

# Phishing Attacks

...what we all want to avoid



[www.ChumrumDigital.com](http://www.ChumrumDigital.com)

# CONTENT



1

WHAT A  
PHISHING  
ATTACK IS



2

RISKS



3

TYPE OF  
PHISHING  
AND HOW TO  
IDENTIFY



4

HOW TO  
PREVENT  
PHISHING  
ATTACKS



5

WHAT TO DO  
IF YOU  
REALIZE  
YOU'VE BEEN  
PHISHED



Q & A

# 1- What is Phishing Attack?



## Phishing vs Fishing



Photo credit to the owner

**Phishing attack is essentially an online scam.**

It starts with some kind of communication - an email, social media, a tweet, a chat message, or an SMS - that is designed to look like it comes from a trusted source.





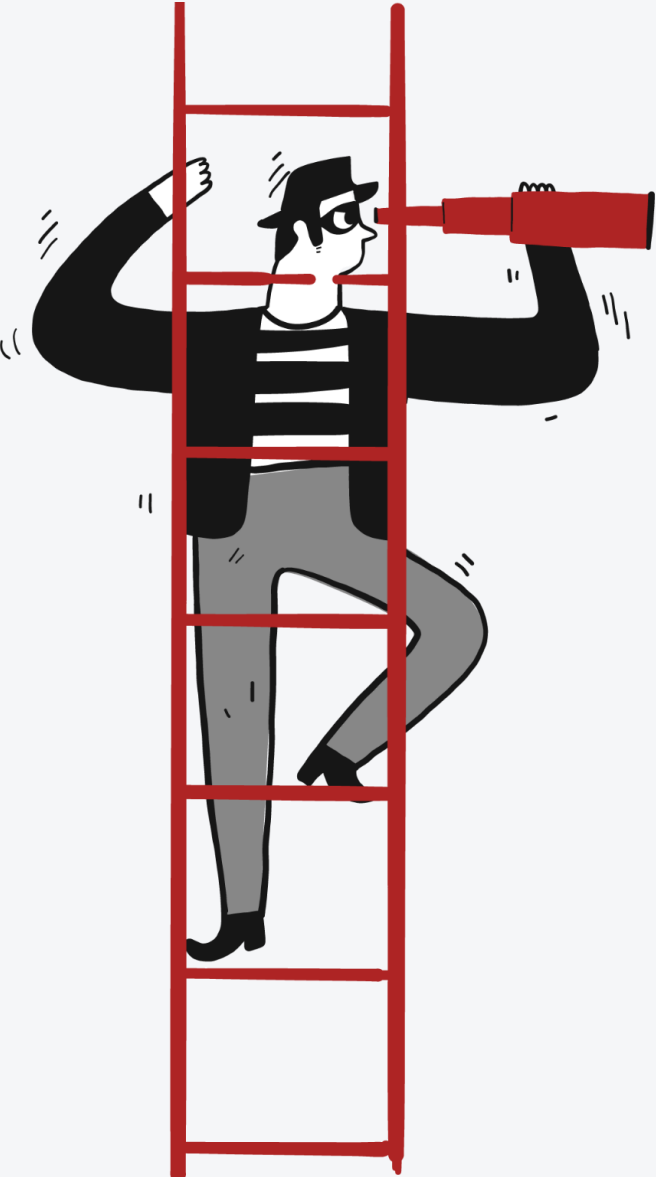
## Phishing attack's common objectives



- Stealing credentials such as username and password (with fake websites)
- Obtaining sensitive or confidential information
- Fraud
- Installing malicious software / ransomware
- Disinformation

## Phishing - Stages of Attack

- Selecting a target
- Collecting information about the target
- Launching the attack
- Following-up with those who fell for the attack
  - This can take the form of ransomware being activated, files being stolen, identity theft... etc



