केन्द्रीय शैक्षिक प्रौद्योगिकी संस्थान

Central Institute of Educational Technology

# NCERT – CIET - WEBINAR

# PHISHING


18-02-2021, Thursday – 4.00 pm to 5.00 pm

Presenter:
M. Vijayakumar.
ICT National Awardee.
Kallakurichi.
Tamil Nadu

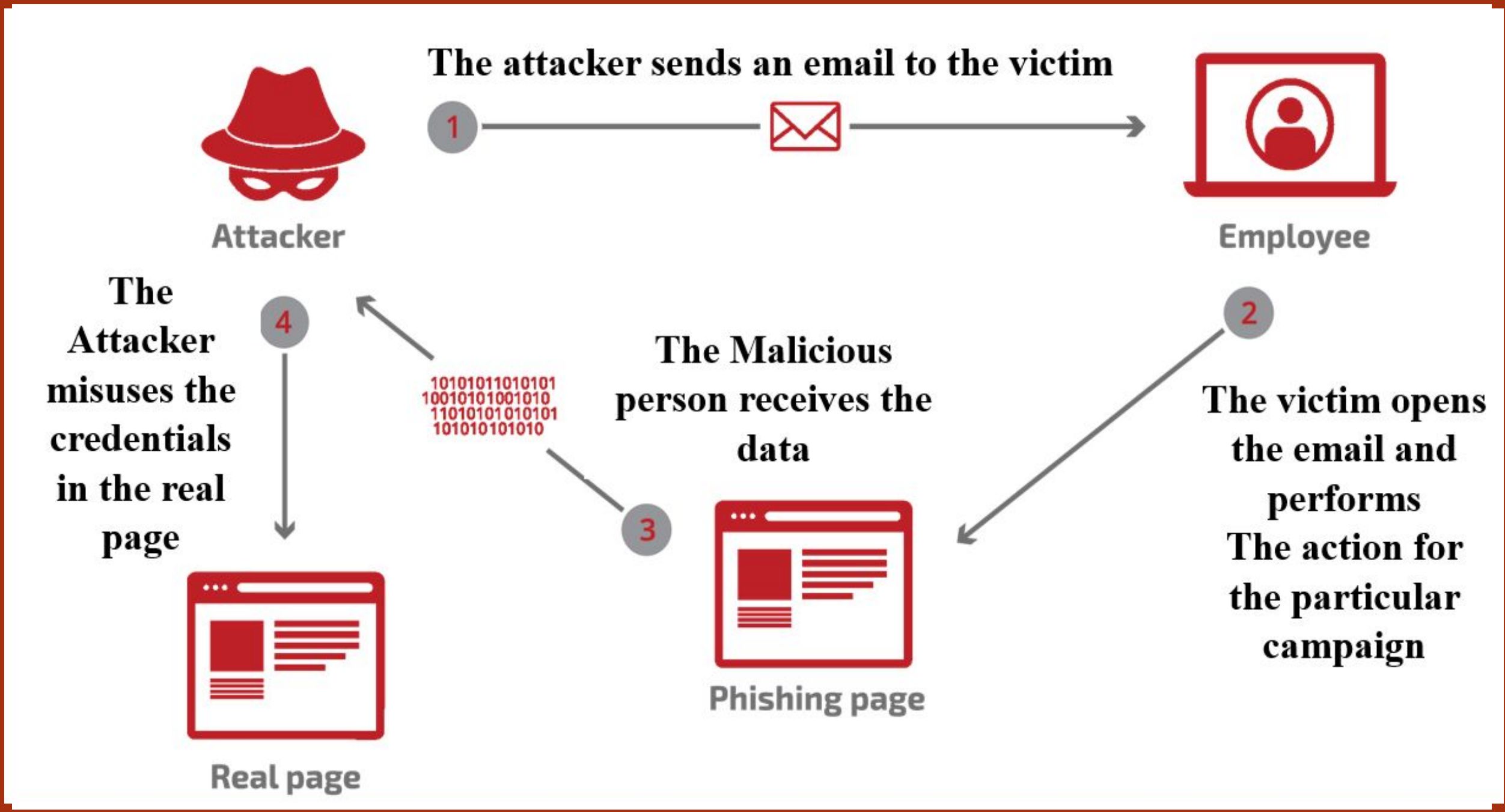

PC : TechUseful

# FISHING & PHISHING

**Phishing is the fraudulent attempt to obtain sensitive information or data, such as**

- **Usernames**
- **passwords**
- **credit card details or**
- **other sensitive details,**

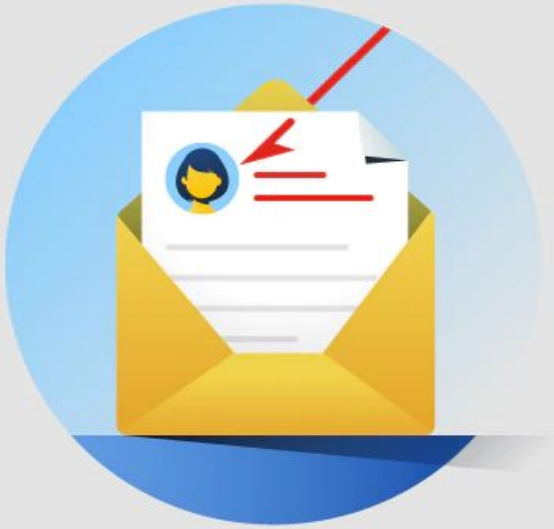

**by impersonating oneself as a trustworthy entity in a digital communication**


The attacker sends an email to the victim
1
Attacker
Employee
2
The victim opens the email and performs The action for the particular campaign
The Malicious person receives the data
3
10101011010101
10010101001010
11010101010101
10101010101
Phishing page
4
The Attacker misuses the credentials in the real page
Real page

# COMMON TYPES OF PHISHING

## EMAIL PHISHING

Scammers create emails that impersonate legitimate companies and attempt to steal your information.

