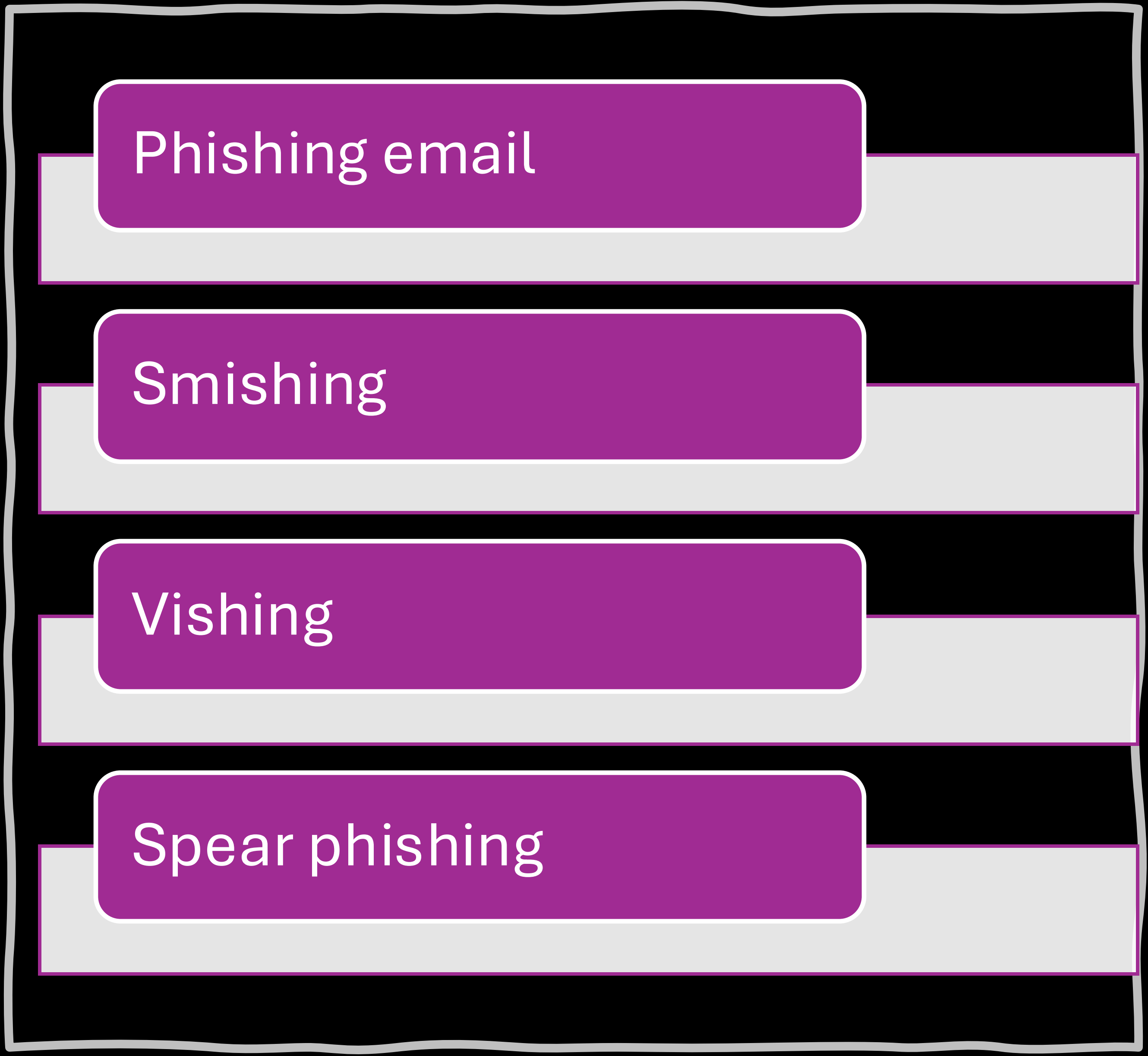
Phishing Awareness Training

By:mahmoud moustafa ibrahim

Common types of phishing attacks:



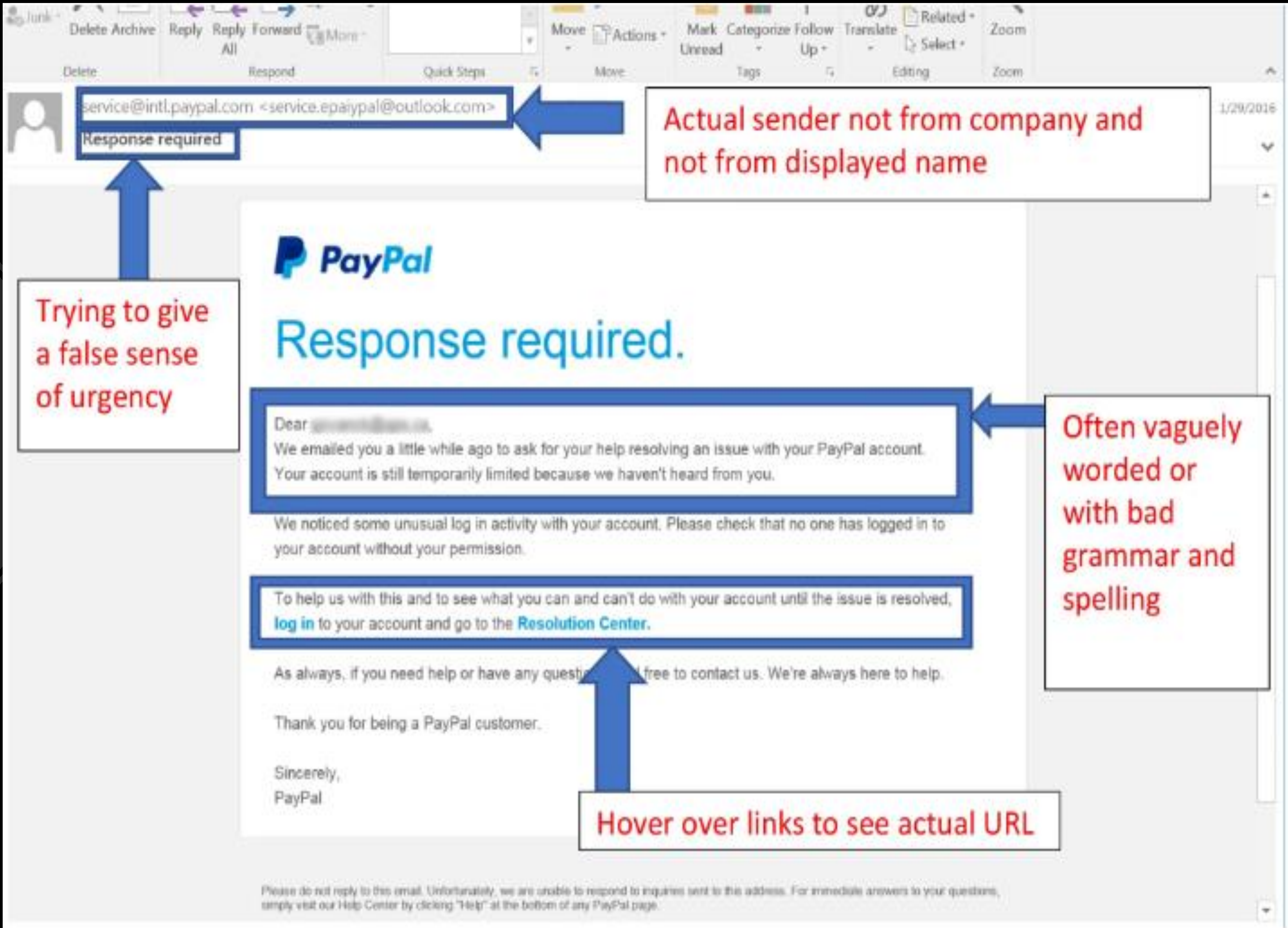
- Phishing email
- Smishing
- Vishing
- Spear phishing

Phishing email

Phishing email is done by the hacker in order to be able to steal passwords or sensitive data, or to encrypt the device’s data, and it relies mainly on social engineering.

The hacker mainly relies on the art of deception, a little understanding of hacking skills, and sometimes a little HTML programming.

