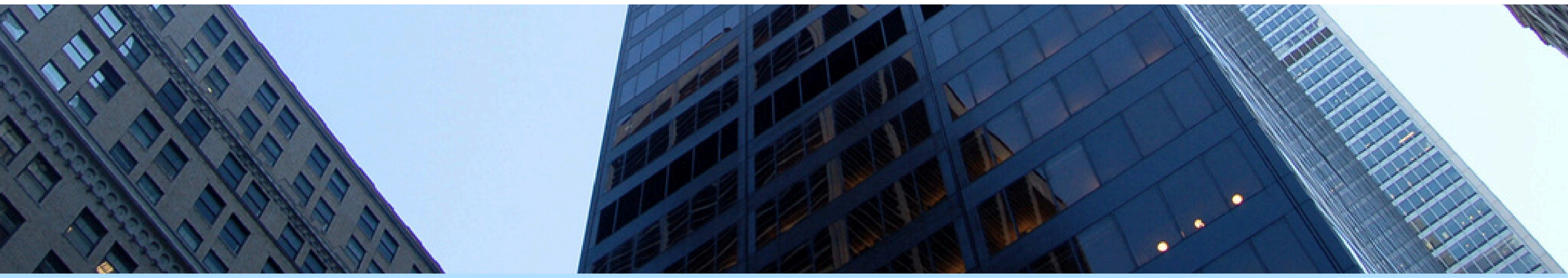
SECURZE

SECURING WHAT MATTERS MOST



8 Steps Guide To Identify Phishing Emails

www.securze.com

info@securze.com

☎ +91 84510 73938

securze

securze_com

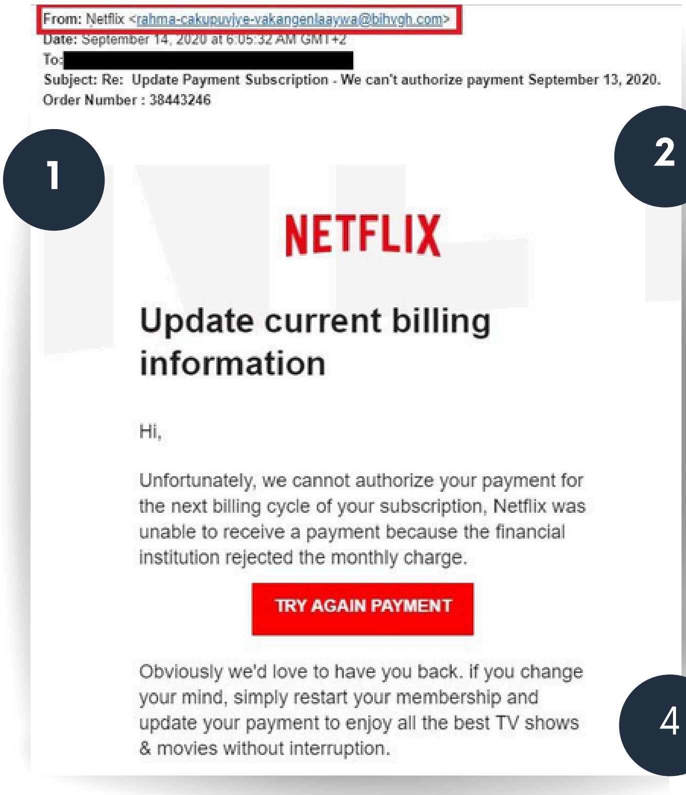
Securze

WHAT ARE PHISHING EMAILS?

Phishing emails are fraudulent messages that appear to come from reputable sources, but they aim to trick individuals into revealing sensitive information, such as passwords or credit card numbers.

EXMAPLES OF PHISHING EMAILS

1



From: Netflix <rahma-cakupuyjye-vakangenlaaywa@bihvgh.com>
Date: September 14, 2020 at 6:05:32 AM GMT+2
To: [redacted]
Subject: Re: Update Payment Subscription - We can't authorize payment September 13, 2020.
Order Number : 38443246