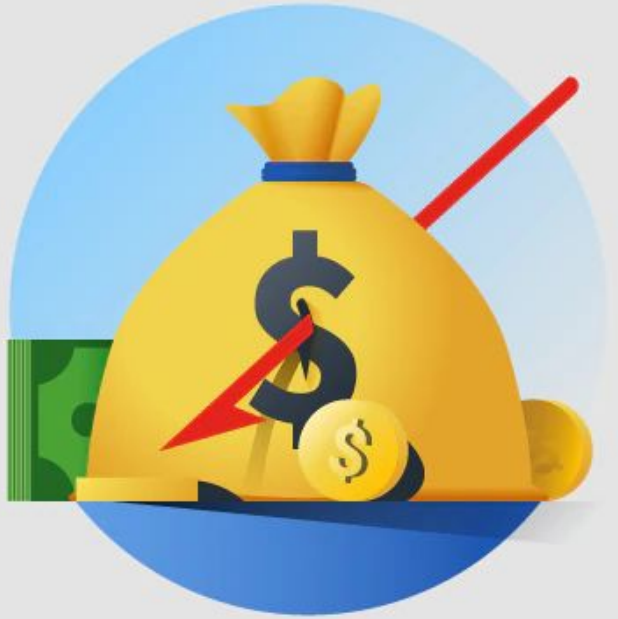


## SPEAR PHISHING

Similar to email phishing, but the messages are more personalized. For example, they may appear to come from your boss.

## CLONE PHISHING

Scammers replicate an email you have received, but include a dangerous attachment or link.



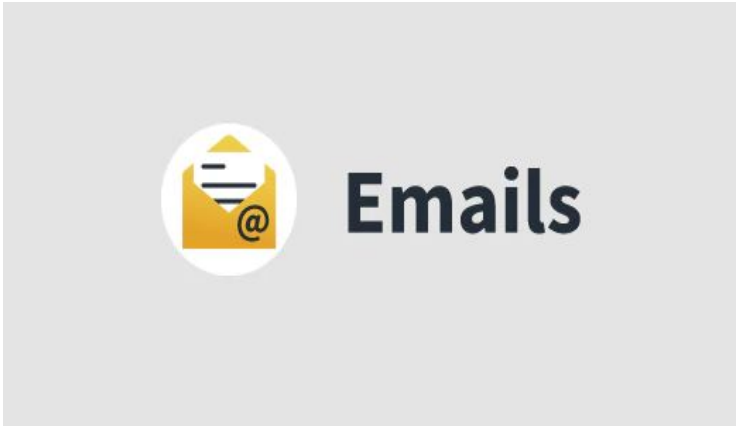
## WHALING

Scammers target high-ranking executives to gain access to sensitive data or money.

## POP-UP PHISHING

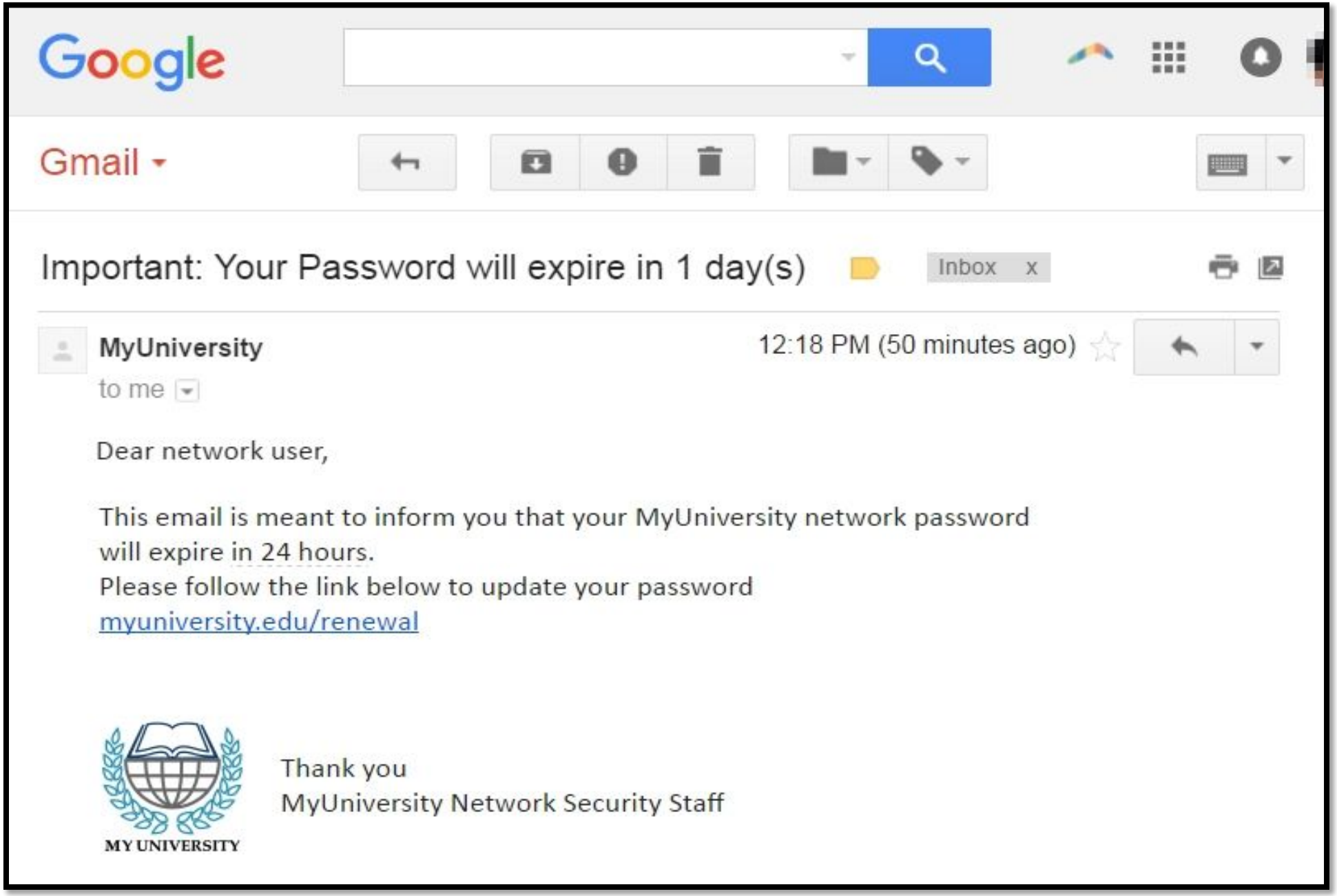
Fraudulent pop-ups trick users into installing malware.

