



# Phishing and Countermeasures

A COMPREHENSIVE GUIDE TO  
**IDENTIFY & AVOID PHISHING**



BY CISO OFFICE

**यूको बैंक**  **UCO BANK**  
(भारत सरकार का उपक्रम) (A Govt. of India Undertaking)

सम्मान आपके विश्वास का

Honours Your Trust

यूको बैंक



**UCO BANK**

विज़न

सूचना की सुरक्षा हेतु बैंक के लिए  
एक सुरक्षित साइबर स्पेस बनाना

*Vision*

*To build a secure and resilient cyber space for the Bank to  
protect information*

मिशन

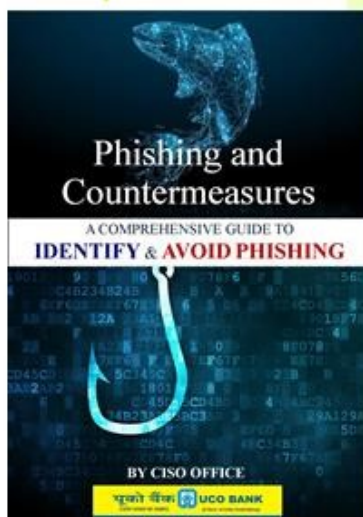
बैंक की बुनियादी संरचना, व्यक्ति, प्रक्रिया और प्रौद्योगिकी के सम्मिलन से  
साइबर स्पेस में सूचना तथा बुनियादी संरचना की सुरक्षा करना, साइबर के  
खतरों को रोकना एवं अनुक्रिया करना

*Mission*

*To protect information and information infrastructure in  
cyber space, build capability to prevent and respond to  
cyber threat, reduce vulnerabilities and minimize damage  
from cyber incidents through a combination of the Bank  
infrastructure, people, process and technology*

# What's Inside

A COMPREHENSIVE GUIDE TO  
IDENTIFY & AVOID PHISHING



### Table of Contents

- > Introduction
- > What is Phishing? Why do we become victims?
- > The Cost of not being Cyber Aware
- > Importance of Phishing Awareness & Mitigation
- > Understanding Phishing Techniques -
  - Email Phishing
  - Vishing
  - Smishing
  - Spear Phishing
- > Anatomy of Phishing Attack
- > Phishing Attack Life Cycle
- > Phishing Attack Vector & Common Entry Points
- > Social Engineering Tactics exploited in Phishing
- > Recognizing Phishing Attempts
  - Identifying Suspicious Emails
  - Spot Fake SMS
  - Indicators of Fake Website
- > Best Practices for End Users
- > Case Studies on Phishing Attacks
- > Reporting of Cyber Fraud Incidents & Phishing
- > Conclusion



## From the Desk of MD & CEO



**Dear UCOites,**

In an era where technology is the cornerstone of modern finance, it is imperative that we understand the risks that accompany its advancements. Phishing, a sophisticated cyber threat, preys on vulnerabilities in the digital landscape.

*"Phishing and Countermeasures: A Comprehensive Guide to Identify & Avoid Phishing"* is more than just a compendium; it is a testament to our collective commitment to cyber-security. It embodies our relentless pursuit of knowledge, our determination to stay one step ahead of cybercriminals, and our unwavering dedication to our customers' trust.

My appreciation to CISO Office team who contributed to this endeavour. Their diligence and passion have yielded a resource that will undoubtedly serve as a beacon of knowledge and empowerment for our employees and customers alike.

As we delve into the pages of this guide, let us remember that cyber-security is a shared responsibility. Each one of us plays a pivotal role in protecting our Bank's reputation, our customers' confidential information, and our Brand image.

I urge all UCOites to absorb the wisdom imparted within these pages, to apply its lessons in daily interactions, and to share this knowledge with your colleagues, friends, and family members. Together, we will fortify UCO Bank's digital fortress against the ever-evolving landscape of cyber threats.

Best wishes,

**(Ashwani Kumar)**

**MD & CEO**



## From the Desk of Executive Director



**Dear UCOites,**

In an era defined by rapid technological advancements, the digital landscape presents us with endless opportunities and conveniences. However, it also exposes us to various risks, and none more insidious than phishing attacks. I always believe that knowledge is our most potent weapon against cyber threats. The compendium "*Phishing and Countermeasures: A Comprehensive Guide to Identify & Avoid Phishing*", is a testament to that belief.