NETFLIX

Update current billing information

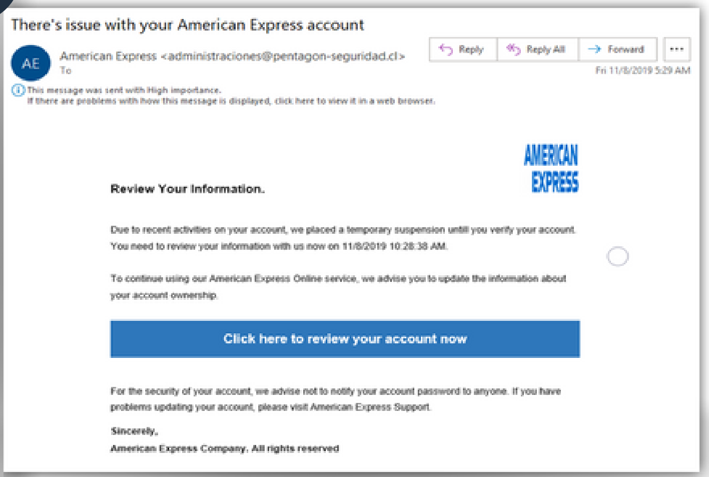
Hi,

Unfortunately, we cannot authorize your payment for the next billing cycle of your subscription, Netflix was unable to receive a payment because the financial institution rejected the monthly charge.

TRY AGAIN PAYMENT

Obviously we'd love to have you back. If you change your mind, simply restart your membership and update your payment to enjoy all the best TV shows & movies without interruption.

2



There's issue with your American Express account

AE American Express <administraciones@pentagon-seguridad.cl>
To

Fri 11/8/2019 5:29 AM

ⓘ This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

Review Your Information.

Due to recent activities on your account, we placed a temporary suspension untill you verify your account. You need to review your information with us now on 11/8/2019 10:28:38 AM.

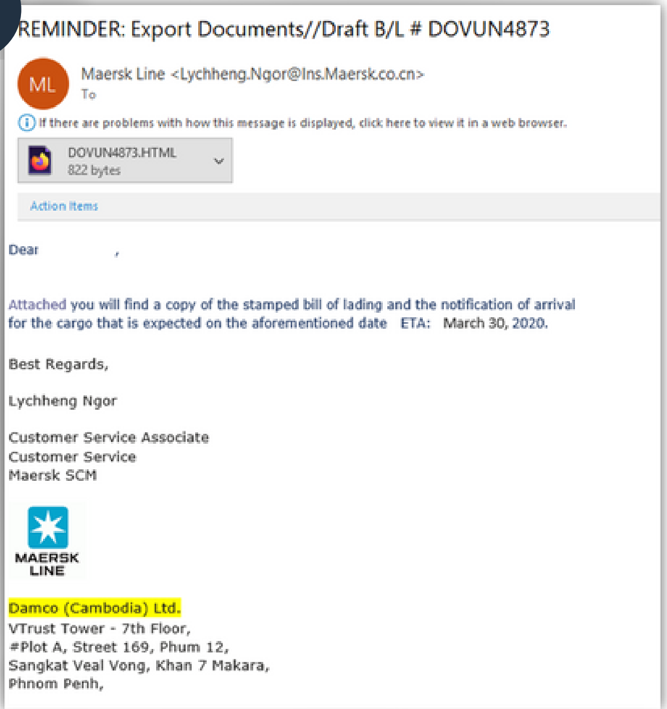
To continue using our American Express Online service, we advise you to update the information about your account ownership.

Click here to review your account now

For the security of your account, we advise not to notify your account password to anyone. If you have problems updating your account, please visit American Express Support.

Sincerely,
American Express Company. All rights reserved

4



REMINDER: Export Documents//Draft B/L # DOVUN4873

ML Maersk Line <Lychheng.Ngor@lns.Maersk.co.cn>
To

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

DOVUN4873.HTML
822 bytes

Action Items

Dear ,

Attached you will find a copy of the stamped bill of lading and the notification of arrival for the cargo that is expected on the aforementioned date ETA: March 30, 2020.

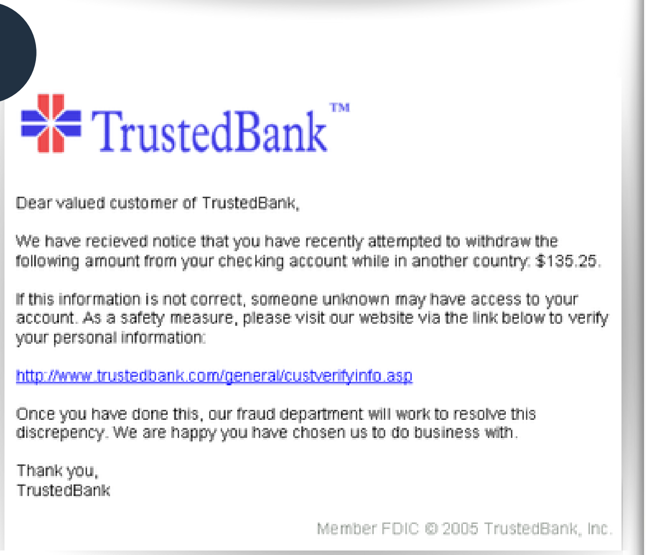
Best Regards,

Lychheng Ngor

Customer Service Associate
Customer Service
Maersk SCM

Damco (Cambodia) Ltd.
VTrust Tower - 7th Floor,
#Plot A, Street 169, Phum 12,
Sangkat Veal Vong, Khan 7 Makara,
Phnom Penh,