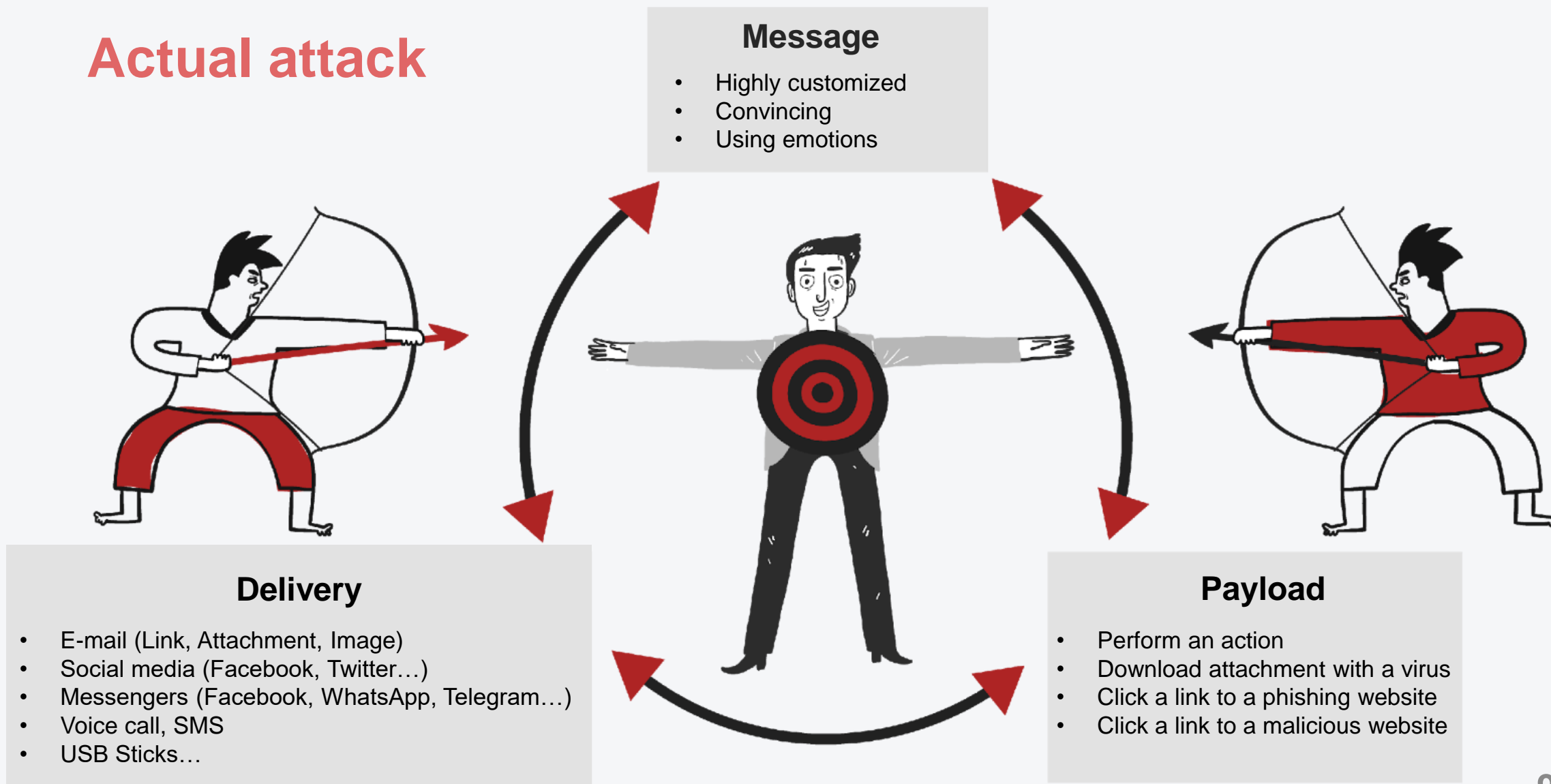
## Sign of Phishing - Common Methods Used

- Rumors (“See what your co-workers said about you!”...)
- Shame (“I have pictures of you doing something horrible...”)
- Hot Topics (“The latest news on...”)
- Emotions (Hate / Sadness / Love / Longing / Nostalgia...)
- Needs / Wants for non-financial things (Residency / Immigration, Conference attendance...)
- Supposed Identity Theft (“Click here to secure your bank information...”)
- Proximity (“I know that you live in xyz city, so do I! Help me out!”)
- Character (“I know that you work on human rights like me...”)
- Greed (“You’ve won TONS of money!”)
- Religious holidays (“Look at this card for [Holiday-Name] that your colleagues made!”)
- Knowledge / Process Insecurity (“YOU DIDN’T PROPERLY SETUP AUTHENTICATION!”)
- Reputation (“You have a message from the United Nations!”)
- No HTTPS and Forged Links (<http://accounts.googl.e.me>)



# 1- What is Phishing Attack?

## Actual attack



## 2- Risks



### Personal Risks



**Money stolen** from your bank account



**Fraudulent charges** on credit cards



**Lost access** to photos, videos, and files



**Fake social media** posts made in your accounts



**Cybercriminals impersonating you**, putting friends or family members at risk

### At Work Risks



**Loss** of corporate funds



**Exposing** personal information of partners, coworkers, and customers



**Files** becoming locked and inaccessible



**Damage** to your organization's reputation




### **3- Types of Phishing and How to Identify**

### E-mail Phishing

The most common form of phishing, this type of attack uses tactics like phony ***hyperlinks*** to lure email recipients into sharing their personal information.

## E-mail Phishing Example – Fake Facebook



The image shows a screenshot of a phishing email that mimics a Facebook password reset notification. The email header has a blue bar with the word "facebook" in white. The body of the email contains the following text:

Hi,

Your Facebook password was been reset on Friday, December 12, 2014 at 07:42PM (UTC) due to suspicious activity of your account.

Operating system: Windows  
Browser: Mozilla Firefox  
IP address: 52.184.64.215  
Estimated location: Hubbard, OH, US

To restore the password complete this form, please, your request will be considered within 24 hours.