Phishing attacks, with their cunning tactics, have become increasingly sophisticated, making it imperative for us to equip ourselves with the insights required to navigate this landscape securely. "Phishing and Countermeasures" is not just a book; it is a shield forged through collective effort and dedicated research. It offers a comprehensive understanding of phishing techniques and, more importantly, empowers us with effective countermeasures.

As we embrace this guide, remember that cyber-security is not the responsibility of a single department or individual. It is a shared duty, a commitment we all undertake to safeguard our digital realm. Let this compendium serve as a constant reminder of our collective responsibility to remain vigilant, to question, and to learn.

I appreciate the good work done by CISO Office team who have made this compendium a reality. I urge all UCOites to equip with the knowledge it imparts, and spread this knowledge far and wide. Together, we will bolster UCO Bank's defenses against the challenges of the digital era and emerge even stronger and more resilient than before.

Best wishes,

**(Rajendra Kumar Saboo)**

**Executive Director**



## From the Desk of Chief Information Security Officer



**Dear Colleagues,**

In a world where our digital interactions have become second nature, the threat of Phishing looms large, exploiting vulnerabilities in even the most robust systems. It is our continuous endeavor to counter unceasing efforts to raise awareness and enhance our resilience against these cyber threats.

*"Phishing and Countermeasures"* is more than just a compilation of information; it represents our commitment to knowledge dissemination and empowerment. It is a testament to our determination to equip our staff members with the tools and insights necessary to navigate the treacherous waters of the digital realm.

As you delve into the pages of this comprehensive guide, remember that each piece of information, strategy discussed, is designed to empower you. In a landscape where a single click can have far-reaching consequences, awareness and proactive steps are the foundation of our defense.

Let this compendium be your constant companion, a guide that enhances ability to discern legitimate communications from potential threats. Use it not just for your personal benefit, but as a resource to educate and empower those around you.

Together, we can transform UCO Bank into an impenetrable stronghold against phishing attacks. Always remember that cyber-security is not an afterthought – it is a cornerstone of our strength, and together, we shape a cyber-secure culture for UCO Bank.

With regards,

**(Mohammad Sabir)**

**Dy. General Manager & CISO**

# Introduction: Phishing & Countermeasures

## *Our Objective*

*We are committed to proactively safeguarding UCO Bank's digital assets and customer data through security strategies, continuous education, and collaboration.*

*With utmost integrity and dedication, we strive to anticipate and mitigate cyber threats, instilling confidence in our customers and maintaining their trust as our foremost priority.*

*From*

**CISO OFFICE  
UCO BANK**

**Head Office, 1st Floor,  
10 BTM Sarani,  
Kolkata - 700001**

**Phone: 033-4455-7903**

**E-mail: [ciso.office@ucobank.co.in](mailto:ciso.office@ucobank.co.in)**



In an increasingly interconnected world, where technology permeates every aspect of our lives, the threat of cyber-attacks looms larger than ever before. Among the myriad of cyber threats, one stands out for its deceptively simple yet highly effective approach: phishing attacks. Like a stealthy predator lurking in the digital shadows, phishing preys upon the unsuspecting, exploiting human vulnerabilities to breach the fortifications of personal and organizational security.

Welcome to our compendium, "Phishing & Countermeasures". Within these pages, we embark on a journey to unravel the intricate web of phishing attacks and empower our staff members with the knowledge and tools needed to shield ourselves and our organizations from these nefarious acts. Our journey begins with a fundamental understanding of phishing attacks. We delve into the anatomy of these malicious endeavors, exploring how cybercriminals cunningly manipulate human psychology to deceive their targets. From deceptive emails to fraudulent websites, we illuminate the diverse array of phishing techniques that lay the groundwork for a successful attack.

Armed with this compendium, we stride forward, prepared to thwart the deceptive tactics of the phishing predators and emerge victorious in the ongoing battle to safeguard our digital world. Together, let us raise the shield of awareness and wield the sword of knowledge to defend against the dark art of phishing.