3



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

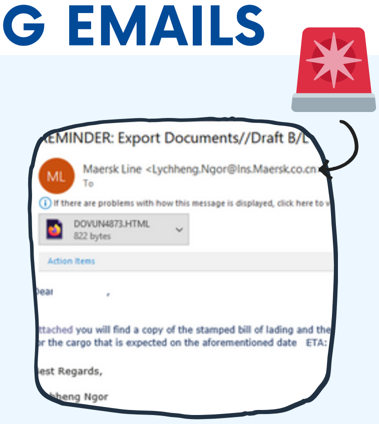
Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Identifying phishing emails can be challenging, especially for beginners. Here are some tips to help you recognize phishing emails, even if you're not tech-savvy:

IDENTIFICATION OF PHISHING EMAILS

1 **Check the Sender's Email Address:** Phishing emails often come from addresses that look similar to legitimate ones but may have subtle differences, such as misspellings or extra characters. Always check the sender's email address carefully.



EMINDER: Export Documents//Draft B/L

ML Maersk Line <Lychheng.Ngor@Ins.Maersk.co.cn>
To

If there are problems with how this message is displayed, click here to v

DOVUN4873.HTML
822 bytes

Action Items

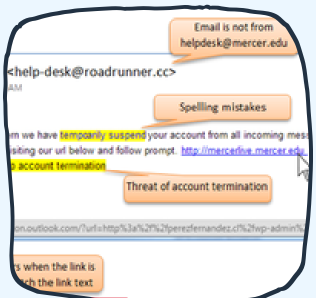
Dear ,

ttached you will find a copy of the stamped bill of lading and the
r the cargo that is expected on the aforementioned date ETA:

est Regards,

heng Ngor

2 **Look for Spelling and Grammar Errors:** Phishing emails often contain spelling and grammar mistakes. Legitimate organizations usually proofread their communications thoroughly.



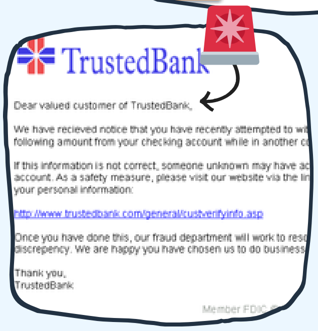
<help-desk@roadrunner.cc>
AM

m we have temporarily suspend your account from all incoming mes
isiting our url below and follow prompt. http://mercerlive.mercer.edu
o account termination

on.outlook.com/?url=http%3a%2f%2fperezfernandez.cl%2fwp-admin%

Email is not from helpdesk@mercer.edu
Spellling mistakes
Threat of account termination
s when the link is
ch the link text

3 **Examine the Greeting:** Generic greetings like "Dear Customer" or "Dear User" instead of your actual name can be a red flag. Legitimate organizations often use your name in their emails.



TrustedBank

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to wi
following amount from your checking account while in another c

If this information is not correct, someone unknown may have ac
account. As a safety measure, please visit our website via the lin
your personal information:

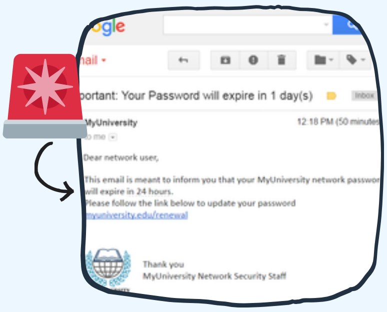
http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to reso
discrepency. We are happy you have chosen us to do business

Thank you,
TrustedBank

Member FDIC ©

4 **Beware of Urgent or Threatening Language:** Phishing emails often create a sense of urgency, stating that your account will be closed or that you will face consequences if you don't act immediately. Be suspicious of such pressure tactics.



portant: Your Password will expire in 1 day(s)