# PHISHERS CAN TRICK US  MOSTLY THROUGH





# Emails


Google
Gmail
Important: Your Password will expire in 1 day(s)
Inbox x
MyUniversity
12:18 PM (50 minutes ago)
to me
Dear network user,
This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal
MY UNIVERSITY
Thank you
MyUniversity Network Security Staff

PayPal

# Update Required!!

Recently, there's been activity in your PayPal account that seems unusual compared to your normal account activities. Please log in to PayPal to confirm your identity.

This is part of our security process and helps ensure that PayPal continue to be safer way to buy online. Often all we need is a bit more information. While your account is limited, some options in your account won't be available.

**How to remove my limitation?**

You can resolve your limitation by following these simple steps:

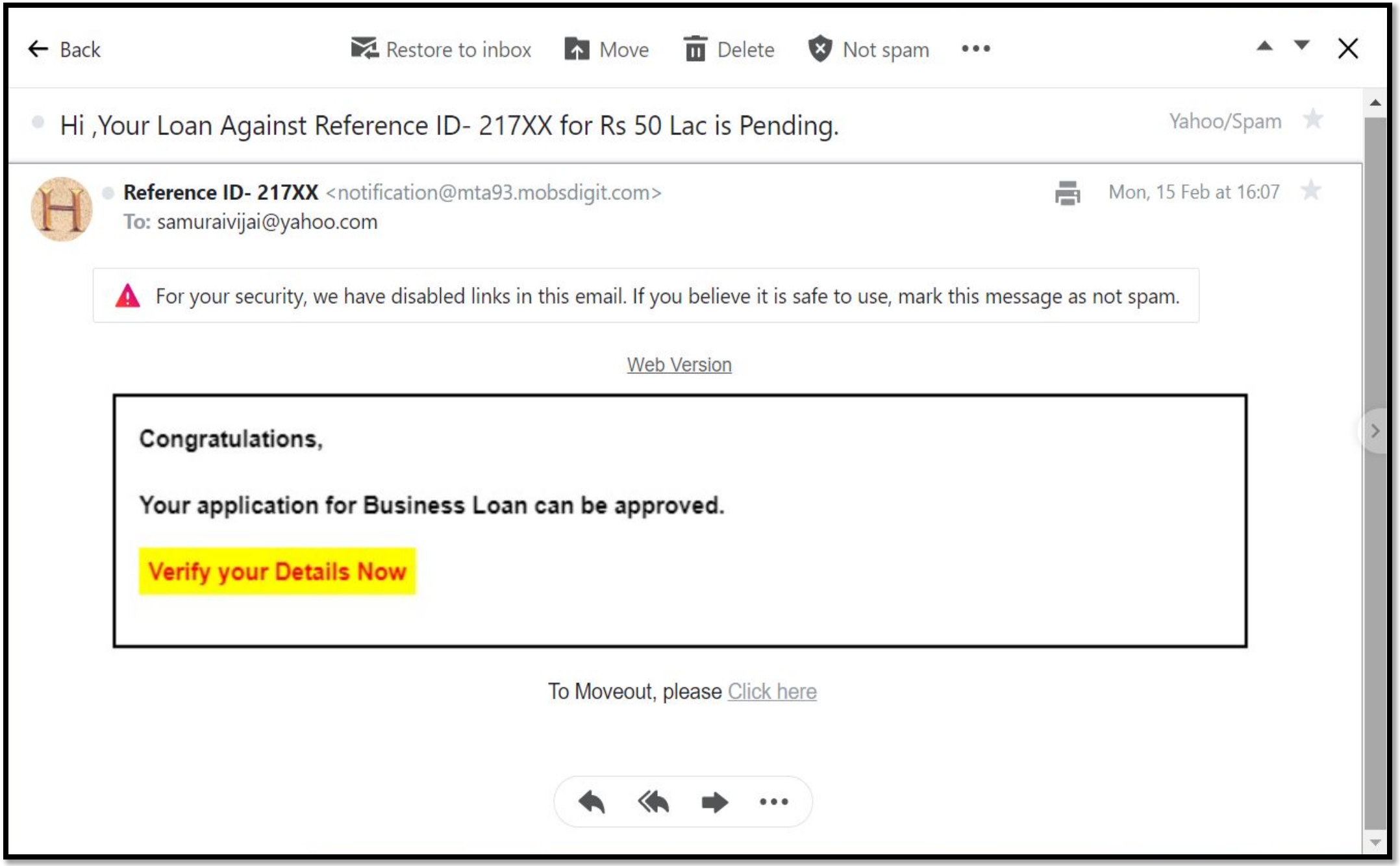
- **Log in here**.

- Provide the information needed. The sooner your provide the information we need, the sooner we can resolve the situation.

**"If this message sent as Junk or Spam, its just an error by our new system, please click at Not Junk or Not Spam"**

Sincerely,

PayPal


Back
Restore to inbox
Move
Delete
Not spam
Hi ,Your Loan Against Reference ID- 217XX for Rs 50 Lac is Pending.
Yahoo/Spam
Reference ID- 217XX <notification@mta93.mobsdigit.com>
To: samuraivijai@yahoo.com
Mon, 15 Feb at 16:07
For your security, we have disabled links in this email. If you believe it is safe to use, mark this message as not spam.
Web Version
Congratulations,
Your application for Business Loan can be approved.
Verify your Details Now
To Moveout, please Click here

Back | Archive | Move | Delete | Spam | ...