# What is Phishing ?

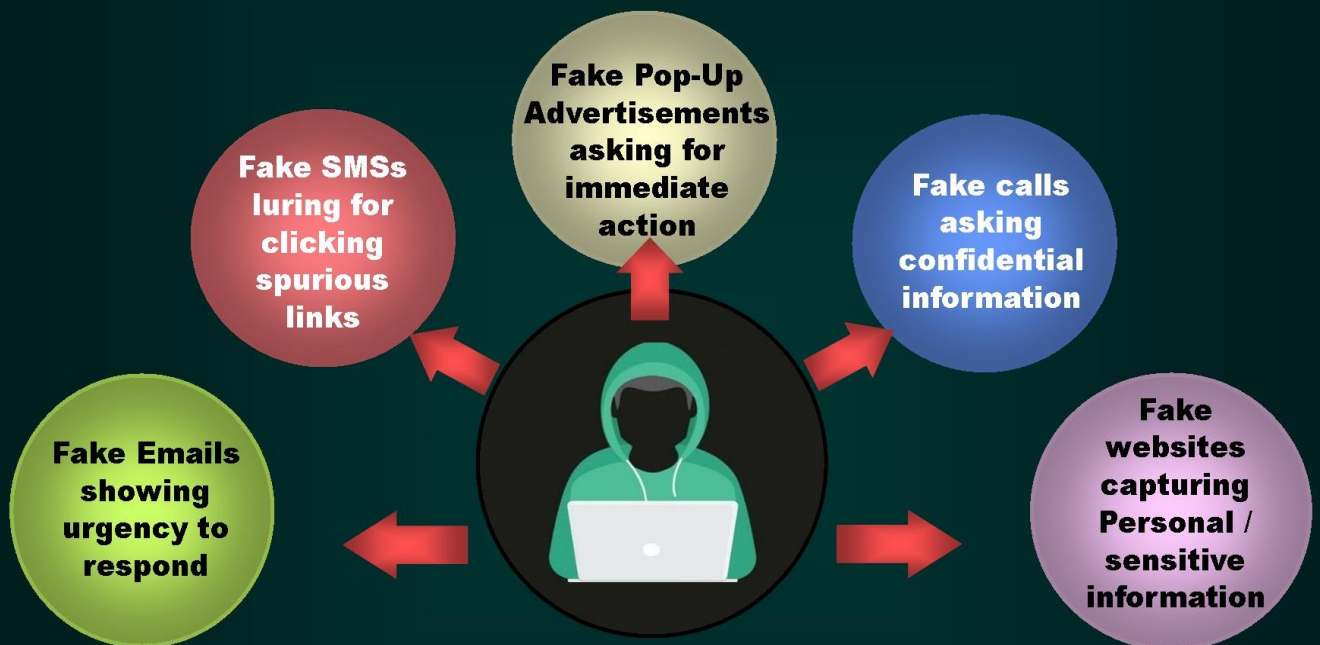


**P**hishing is a type of cyber attack in which malicious actors attempt to deceive individuals or organizations into revealing sensitive information, such as login credentials, financial data, or personal details. The attackers usually masquerade as trusted entities, such as banks, social media platforms, or reputable companies, to manipulate their victims into taking specific actions. These actions

often include clicking on malicious links, downloading infected files, or providing sensitive information.

Phishing attacks typically involve the use of deceptive communication methods, such as fraudulent emails, fake websites, or social engineering tactics, to trick recipients into believing the messages are legitimate. Attackers rely on human psychology and emotions, exploiting factors like fear, urgency, curiosity, and trust to increase the

## BEWARE OF TRICKS USED BY FRAUDSTERS !!



**DO NOT FALL PREY**

**ALWAYS STOP.. THINK.. VERIFY.. AND THEN ACT..**



# Why do we become Victims ?

Despite advances in cybersecurity, falling victim to phishing attacks remains a prevalent and disconcerting reality. The persuasive tactics of cybercriminals, coupled with our innate vulnerabilities to social engineering, make us susceptible to phishing attempts.



# The Cost of not being Cyber Aware

Phishing, a treacherous cyber threat, inflicts significant negative impacts on both individuals and organizations. For individuals, it spells financial loss, privacy breaches, and emotional distress. Conversely, organizations face tarnished reputations, financial setbacks, and operational disruptions when succumbing to the deceitful ploys of phishing attackers. Vigilance and proactive cyber-security measures are imperative to mitigate these grave consequences.