An image showing some of the mistakes that can reveal a phishing email



service@intl.paypal.com <service.epaiypal@outlook.com>

Response required

1/29/2016

Actual sender not from company and not from displayed name

Trying to give a false sense of urgency

PayPal

Response required.

Dear [redacted]

We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

Often vaguely worded or with bad grammar and spelling

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

As always, if you need help or have any questi[...] free to contact us. We're always here to help.

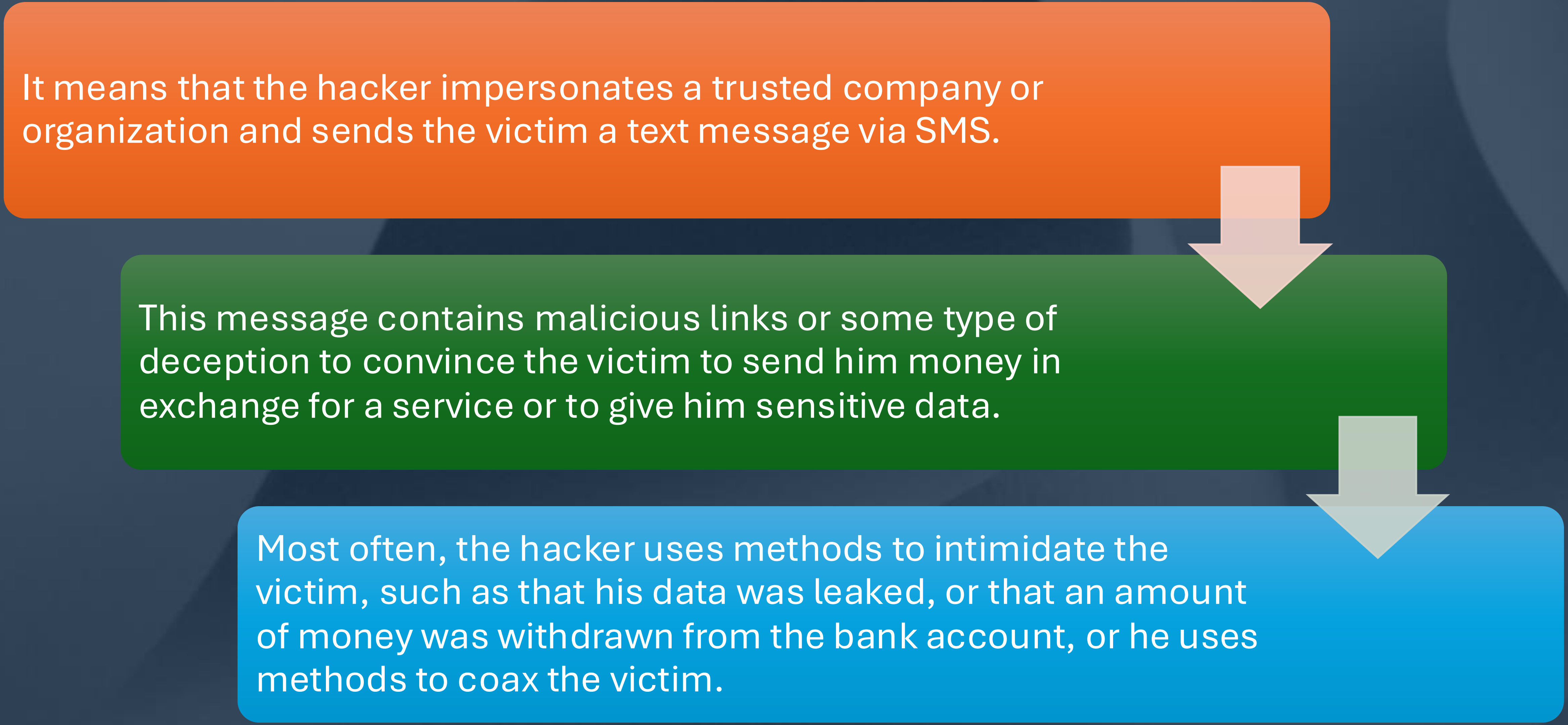
Thank you for being a PayPal customer.