Welcome,Your Application is selected, Check Now

Yahoo/Inbox

NS

**Loan Passed** <notification@rbd14.rebynder.com>

**To:** samuraivijai@yahoo.com

Fri, 25 Dec 2020 at 20:36

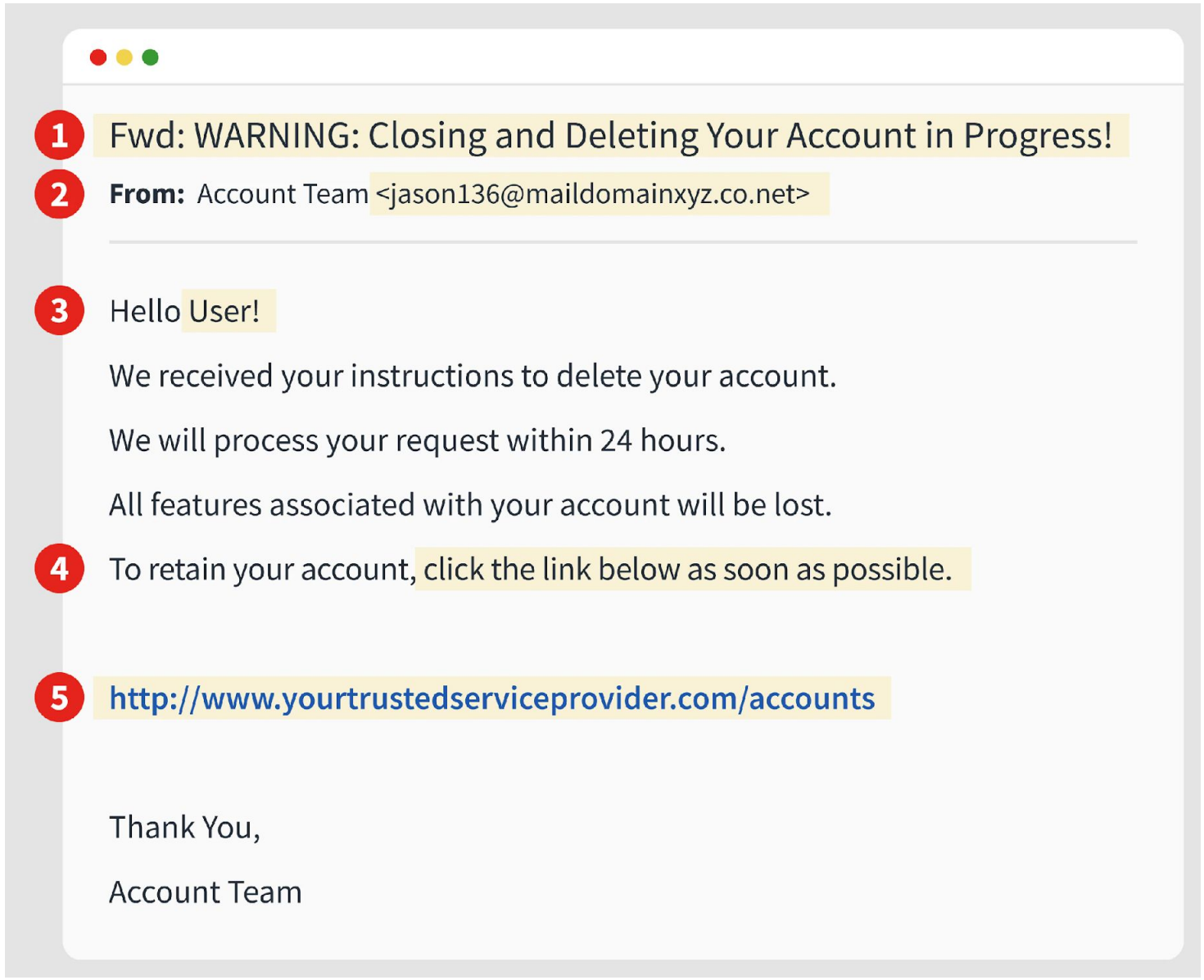
Back | Archive | Move | Delete | Spam | ...

