


Cyber Tales by Tenali

- a fortnightly series



CEO EMAIL SCAM


यूको बैंक **UCO BANK**
 (भारत सरकार का उपक्रम) (A Govt. of India Undertaking)
 सम्मान आपके विश्वास का Honours Your Trust

Cyber tales by Tenali
 Vol 20, September 2021, II Issue

Published by:
 UCO Bank, CISO Office

What's Inside:

1. Introduction & Cover Story of CEO Email Scam
2. How this Scam works
3. How to recognize CEO Email Scam
4. Safety measures & Advisories



Phishing scams existed for several decades and continued as a major problem in today's world. It is a popular method of stealing credentials and distributing malware. Attackers are adopting multiple new and innovative methods to trick senior executives or other high-profile individuals of an establishment for siphoning off money or access sensitive information for malicious purposes. Such attempts have increased multifold during Pandemic.

Today I will give you an example of an advanced phishing scam which often target or impersonate CEOs or other Top level executives of an establishment.

How Mr. Chandu was Targeted ?

Mr. Chandu was working at ABC Company in the post of Finance Manager. One day, he received an email from his Managing Director & CEO.



From: Sarin Khurana, CEO & MD <ceo.webmail.1337@hotmail.com>
To: Chandu Sur <chandu.sur@abc.co.in>
Subject: Urgent Payment instruction

Mr. Chandu,

As I'm tied up in a meeting and there is something I need you to take care of.

An important payment for a consultant that was supposed to go out in the last week has to be completed immediately. **Transfer Rs.49000/- asap** to below account details and send me the confirmation.

Name: P Shaw, Account No:3215XXXXXXXXXX, IFSC: KBIC0003215,
Bank Branch: KBI Bank, XYZ Branch

Can't take calls now, an email will be fine.

MD & CEO
ABC COO.

CEO EMAIL SCAM... Contd

Mr. Chandu immediately completed the payment and sent the payment confirmation by replying to the previous mail.



Respected Sir,
Payment of Rs.49000/- has been done for the consultant. Payment Ref No. 0000XXXX.

Regards
Chandu Sur

After sometime he got an another email from his MD.

Amount Wrongly mentioned in previous email !

Mr. Chandu,
In hurry the amount had been mistaken. It will be 94000/- instead of 49000/-. Transfer balance amount immediately to the consultant and send me the confirmation asap.



This time Mr. Chandu was a little bit surprised. Since MD was busy in a meeting, he could not call his MD for confirming the same.. He waited for a while. After 5 minutes he saw an another email.

You will be fired if you don't make the payment asap !

Mr. Chandu,
Have you not understood the urgency of the payment ? You will be fired if you will not transfer the balance amount in 5 minutes.

MD & CEO



Seeing the threatening language of the email, Mr. Chandu got suspicious. He then called Tenali and briefed the complete scenario.



Hello.. Tenali..

Mr. Chandu! How could you be so sure that the mail was actually been sent by your MD?



The name displayed in the mail is same as of our MD's Name and the email also looked genuine to me.

Have you matched the Name with the sender's email address? Have you checked whether the email has been sent from your official domain or not?



Mr. Chandu again checked the sender mail address.

Display Name

From: Sarin Khurana, CEO & MD
<ceo.webmail.1337@hotmail.com>



Oops !

Domain Name

Office domain is
abc.co.in

After verifying the domain name with his official mail, he understood that he has been duped by a Fake Email Id.

Oh No! I was absolutely confused to see my MD's Name and totally overlooked the email address. I have transferred Rs.49000/- to the fraudster's account mentioned in it. What should I do now?



CEO EMAIL SCAM... Contd

Immediately go to the nearest Cyber Crime police station with all copies of emails and file an FIR. With the FIR copy and payment confirmation inform your bank and also Lodge a complaint in National Cyber Crime Reporting Portal. Don't forget to report it to your MD and IT Security Department of your office.



WHAT HAPPENED HERE?

Here Mr. Chandu got victimised by a different kind of email phishing scam named "Whaling" or sometimes it is called as "CEO Fraud". CEO fraud is a type of cybercrime where attackers impersonate a company's CEOs or MDs, or other Top level executives in order to trick an employee into sending unauthorized fund transfers or divulging sensitive information.



How This type of scam occurs?

1



Fraudsters research potential victims and their companies online, learning everything they can from the organization's website, as well as information from social media sites.

2 THE TARGETS



Mid-level staff members of the Sensitive Departments.



3

→ Crafts highly realistic-looking email.



→ Appears to come from the company's CEO or another high-level executive.

→ Uses gathered information about the target to make the email seem authentic.

IMPORTANT ADVISORY

- ✓ Do not open emails or download attachments from unknown or untrusted senders.
- ✓ Correlate the Display Name & the sender's email address.
- ✓ Avoid responding or clicking links on unsolicited or spam email. Simply delete those emails which come from suspicious mail id.
- ✓ Do hover over hyperlinks at emails to know exact URL address.
- ✓ Always check the domain name of email sender. UCO Bank's Official domain is "ucobank.co.in".

Beware of Email Scams !



Cyber Guru

Tenali's Mantra

KEEP EYES OPEN

Don't Rush.

**Examine Email Closely
Before Doing Any Act**

CEO EMAIL SCAM... Contd



Examine Email Closely to recognize CEO Email Scam ?

Mismatches between the sender's display name and email address

impersonates CEO or top-level executives

unofficial domain of email sender

creates urgency to act immediately

Often says email sender executives are unavailable for communications for the period

asks for immediate action

requests for money transfer to unusual account number

requests secrecy or confidentiality which prevent employees for checking the legitimacy of the request with other employees

spelling of establishment may be changed

MD & CEO ABC COO.

From: Sarin Khurana, CEO & MD <ceo.webmail.1337@hotmail.com>
To: Chandu Sur <chandu.sur@abc.co.in>
Subject: Urgent Payment instruction

Mr. Chandu,
 As I'm tied up in a meeting and there is something I need you to take care of.
 An important payment for a consultant that was supposed to go out in the last week has to be completed immediately. **Transfer Rs.49000/- asap** to below account details and send me the confirmation.
Name: P Shaw, Account No:3215XXXXXXXXXX, IFSC: KBIC0003215,
Bank Branch: KBI Bank, XYZ Branch
 Can't take calls now, an email will be fine.

Scan this QR Code to Download & know the whole story

Stop Look Think Act

In case you have fallen prey to any such fraud - **REPORT IMMEDIATELY TO THE NEAREST CYBER CRIME POLICE STATION & NATIONAL CYBER CRIME REPORTING PORTAL**

<https://cybercrime.gov.in>

We welcome your valuable suggestions / feedback at ciso.office@ucobank.co.in