# Importance of Phishing Awareness and Mitigation

The significance of understanding and effectively countering phishing attacks cannot be overstated. Here's why phishing awareness and mitigation are crucial:

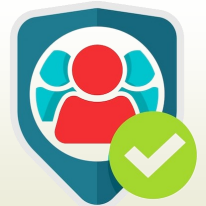
⇒ **Protecting Sensitive Information:** Phishing attacks aim to steal sensitive data, such as usernames, passwords, financial information, and personal details. By raising awareness about phishing techniques and tactics, individuals and organizations can be better equipped to safeguard their valuable information.



⇒ **Preventing Financial Loss:** Phishing attacks can lead to substantial financial losses, both for individuals and businesses. Cybercriminals may use stolen information to conduct fraudulent transactions, compromise financial accounts, or engage in identity theft. By implementing effective mitigation strategies, potential financial damage can be mitigated or avoided altogether.



⇒ **Safeguarding Personal Privacy:** Phishing attacks can result in the exposure of private information, leading to a breach of personal privacy and potential consequences like blackmail, harassment, or reputational damage. Awareness and mitigation measures help individuals protect their privacy and maintain control over their data.



⇒ **Protecting Organizational Data and Reputation:** For organization, falling victim to a phishing attack can have severe repercussions. Data breaches can damage a company's reputation, erode customer trust, and result in legal and regulatory consequences. Phishing awareness and mitigation efforts are essential to safeguarding sensitive business data and maintaining a positive brand image.



⇒ **Reducing Downtime and Productivity Loss:** Phishing attacks can disrupt normal operations, causing downtime and productivity loss. Educating employees about phishing risks and best practices can minimize the likelihood of successful attacks, leading to a more secure and efficient work environment.



⇒ **Enhancing Cyber-security Culture:** Promoting phishing awareness and mitigation contributes to building a strong cyber-security culture within an organization. When all employees are vigilant and informed, they become an active line of defense against cyber threats.



# Understanding Phishing Techniques

In the treacherous landscape of cybersecurity, where cyber threats loom like lurking shadows, phishing stands as one of the most insidious and effective forms of attack. To confront this peril head-on, one must first comprehend the diverse array of phishing techniques deployed by cunning cybercriminals.

## COMMON PHISHING LURES

### *Email Phishing:*

These are Fake emails that appear trustworthy. Contain links that might lead victims to illegitimate websites that can trick them into handing over personal data.



#### TIPS

Never click on any unknown link and avoid sharing your sensitive data on random websites

#### TIPS

Never answer a call from an unknown number and never give your Personal details to anyone over the phone



### *Phone Call (Vishing):*

Cybercriminal scams victims through phone calls and tricks them into revealing their Personal details such as Card number, CVV, Expiry date, PIN, OTP etc.

#### TIPS

Do not reply to such SMSs and avoid clicking on any link. Always delete the message and block the sender

### *Text Messages (SMiShing):*

Fraudsters use text messages (SMS) to lure victims into downloading mobile malware, visiting malicious websites, or calling a fraudulent phone number.



#### TIPS




Resist the temptation to insert an unknown USB device into your system



### *USB Baiting:*

Cybercriminals leave USB devices for people to find and plug into their computers either out of curiosity or in the hope of finding a rightful owner.

# Understanding Phishing Techniques.....contd.

	<p><b>Spear Phishing</b></p> <p>Spear phishing often targets high-profile individuals, executives, or employees within an organization. Attacker may use details such as the target's name, job title, or affiliations to make the email seem legitimate to create convincing messages to lure individuals.</p>
	<p><b>Whaling</b></p> <p>Whaling attacks specifically target high-ranking individuals / high-level executives within an organization. Attackers attempt to gain access to sensitive data or financial information by impersonating these individuals.</p>
	<p><b>Pharming</b></p> <p>Redirect victims to fraudulent websites without their knowledge or consent to divulge sensitive / confidential information like username, password, Financial credentials, Card Details etc.</p>

## Some Phishing Baits

 <p><b>SEEMS URGENT</b> By suggesting to do something immediately</p>	 <p><b>PROVOKES FEAR</b> By threatening to face negative consequences</p>	 <p><b>REQUESTS TO RESPOND</b> By asking personal information</p>	 <p><b>TOO GOOD TO BE TRUE</b> By offering unusual lotteries or prizes</p>	 <p><b>EXERCISING AUTHORITY</b> By impersonating as Top Management</p>
--	--	--	---	---