**Htr9 Hubsstar Info**

Your Item Placed Successfully & Delivered within 2 Days — Yahoo/Inbox

**Order Placed** <info@htr9.hubsstar.com> Unsubscribe
**To:** samuraivijai@yahoo.com
Fri, 25 Sept 2020 at 19:20

# SIGNS OF EMAIL PHISHING




**1 SUBJECT LINE**
Sense of urgency

**2 SENDER**
Legitimate sender you deem trustworthy

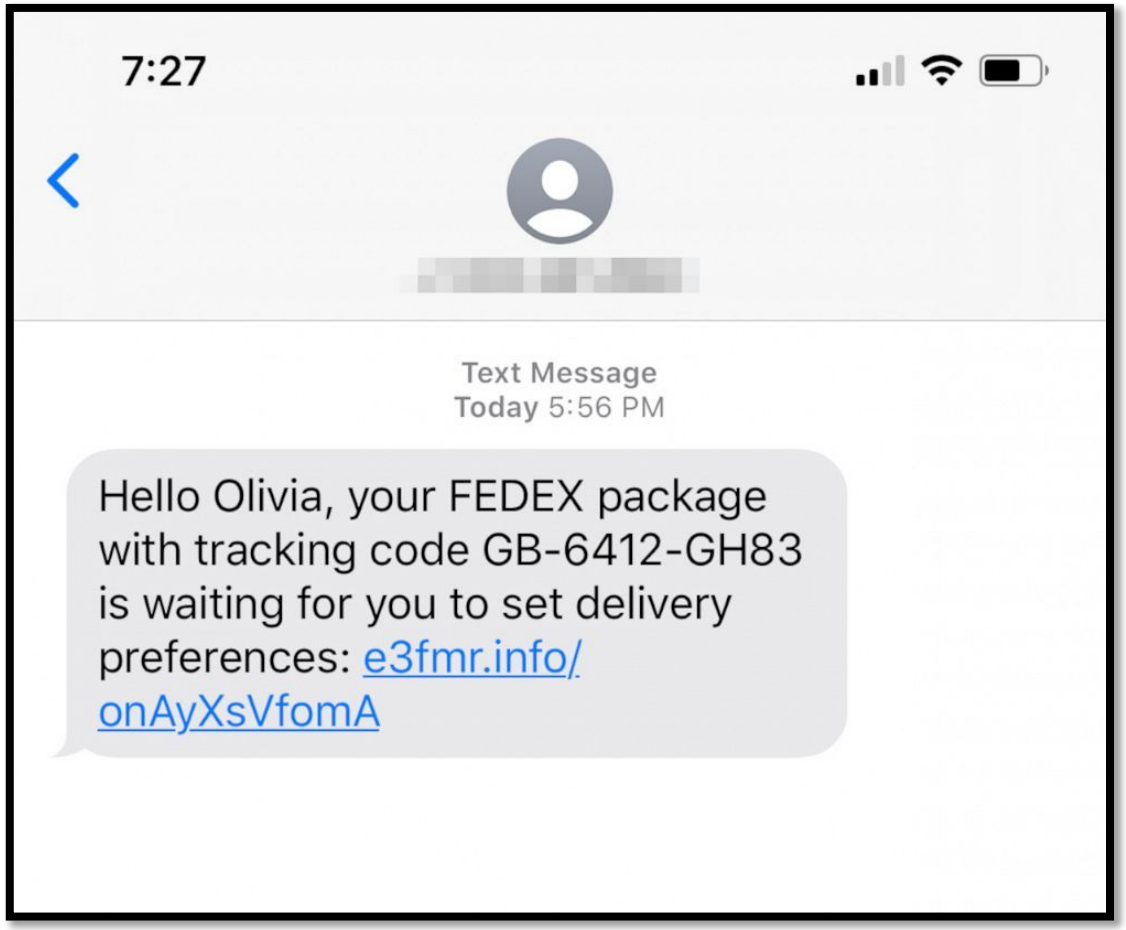
**3 GREETING**
Generic greeting

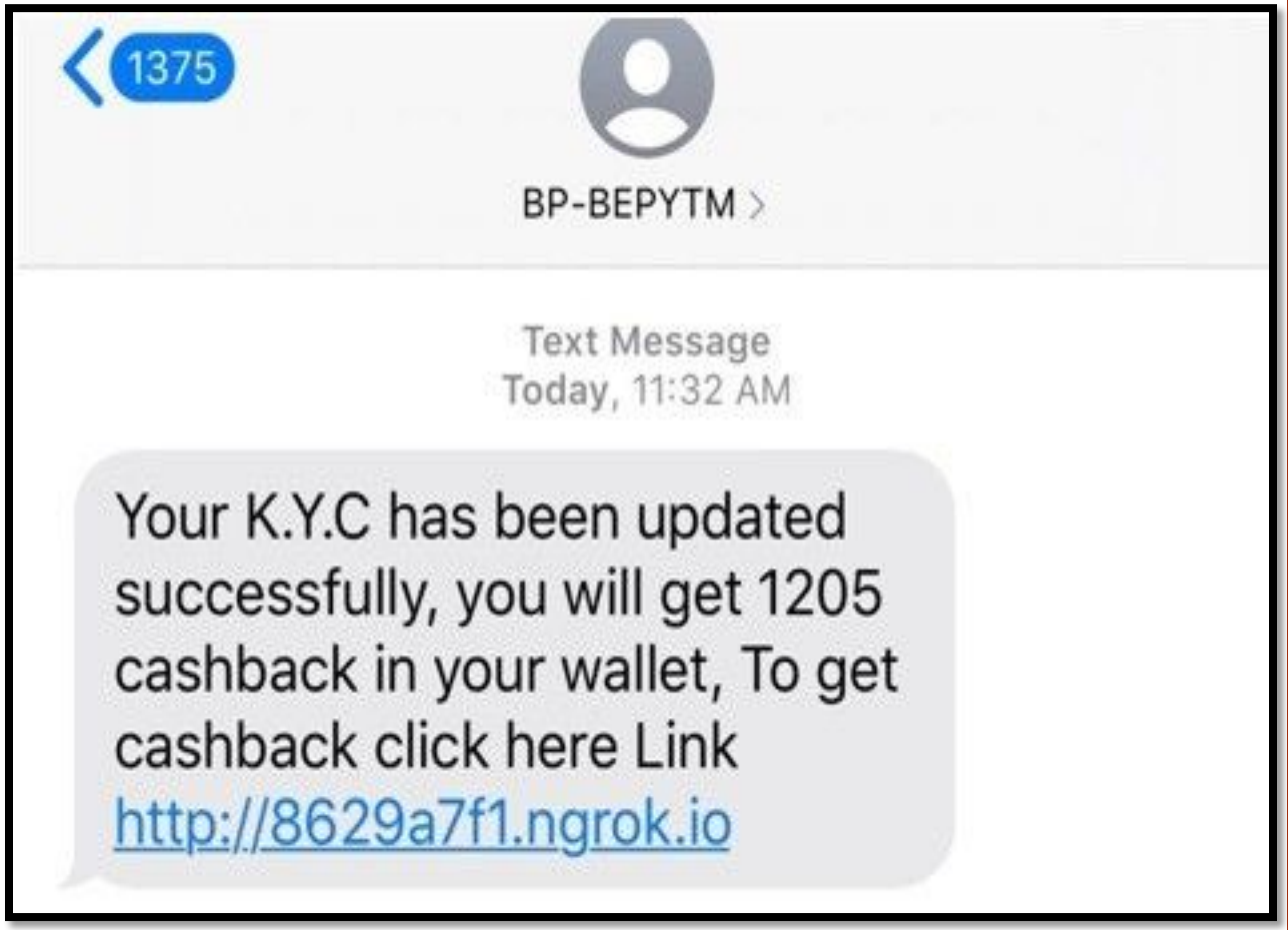
**4 CLOSING REQUEST**
A call for immediate action