Thanks,  
The Facebook Security Team

---

Facebook, Inc., Attention: Department 425, PO Box 10005, Palo Alto, CA 94303

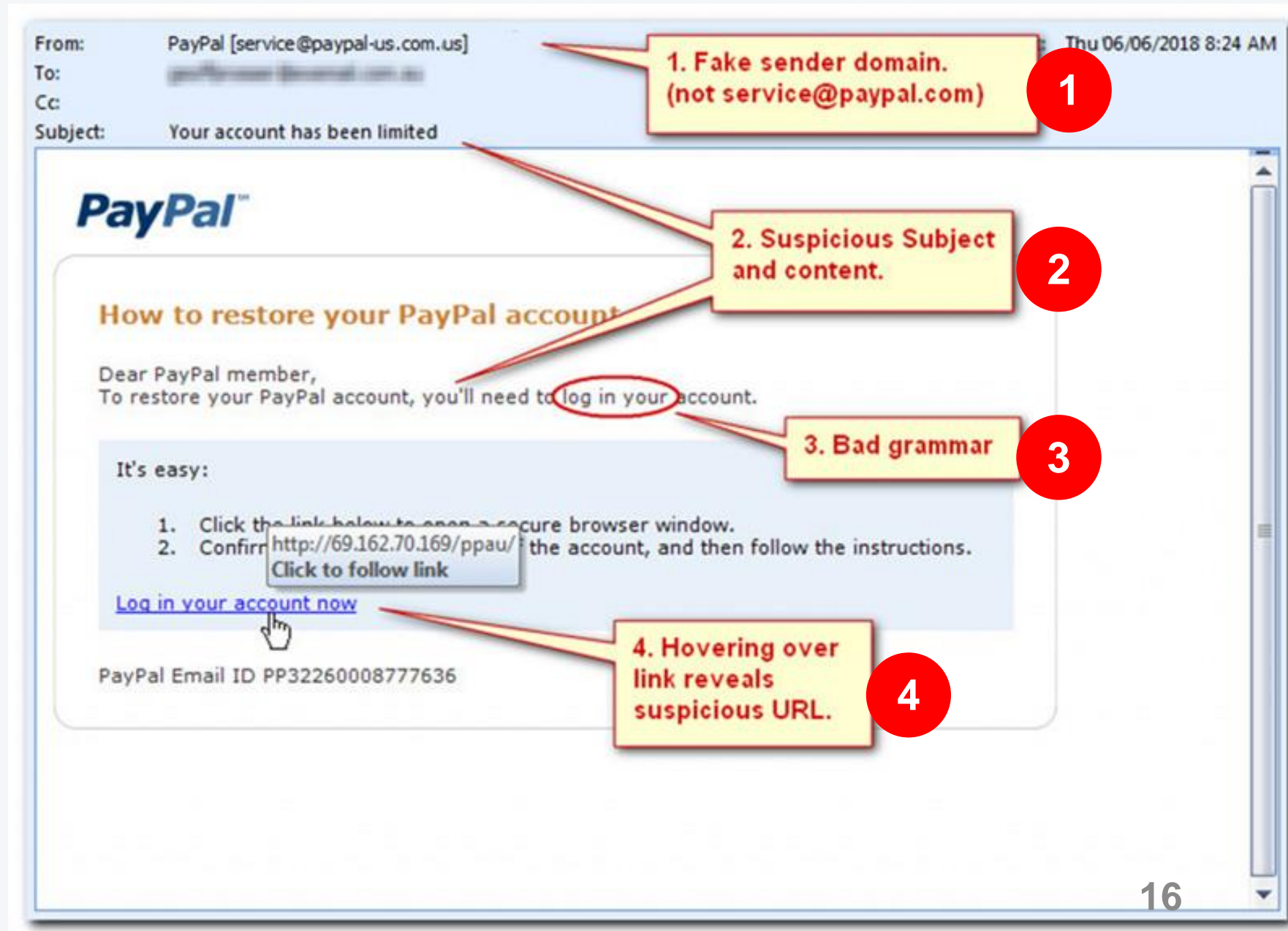
At the bottom, there is a long, complex URL: `gazetabrasovului.ro/lib.php?fb=+pQF0syZIOPFHR9ITmPR/aM4QIG4ZasPrgiSapqdMWs=`

Annotations on the image include:

- 1**: A red circle with the number 1 and an arrow pointing to the word "Hi," which is enclosed in a red box.
- 2**: A red circle with the number 2 and an arrow pointing to the underlined text "complete this form". A red box labeled "Hover over the link" is positioned above the text, with a red arrow pointing to the underlined text. Below this, another red box labeled "This link does not go to facebook!" has a red arrow pointing to the underlined text.
- 3**: A red circle with the number 3 and an arrow pointing to the long URL at the bottom of the email.

# 3- Types of Phishing and How to Identify

## E-mail Phishing Example - Fake PayPal



**From:** PayPal [service@paypal-us.com.us] **To:** [redacted] **Cc:** [redacted] **Subject:** Your account has been limited Thu 06/06/2018 8:24 AM

**1. Fake sender domain. (not service@paypal.com)**

**2. Suspicious Subject and content.**

**3. Bad grammar**

**4. Hovering over link reveals suspicious URL.**

**PayPal™**

**How to restore your PayPal account**

Dear PayPal member,  
To restore your PayPal account, you'll need to log in your account.

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm <http://69.162.70.169/ppau/> the account, and then follow the instructions.

[Log in your account now](#)

PayPal Email ID PP32260008777636



### Vishing attacks

It is a phone scam. Scammers carrying out such attacks often pose as employees from government agencies or bank, etc.