***Do not Click, Respond or Download !!!***

**Stop...**  **Think...**  **Connect** 

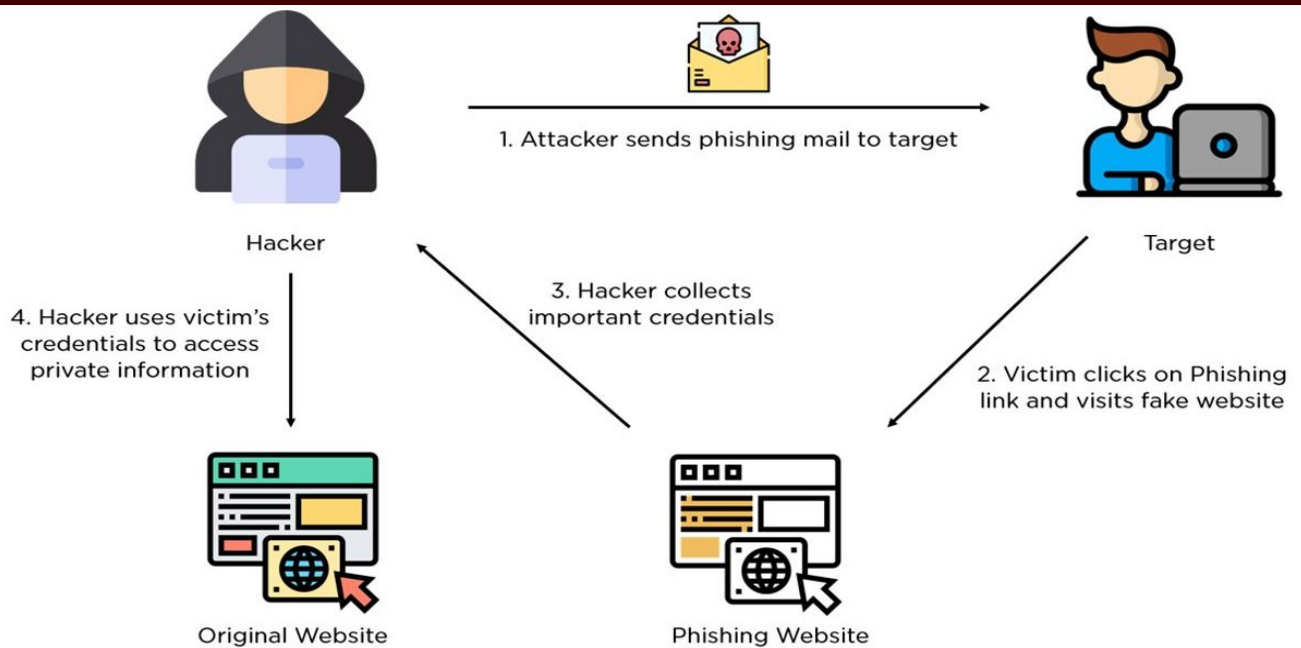
## **Phishing Red Flags**

<p><b>TEXT MESSAGE</b></p> <p>Ask to call a number to claim prize money</p> <p>Ask for KYC Updation</p> <p>Ask for Aadhaar Number</p>	<p><b>EMAIL</b></p> <p>Ask to download attachment / click link</p> <p>Ask to fill out forms</p> <p>Misspelled words</p>	<p><b>PHONE CALL</b></p> <p>Ask for immediate response</p> <p>Ask for OTP / Passwords</p> <p>Ask for address / birthdate</p>
---	---	--

# Email Phishing

Email phishing, often simply referred to as phishing, is a type of cyber attack in which malicious actors use deceptive emails to trick individuals into taking certain actions, such as clicking on malicious links, downloading infected attachments, or divulging sensitive information like login credentials or financial data. Phishing emails are carefully crafted to appear legitimate, often mimicking well-known companies, trusted institutions, or individuals known to the recipient.