Sincerely,
PayPal

Hover over links to see actual URL

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

Smishing

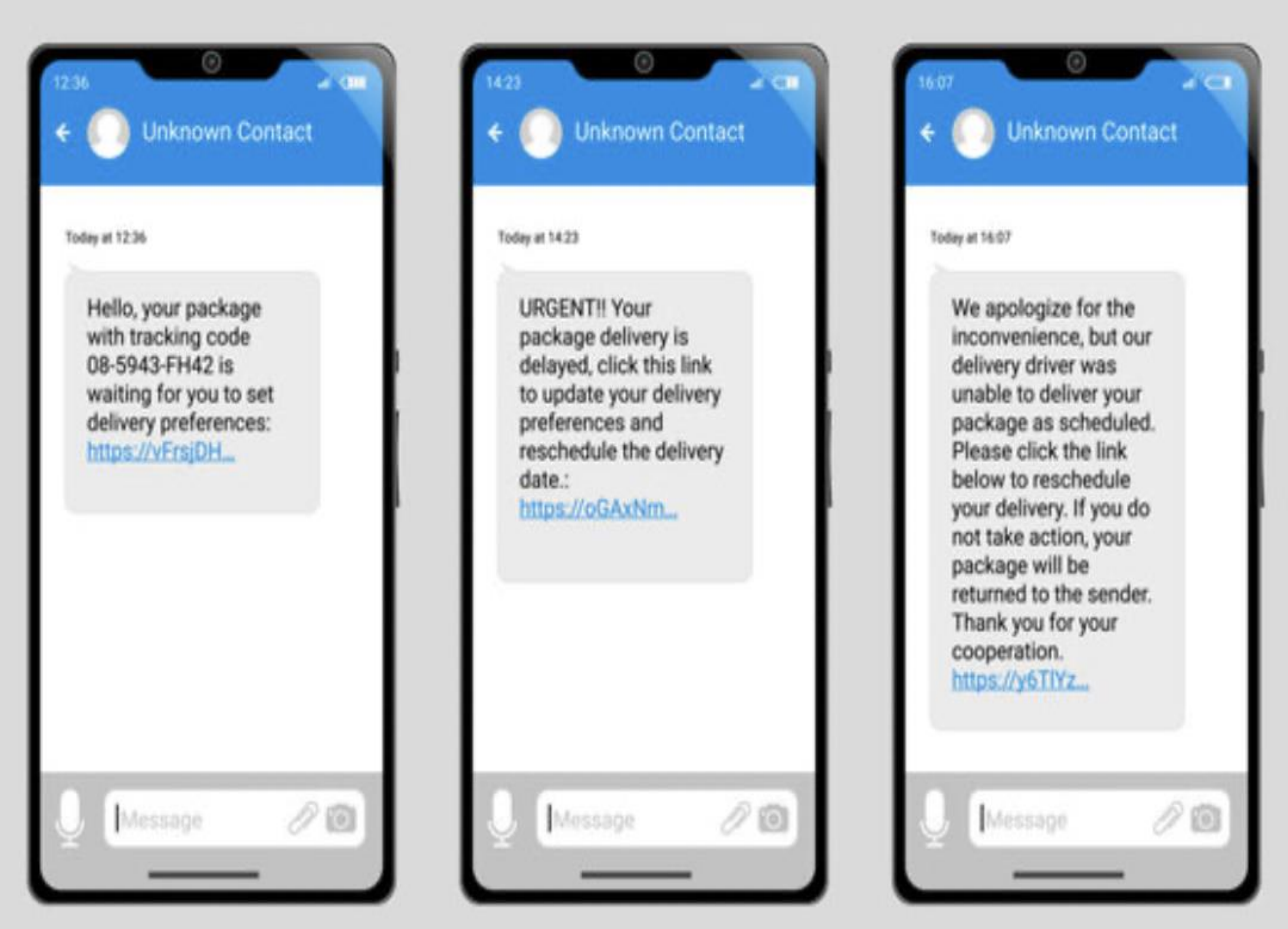


It means that the hacker impersonates a trusted company or organization and sends the victim a text message via SMS.