## Vishing Example



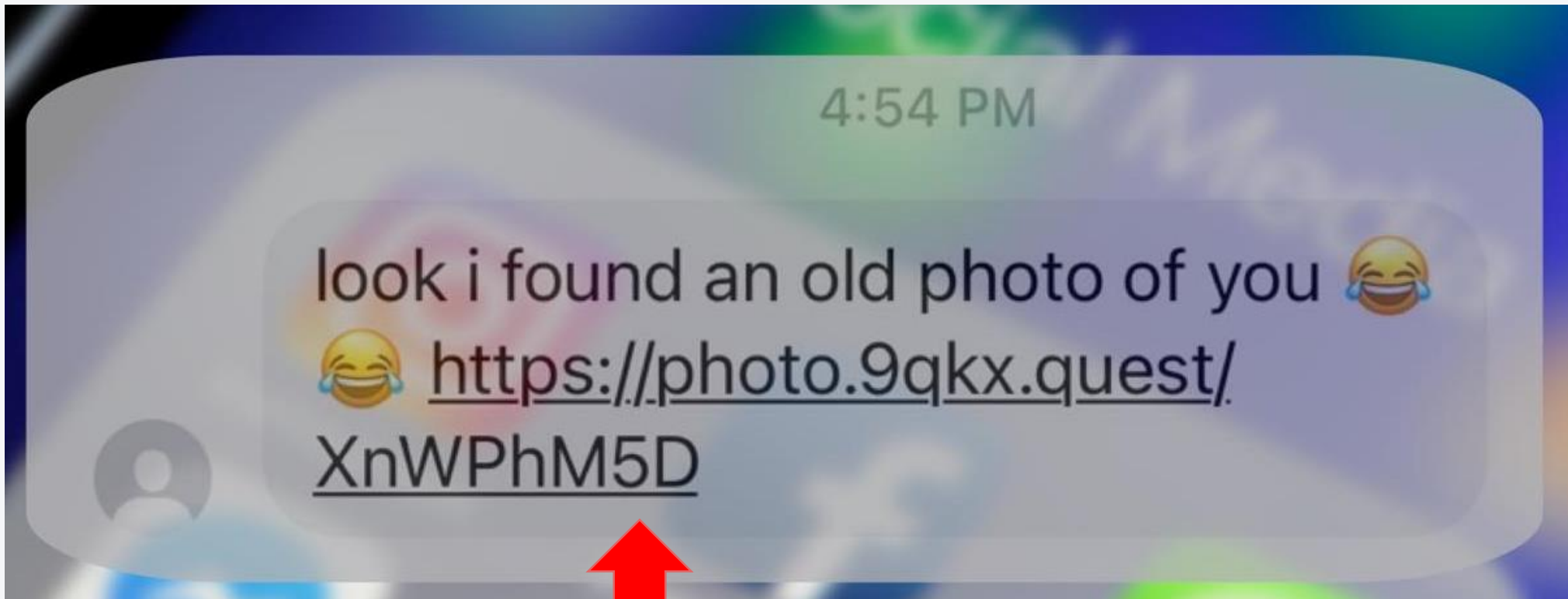
Photo credit to the owner

### SMiShing attacks

It involves SMS messages (texts). Attacker may impersonate someone you know to ask for money or personal information.

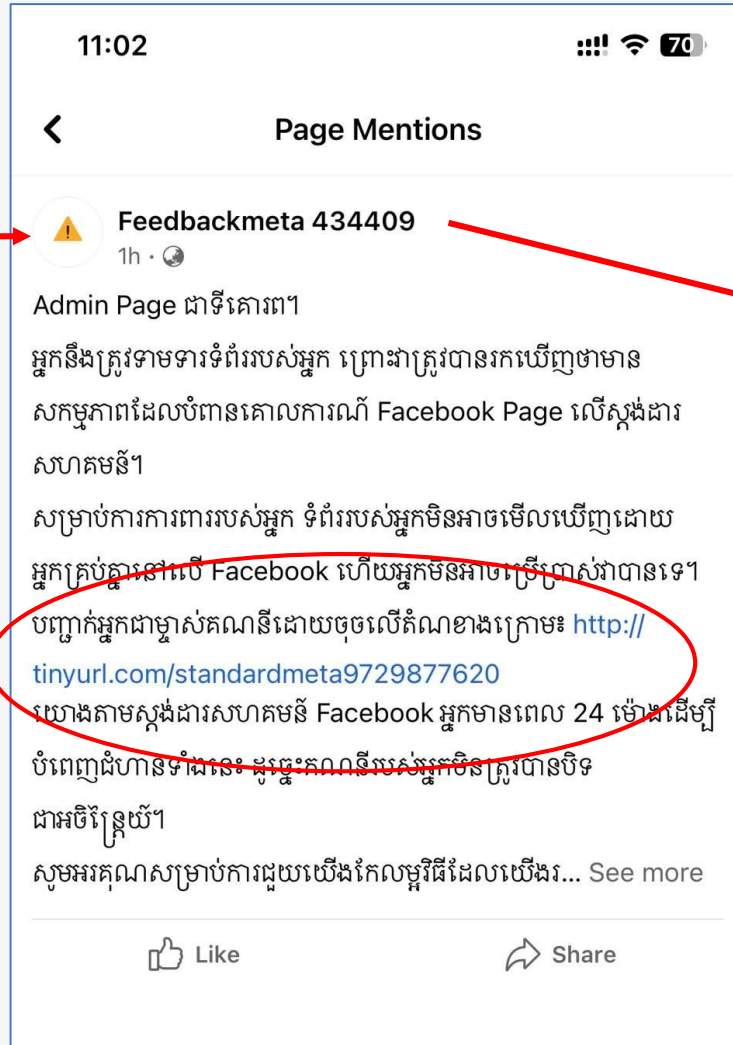
Increasingly often they pose as WhatsApp, Facebook or another social media to ask you for the verification code that you receive via the platform.

