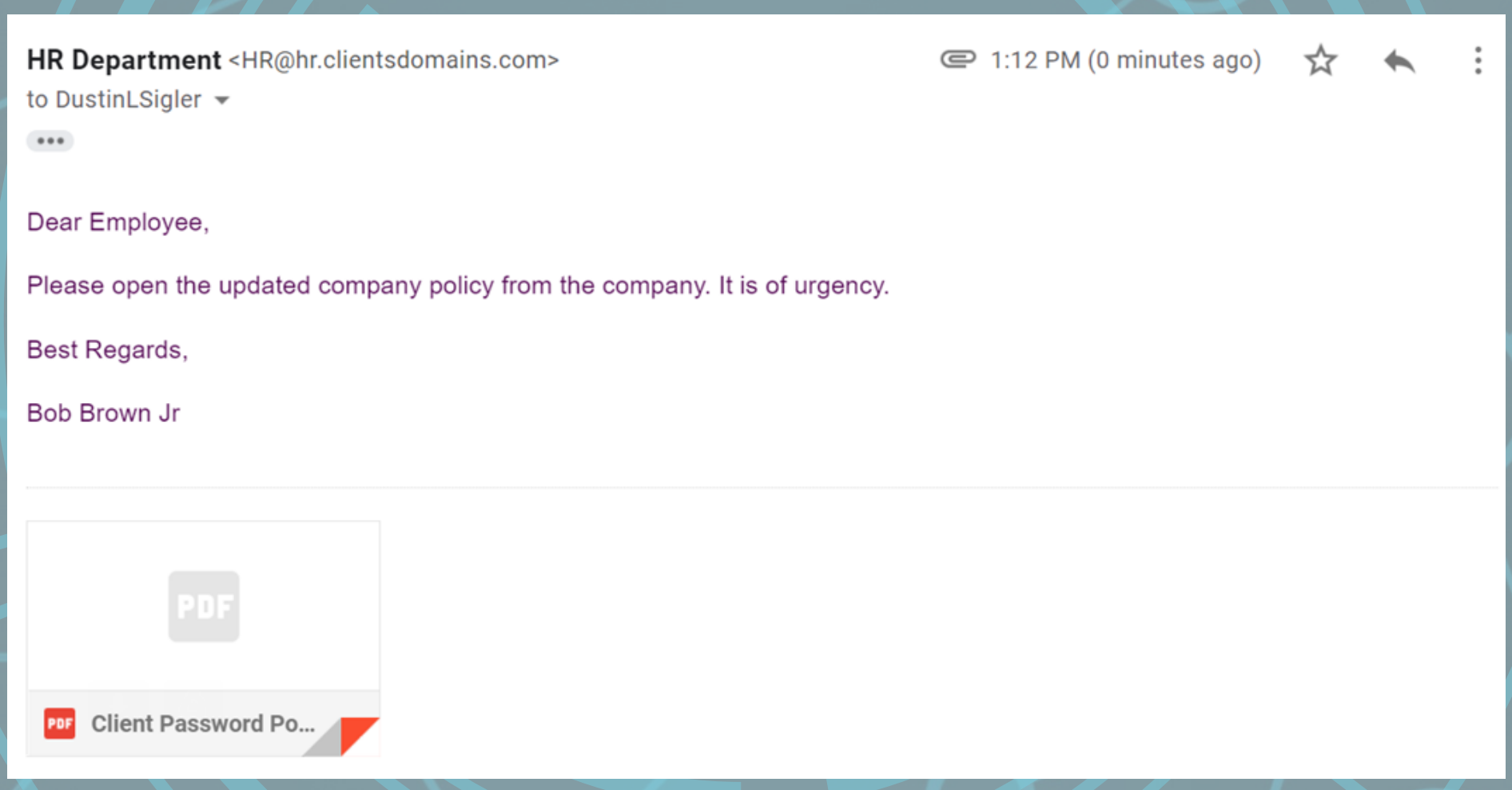
As in the previous email, we have again the domains of the clients

customerdomains != customerdomain:
As we can see in the previous task document "Organization Password Policy", business emails use the @clientdomains domain, and we can see that the sender of this email is @clientsdomains which has an extra "s".

Sense of urgency and threats of being suspended:
This is very common in phishing emails, they try to convince you that you need to take urgent action within the next 10 minutes to avoid bad consequences like getting banned. That way, people tend to think less about the risk they're taking and make the wrong move by clicking on links.

Be cautious with your personal data:
It is better to suspend your account and then repair it than to give your personal social security number to someone with malicious intent.

Email 4 review



As in the previous emails, we again have the wrong domain name.

<u>customerdomains != customerdomain:</u>
As we can see in the previous task document "Organization Password Policy", commercial emails use the domain @clientdomains, and we can see that the sender of this email is @clientsdomains which has an additional "s".

<u>Beware of attachments:</u>
It also includes a PDF file, and this is where we have to remember that only .txt files could be considered harmless. Any other type of file could hide some kind of danger.

THE BEST RUN SAP®

Forage

Email 5 review

Your PayPal Access Blocked !

PayPal <paypalaccounts@mailbox.com> Unsubscribe
to me

Your PayPal Account is Limited, Solve in 24 Hours!

Dear PayPal Customer,

We're sorry to say you cannot access all the paypal account features like payment and money transfer.
Click here to fix your account now. .

Why is it blocked?
Because we think your account is in danger of theft and unauthorized uses.

How can I fix the problem?
Confirm all your details on our server. Just click below and follow all of the steps.

Confirm Account Details Now

The sender of the email is obviously not from an official PayPal domain (@mailbox.com). This indicates a possible attempt to steal your account information, such as your username and password.

It feels somewhat rushed, says you need to fix your situation within the next 24 hours, and has links trying to convince you to give them your account details.

Email 6 review

Request Inbox ×

Sal Khan <executivee197@gmail.com> 12:14 AM (11 hours ago)
to me

When you get a minute, could you please drop me an email.

Best Regards
Sal Khan
CEO

This email should be considered malicious because the sender is not using the company's official email domain. Even if he is the real CEO, he should use his company email address to avoid potential security issues.

Another indicator of a possible malicious email is that the text written in it is very impersonal, it could be for anyone and anywhere.

Finally, the time the email was sent (00:14) is a bit strange for a work-related email, and should be considered at least highly unusual.

THE BEST RUN SAP®

Forage

Email 7 review

Important Company Meeting Inbox ×

Cathy Frisbie <CFrisbie@clientdomains.com>
to CarlEYoung

9:17 AM (0 minutes ago)

Hi Carl,

We have an important company meeting today at 3PM.

Here is the link to my part of the presentation.

sharepoint.clientdomains.com

It is under the "IMP2021 Presentation" folder.

See you later today!

Best Regards,

Cathy Frisbie

CFrisbie@clientdomains.com

www.clientdomains.com

EXT 111

This last email seems safe, coming from the correct domain (@clientdomains), but you still need to hover over the link before clicking to ensure you're not redirected to a malicious site.