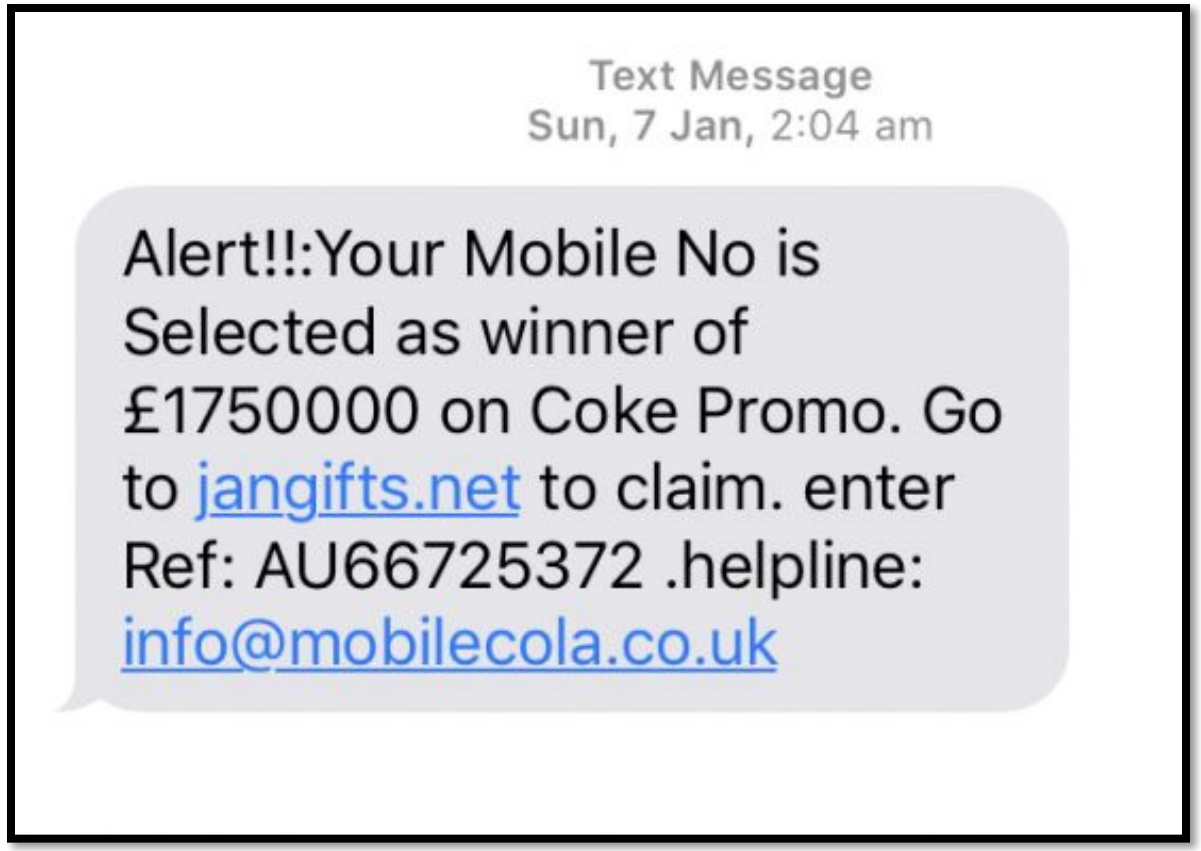
**5 HYPERLINK**
Statement requesting you link

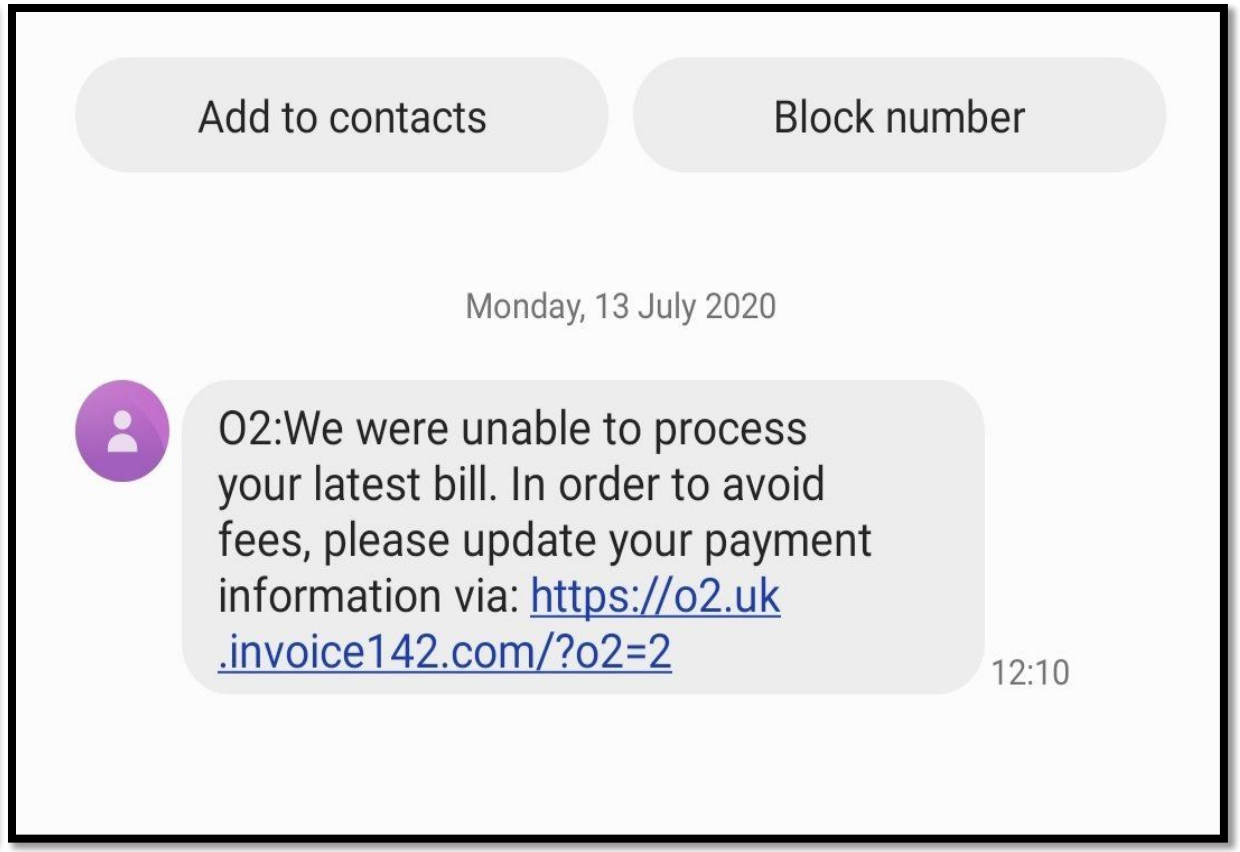
https://us.norton.com/internetsecurity-online-scam-what-is-phishing.html PC: Norton.com