## SMiShing Example – SMS with fake website



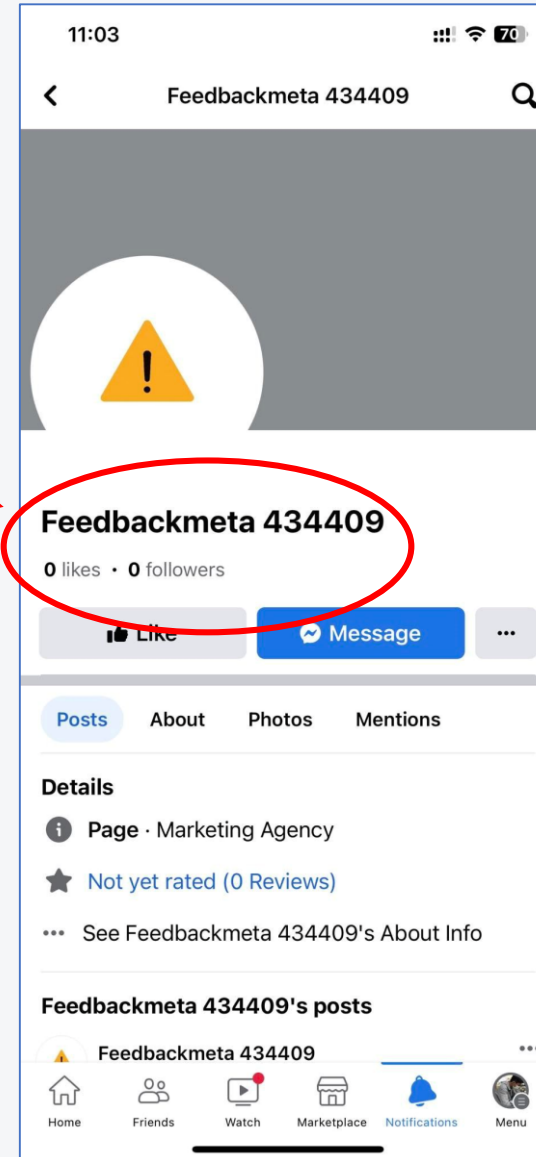
## SMiShing Example - Facebook

1

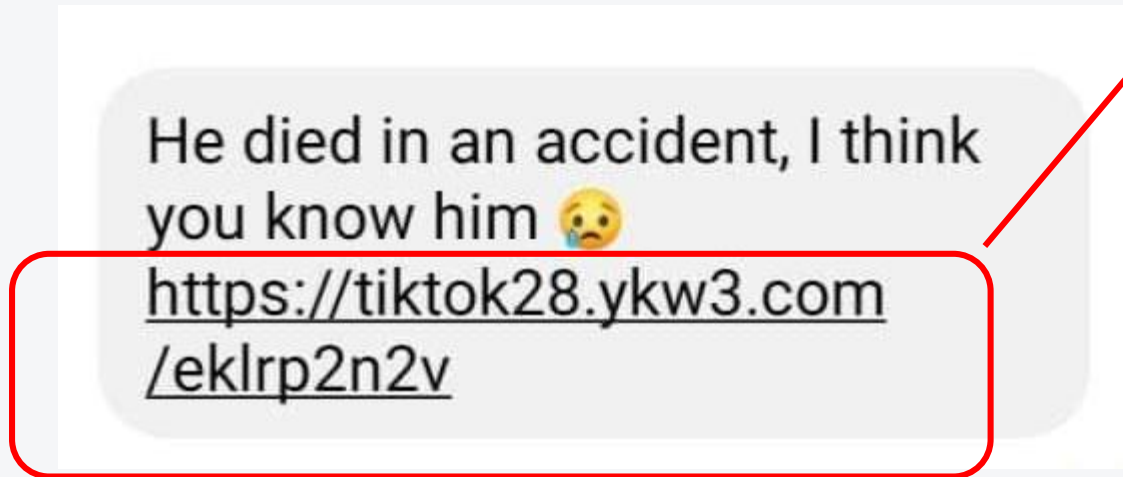


2

3



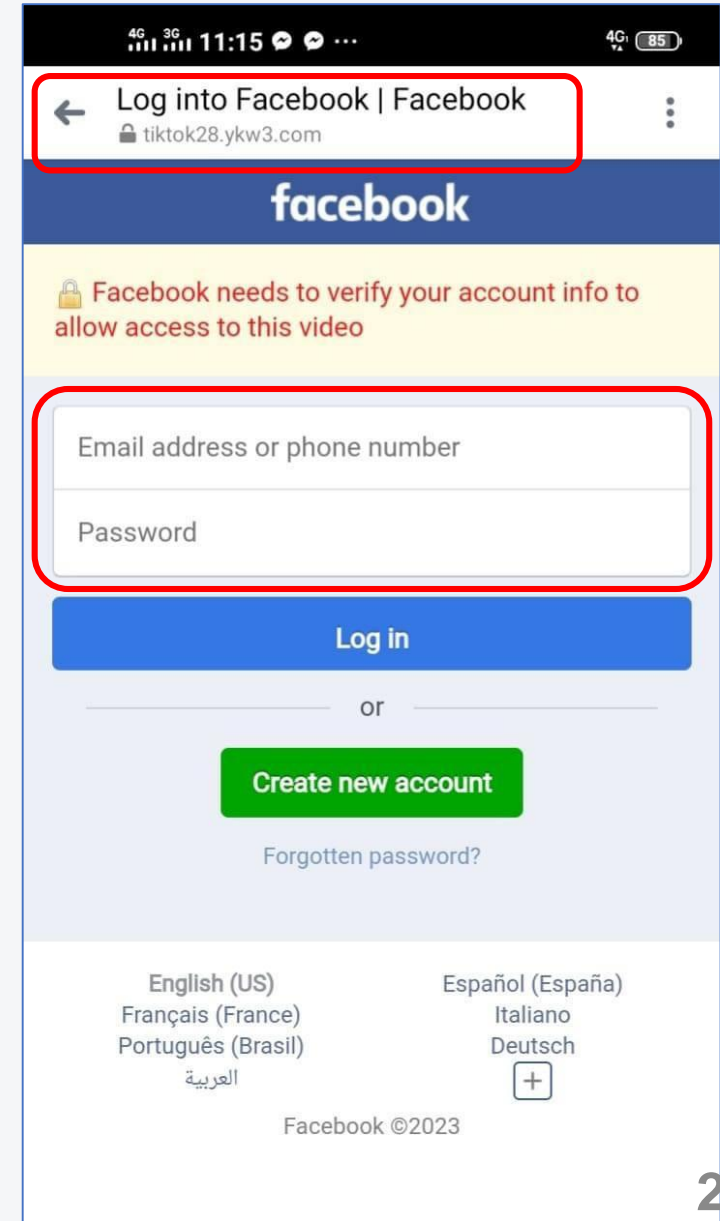