This message contains malicious links or some type of deception to convince the victim to send him money in exchange for a service or to give him sensitive data.

Most often, the hacker uses methods to intimidate the victim, such as that his data was leaked, or that an amount of money was withdrawn from the bank account, or he uses methods to coax the victim.

This is a real picture of the ways smishing happens



12:36

Unknown Contact

Today at 12:36

Hello, your package with tracking code 08-5943-FH42 is waiting for you to set delivery preferences: https://vFrsjDH...

14:23

Unknown Contact

Today at 14:23

URGENT!! Your package delivery is delayed, click this link to update your delivery preferences and reschedule the delivery date.: https://oGAxNm...

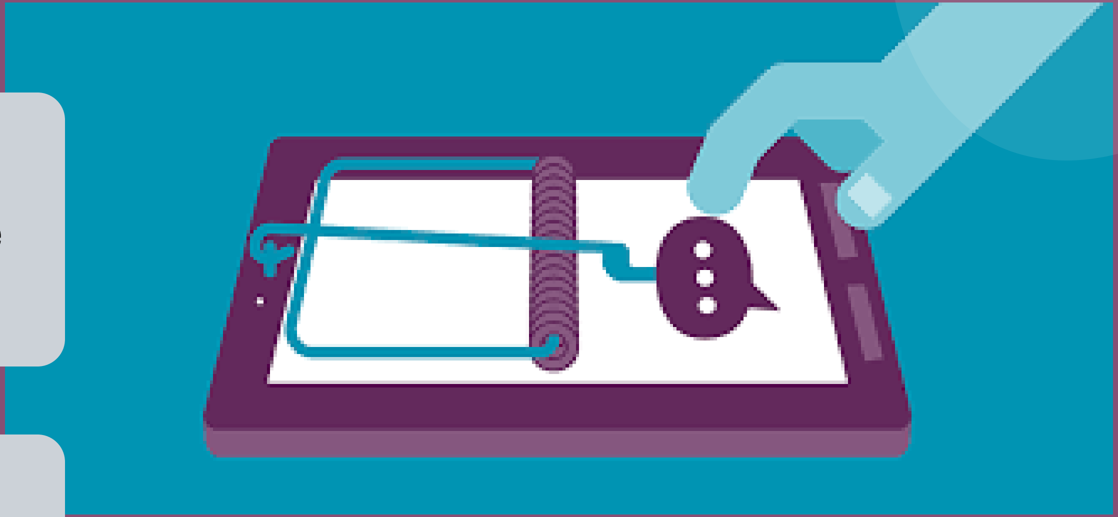
16:07

Unknown Contact

Today at 16:07

We apologize for the inconvenience, but our delivery driver was unable to deliver your package as scheduled. Please click the link below to reschedule your delivery. If you do not take action, your package will be returned to the sender. Thank you for your cooperation. https://y6TlYz...

How can you protect yourself from smishing operations?



Check the number that sent the message, messages from official parties usually come from known or short numbers

Be careful of messages if they contain a spelling or grammar error, as it is a phishing scam

Be careful if the message requests sensitive information. Verified companies usually do not ask the customer for information

Vishing

01

It is a type of phishing where the attacker makes a phone call to the victim Attackers may use identity-swapping techniques to make phone numbers appear to be from trusted parties

02

This also depends on social engineering, where the attacker impersonates a trusted organization to extract sensitive information from the victim.

How to recognize voice phishing?

1

Verify the caller's identity by calling the concerned authority using the official phone number listed on its official website.

2

Be wary of calls that use scare tactics or urgency to get you to take immediate action.

3

Activate unwanted call blocking features on your phone.

Spear Phishing

- All phishing attacks before this were random, but this one targets a specific victim.
- It collects accurate information about a specific person from various sources, such as social media, websites, or even leaked data.
- The hacker's current goal may be to mess with a person, bring down a system, or steal it entirely

How to protect yourself

- You can protect yourself with the methods we presented above, or there are other things.
- This site can help you learn about leaked email and password data

https://haveibeenpwned.com/

- T.his site can help you know if the link, PDF, or file is harmful or not.

https://www.virustotal.com/gui/home/upload

Thank you for reading🤍