# Smishing
# SMS - Phishing

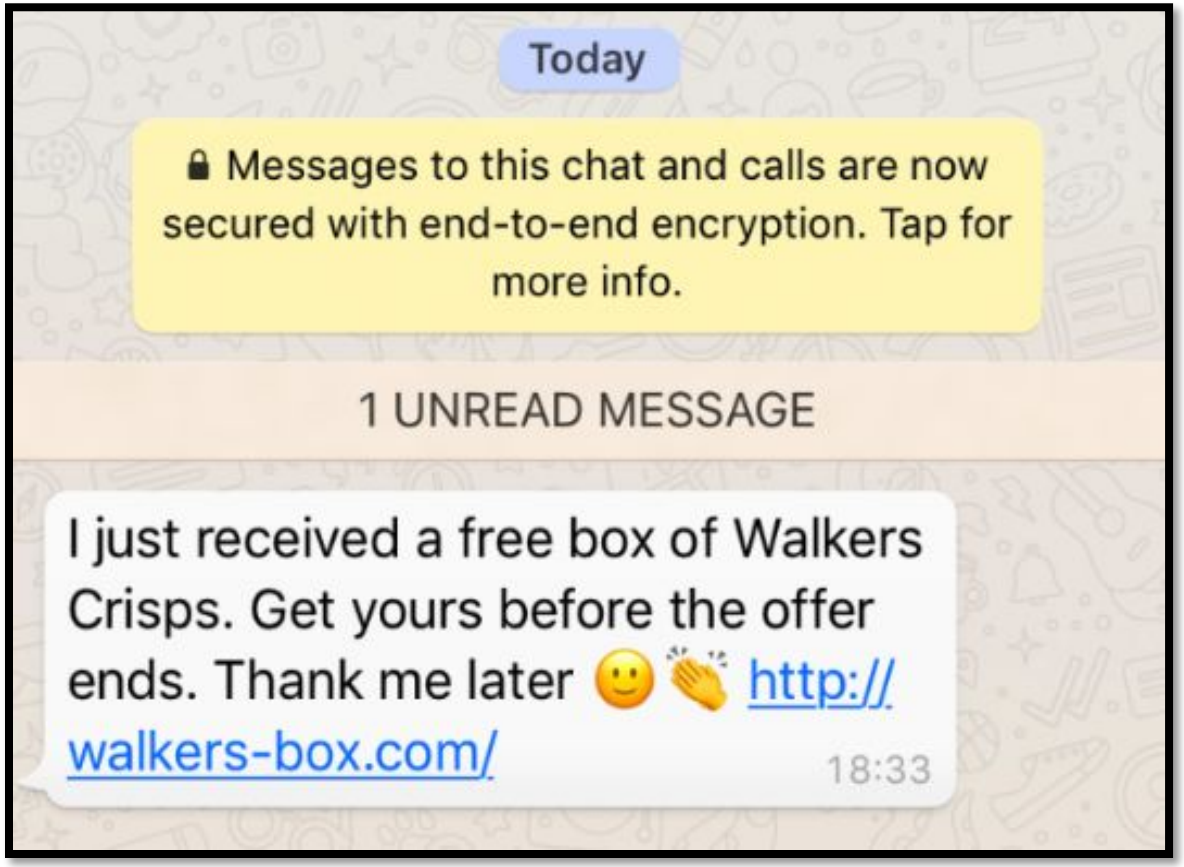

7:27
Text Message
Today 5:56 PM
Hello Olivia, your FEDEX package with tracking code GB-6412-GH83 is waiting for you to set delivery preferences: e3fmr.info/onAyXsVfomA


1375
BP-BEPYTM
Text Message
Today, 11:32 AM
Your K.Y.C has been updated successfully, you will get 1205 cashback in your wallet, To get cashback click here Link http://8629a7f1.ngrok.io