## SMiShing Phishing Example - Fake Facebook



1

2

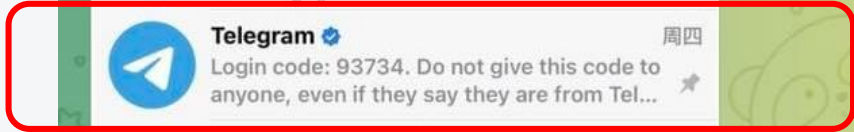
3



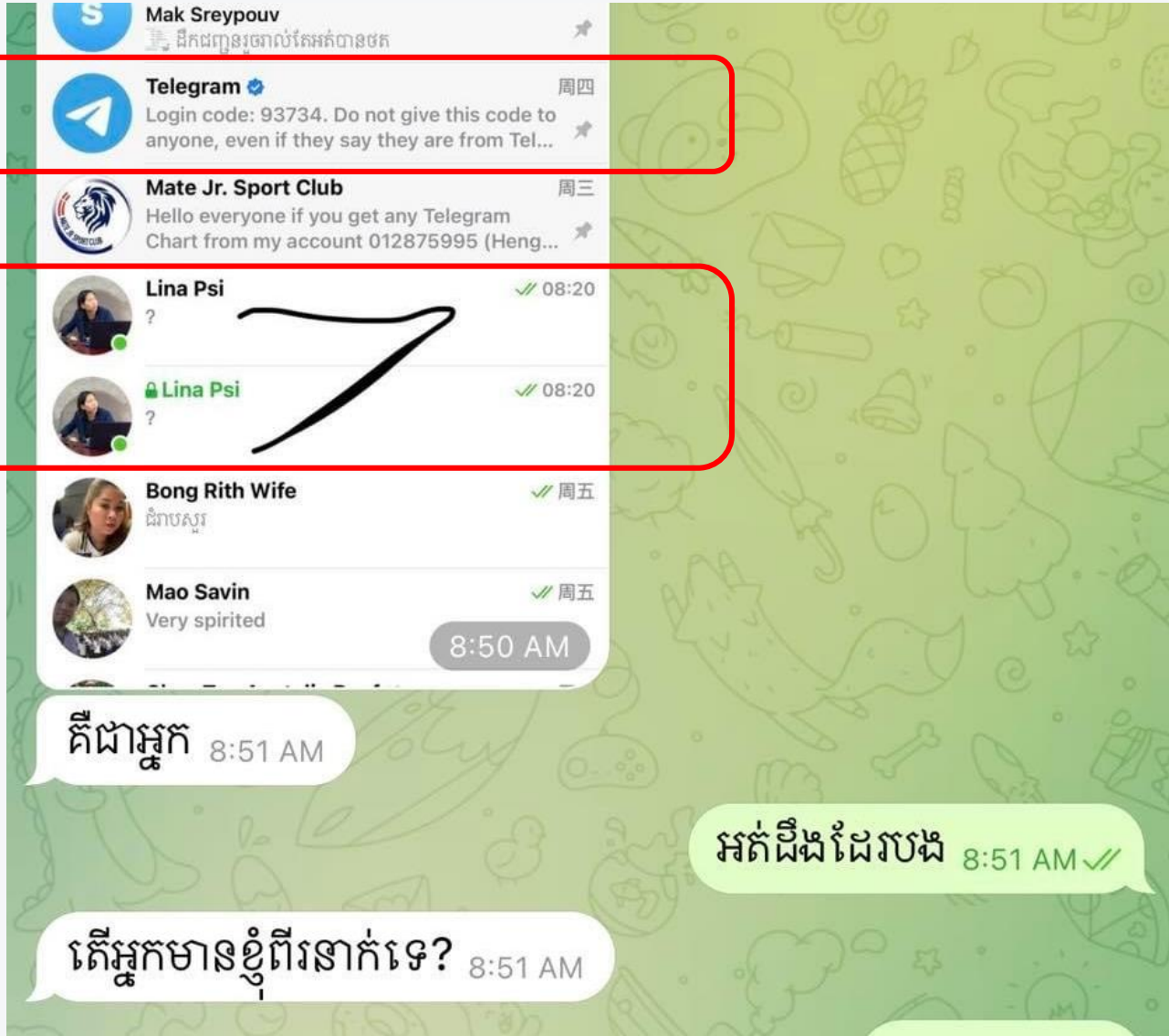
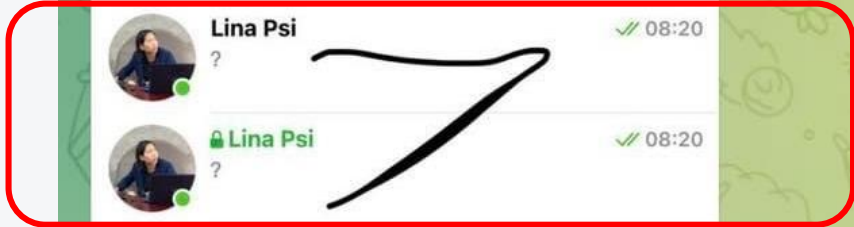
## SMiShing Example - OTP Code Telegram