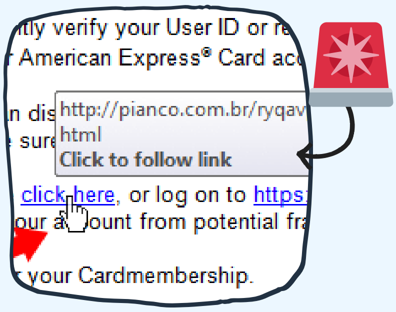
MyUniversity 12:18 PM (50 minutes
to me

Dear network user,

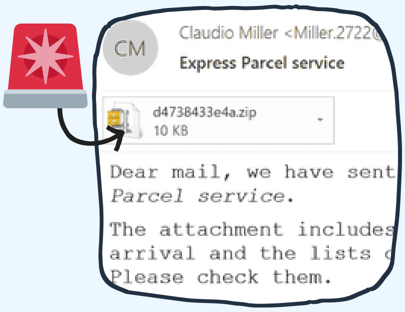
This email is meant to inform you that your MyUniversity network passwor
will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

Thank you
MyUniversity Network Security Staff

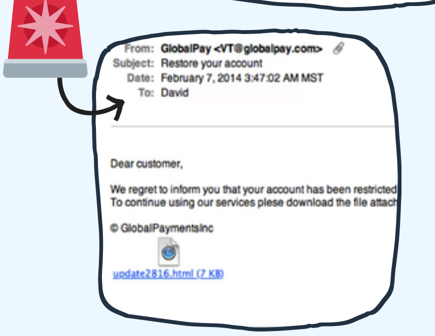
5 **Avoid Clicking on Suspicious Links:**
Hover your mouse over any links in the email (without clicking) to see the actual URL. If the URL looks suspicious or doesn't match the legitimate website of the supposed sender, it's likely a phishing attempt.


tly verify your User ID or re
r American Express® Card acc
n dis http://pianco.com.br/ryqav
sure html
Click to follow link
click here, or log on to https:
our account from potential fra
r your Cardmembership.

6 **Be Cautious with Attachments:**
Don't download attachments from unknown or unexpected sources. These attachments might contain malware.


CM Claudio Miller <Miller.2722@
Express Parcel service
d4738433e4a.zip
10 KB
Dear mail, we have sent
Parcel service.
The attachment includes
arrival and the lists c
Please check them.

7 **Verify with the Company:**
If you're unsure about the authenticity of an email, contact the company or organization directly using official contact information. Don't use the contact details provided in the email, as they might be fake.


From: GlobalPay <VT@globalpay.com>
Subject: Restore your account
Date: February 7, 2014 3:47:02 AM MST
To: David

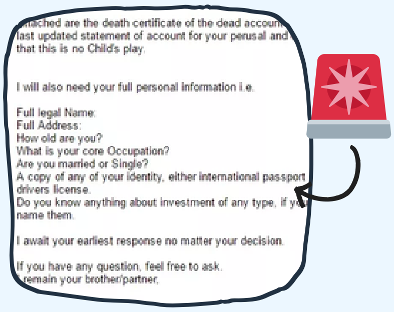
Dear customer,

We regret to inform you that your account has been restricted
To continue using our services plese download the file attach

© GlobalPaymentsInc

update2816.html (7 KB)

8 **Check for Personal Information Requests:**
Be suspicious of emails requesting personal or financial information. Legitimate organizations don't ask for such details via email.


ttached are the death certificate of the dead accoun
last updated statement of account for your perusal and
that this is no Child's play.

I will also need your full personal information i.e.

Full legal Name:
Full Address:
How old are you?
What is your core Occupation?
Are you married or Single?
A copy of any of your identity, either international passport
drivers license.
Do you know anything about investment of any type, if you
name them.

I await your earliest response no matter your decision.

If you have any question, feel free to ask.
I remain your brother/partner,

Remember, it's always better to be overly cautious than to fall victim to a phishing attack. If you receive an email that seems suspicious, trust your instincts and take the time to verify its authenticity before taking any action.

How Securze can help?

At Securze, we offer comprehensive Cyber Security Awareness Training to elevate your employees' security practices to a best-in-class level for your business. A single oversight from an employee can lead to significant consequences due to inadequate training on common cyber attack vectors. We specialize in training your employees, equipping them with effective cyber attack defense strategies, and ensuring they stay consistently updated on the latest cyber trends. For more info, reach out to us at info@securze.com

A TEAM OF PROFESSIONALS WHO HAVE TRAINED -

ICICI Lombard
GENERAL INSURANCE

AXIS BANK

IDBI BANK

ICICI Bank

HDFC BANK

IDFC FIRST
Bank

आर सी एफ

and many more...

SECURZE

SECURING WHAT MATTERS MOST

For business inquiries,
contact us.

www.securze.com

info@securze.com

+91 84510 73938

securze

securze_com

Securze