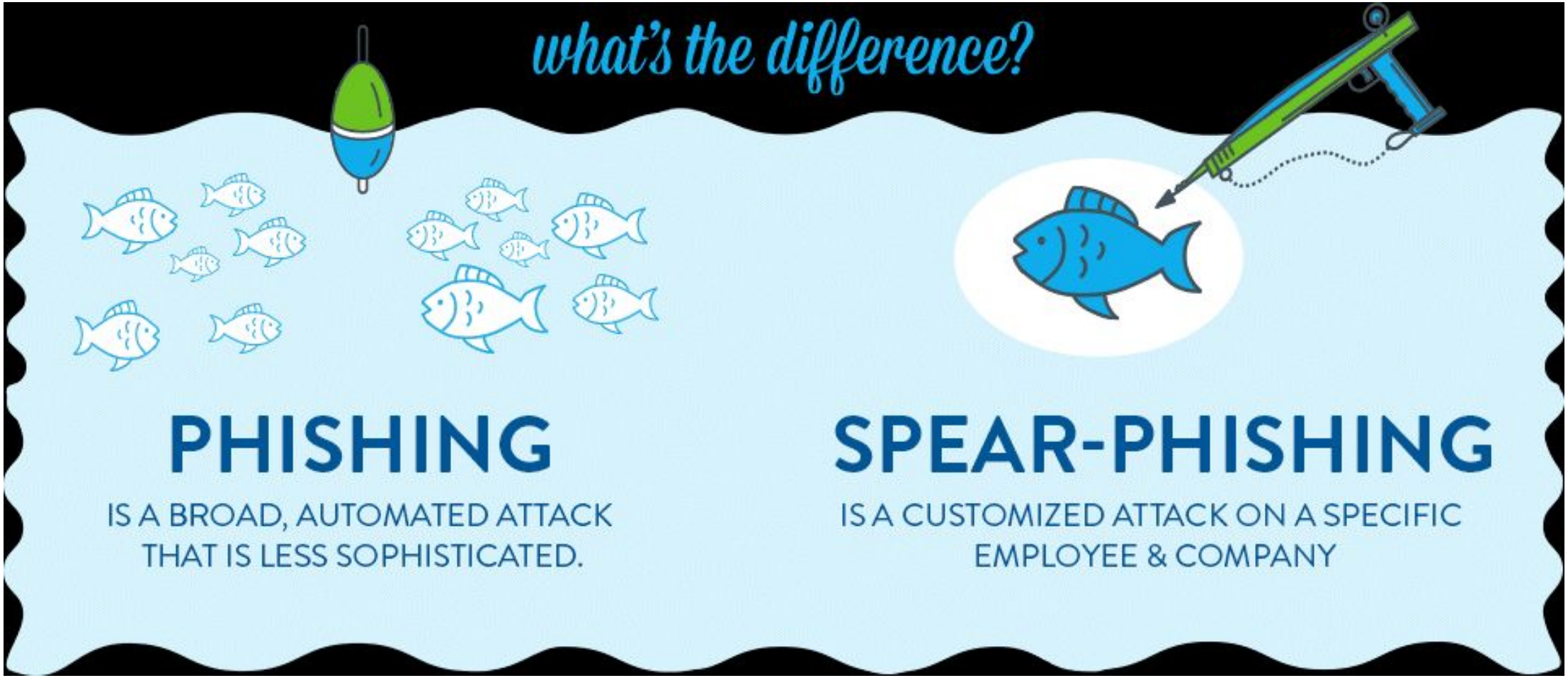

Text Message
Sun, 7 Jan, 2:04 am
Alert!!:Your Mobile No is Selected as winner of £1750000 on Coke Promo. Go to jangifts.net to claim. enter Ref: AU66725372 .helpline: info@mobilecola.co.uk


Add to contacts
Block number
Monday, 13 July 2020
O2:We were unable to process your latest bill. In order to avoid fees, please update your payment information via: https://o2.uk.invoice142.com/?o2=2
12:10


# WhatsApp - Phishing


Today
Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.
1 UNREAD MESSAGE
I just received a free box of Walkers Crisps. Get yours before the offer ends. Thank me later 🙂👏 http://walkers-box.com/
18:33


Cadbury
Cadbury FREE chocolate Basket
www.cadburyindia.com
SCAM!
WOW 😍 Cadbury India is giving FREE chocolate🍫🍫 basket gift Hamper to celebrate their 70th anniversary,Click here to Get yours: http://www.cadburyindia.com .
1:21 PM


what's the difference?
PHISHING
IS A BROAD, AUTOMATED ATTACK THAT IS LESS SOPHISTICATED.
SPEAR-PHISHING
IS A CUSTOMIZED ATTACK ON A SPECIFIC EMPLOYEE & COMPANY

# HOW TO PREVENT?

- Don’ t open suspicious mails / SMS
- Don’t click on suspicious hyperlinks in the mails
- Don’t send any financial info through mails to anyone.

( Account numbers, Usernames, Password..)

# HOW TO PREVENT?

- Don’t click on Pop-up Ads.
- Use Spam filters.
- Encrypt all sensitive company information
- Use Two – factor authentication

# HOW AN ORGANIZATION CAN WITHSTAND PHISHING?

TWO-FACTOR AUTHORIZATION

STRICT PASSWORD POLICY

ANTI-PHISHING TRAINING FOR EMPLOYEES

# HOW TO RECOVER IF RESPONDED TO PHISHING?

- Change your Passwords
- Contact the Organization that was spoofed
- Contact your card providers /

  Study your transaction statements
- Don’t send any financial info through mails to anyone.

  ( Account numbers, Usernames, Password..)

# HOW TO RECOVER IF RESPONDED TO PHISHING?

- Don’t click on Pop-up Ads.
- Use Spam filters.
- Scan your computer for any Malware.
- Encrypt all sensitive company information
- Initiate the Cyber Crime to take actions by complaining to them

# LEGAL ACTS AGAINST PHISHING

**Phishing-A Cyber Crime, the provisions of Information Technology Act, 2000**

The phishing fraud is **an online fraud** in which the fraudster disguise themselves and use false and fraudulent websites of bank and other financial institutions, URL Links **to deceive people into disclosing valuable personal data**, later on which is used to swindle money from victim account. Thus, essentially it is a **cyber crime** and it attracts many penal provisions of the Information Technology Act, 2000 as amended in 2008 adding some new provisions to deal with the phishing activity.

# LEGAL ACTS AGAINST PHISHING

The following Sections of the Information Technology Act, 2000 are applicable to the Phishing Activity:

**Section 66:** The account of the victim is compromised by the phisher which is not possible unless & until the **fraudster fraudulently effects some changes by way of deletion or alteration of information/data electronically in the account of the victim residing in the bank server.** Thus, this act is squarely covered and punishable u/s 66 IT Act.

**Section 66A:** The disguised email **containing the fake link of the bank** or organization is used to deceive or to mislead the recipient about the origin of such email and thus, it clearly attracts the provisions of Section 66A IT Act, 2000.

# LEGAL ACTS AGAINST PHISHING

**Section 66C:** In the phishing email, the fraudster disguises himself as the real banker and **uses the unique identifying feature of the bank or organization say Logo, trademark** etc. and thus, clearly attracts the provision of Section 66C IT Act, 2000.

**Section 66D:** The fraudsters through the use of the phishing email containing the link to the fake website of the bank or organizations **personates the Bank or financial institutions to cheat upon the innocent persons**, thus the offence under Section 66D too is attracted.

*Thank you all for joining this webinar!*