**DO NOT  
SCREENSHOT**

1



2



## SMiShing Example - Fake Website



The diagram illustrates the flow of a SMiShing attack. It starts with a social media post (1) containing a long URL (2) and a domain name (3). An arrow points to a mobile phone screen (4) showing a fake website with a congratulatory message (5) and instructions to share the post to claim a prize.

**1** → <http://fbencmklab.rhzriq.tw/74e4W0hRfWpeVAVjWHoNUQRRU1tWYEFxP1ABGAEAIQM4XTAGCkUAIDsZUBwDORgMMQR0K1waJlEpJ2RaCSg?flm1645414786988>

**2** → **Kampuchea TELA 25th Anniversary Gift!**

**3** → fbencmklab.rhzriq.tw

**4** → **z6xe0qc.cn**

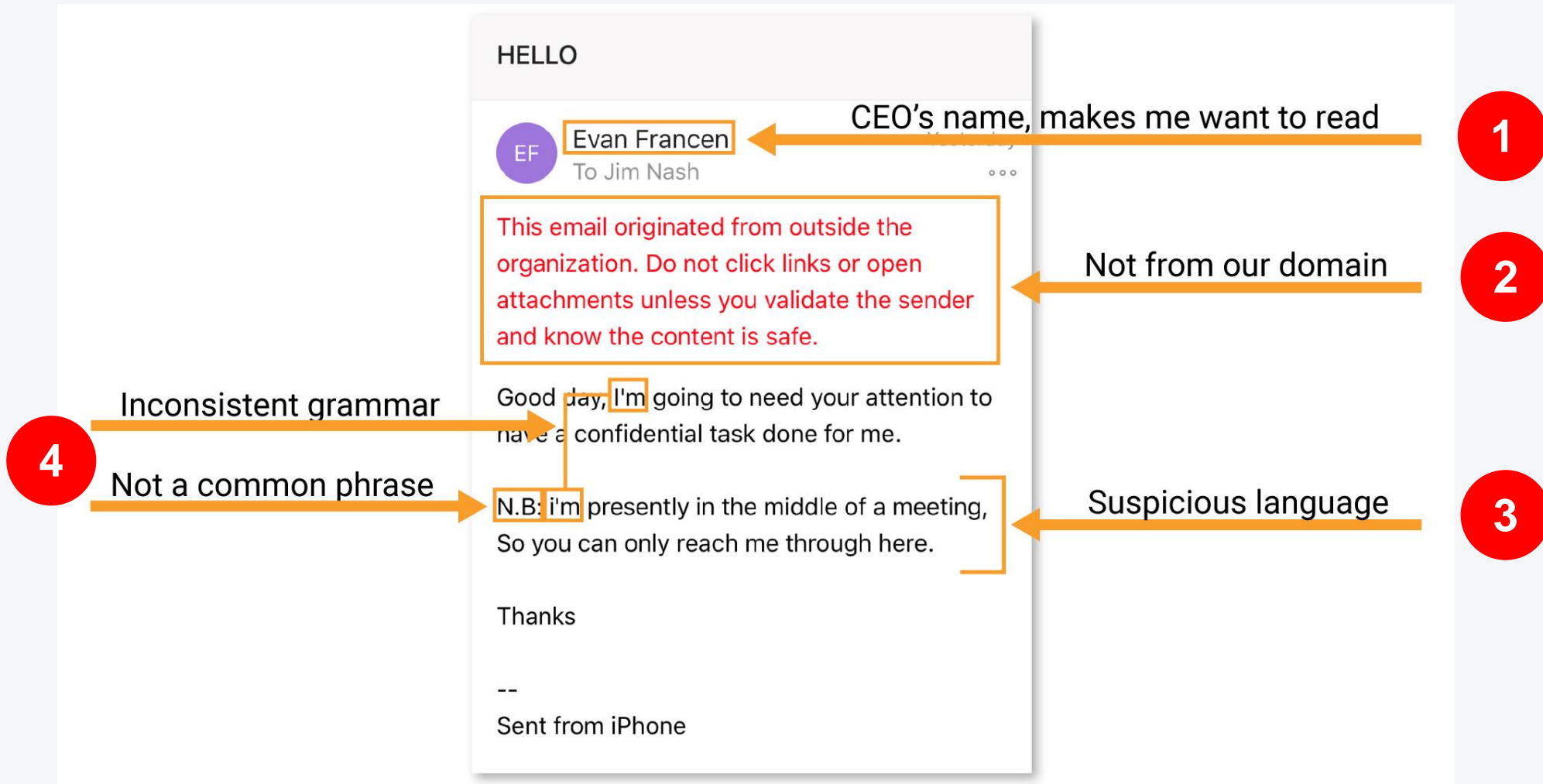
**5** → **Congratulation!**  
Your prize is: 1000000 ៛, Follow the instructions on the next page to claim your prize !  
1. Share with 5 groups/20 friends (click the "Share" icon below)  
2. Click "Continue" and claim your prize.



### Spear phishing

**Spear phishing** is attack that target a ***specific person*** through email, social media, SMS, or chat messages that look convincingly like they come from someone the target knows – like a colleague or friend.

## Spear Phishing Example



The image shows a screenshot of an email with several annotations identifying red flags for spear phishing. The email content is as follows:

HELLO

**EF** Evan Francen  
To Jim Nash

This email originated from outside the organization. Do not click links or open attachments unless you validate the sender and know the content is safe.

Good day, I'm going to need your attention to have a confidential task done for me.

N.B: i'm presently in the middle of a meeting, So you can only reach me through here.

Thanks

--  
Sent from iPhone

Annotations and their corresponding red flag numbers:

- 1**: CEO's name, makes me want to read (points to the sender name 'Evan Francen')
- 2**: Not from our domain (points to the warning box)
- 3**: Suspicious language (points to the N.B. note)
- 4**: Inconsistent grammar (points to 'Good day, I'm') and Not a common phrase (points to 'N.B: i'm')

### Whaling attacks

**Whaling attacks** are spear phishing attacks that target the “**big fish**”, such as ***heads of organizations*** and ***owners or chief editors of media organizations***

## Whaling Phishing Example

From: David McFaddin <[biojasinti1980@aol.com](mailto:biojasinti1980@aol.com)>

Sent: Wednesday, January 09, 2019 3:42 PM

To: [REDACTED]

Subject: Payroll

Krista,

I have recently had to change my direct deposit information and would like to have my paycheck deposited to my new account.

I need your prompt assistance in this matter.

Thank you,  
David McFaddin

## 4- How to Prevent Phishing Attack



**Think before you click!**

### Best Practices:

1. Continue learning
2. Do not post / reveal personal information on social media
3. Do not provide your personal information via link attached in emails / messages
4. Do not believe in words of comfort, lure or fall for reward offering trick
5. Check the link carefully before clicking by hovering over the link with the mouse
6. Make sure the sender's email address is legitimate
7. If you don't know that sender, DO NOT click the link
8. Delete the suspicious message
9. If you receive an email asking to provide confidential information or change your password, try verifying it with the relevant source first
10. Do not install unnecessary software and update the software regularly
11. Update apps on smartphone regularly
12. Update OS both on computer and smartphone regularly
13. Never share your password with others
14. Enable the two-factor authentication
15. NEVER give away your 6 digit OTP code to anyone



### Before you click:

- Verify Sender's email address & Reply to Address
- Is it sense of Urgency?
- On any email client: You can examine hypertext links
- Use <https://unshorten.it/> to reveal the short URL to a real URL
- Use <https://www.virustotal.com/> to check the URL or attached files



## **5- What to do if you realize you're been phished**



**If you have clicked on a phishing link and entered your login details or credit card information into a fake website:**

1. Do not panic.
2. Change your password.
3. Cancel your credit card and notify your bank.
4. Check to see if attacker hasn't entered a strange email, phone number, or secondary email address.
5. Check other accounts linked to your email if attacker has not tried to reset the password.
6. Change password for all accounts if you use the same password.
7. Let your contacts know you have been phished.
8. Tell your Org's IT person about this phished.
9. If you've been logged out of the account, reach out to the platform.

### You got phished and downloaded a virus - what do you do now?

1. Do not panic.
2. Disconnect the device from the internet.
3. Check to see if you still can access to the device, or are you locked out (by ransomware).
4. If possible, contact a digital security expert (Your Org's IT person, or a trusted local IT specialist).
5. Run antivirus scanner if you still can access your device.
6. If you no longer have access to your device, ask your IT person to wipe your device and restore your latest backup.
7. Tell your contacts and colleagues that you have been phished.

# Thank You!



**ជំរុំឌីជីថល**



**Website**

chumrumdigital.com



**Facebook**

chumrumdigital



**Instagram**

chumrum\_digital



**Telegram**

<https://t.me/chumrumdigital>



**E-mail**

meet@chumrumdigital.com

Q&A