## How does it work ?



**New Email  
Received ?**



**LOOK**

**ACT!**

## Watch out for Warning Signs

is sent from suspicious email address



*yourBank@ymail.com*

includes suspicious links / attachments

CLICK HERE



asks for personal / sensitive information



has improper spelling / grammar

*you have not confirmed*



lures users with the promise of free gifts / offers / rewards



**FREE Gift Card of Rs.5000**

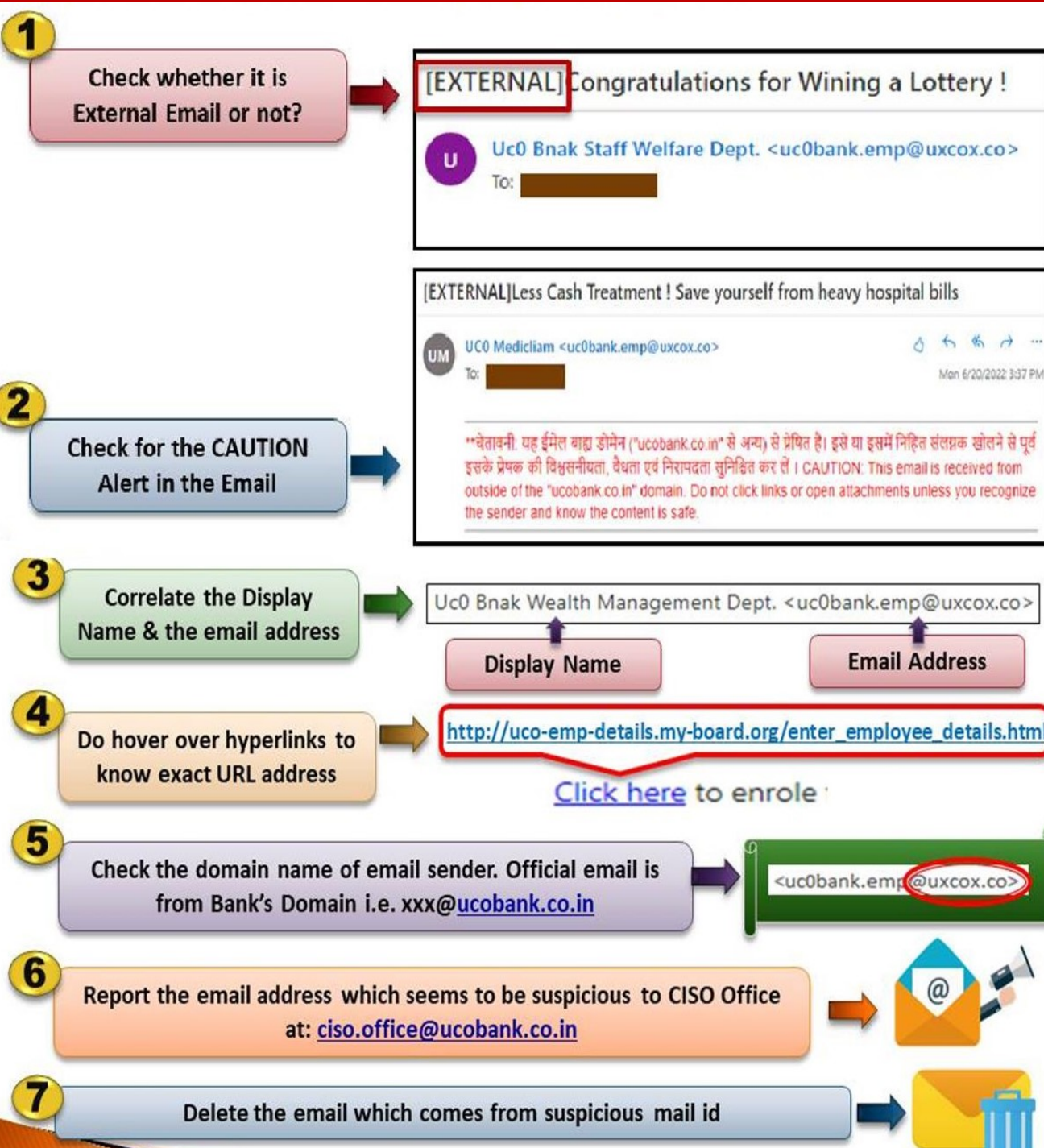
asks for immediate action by creating a sense of urgency/fear



**URGENT**



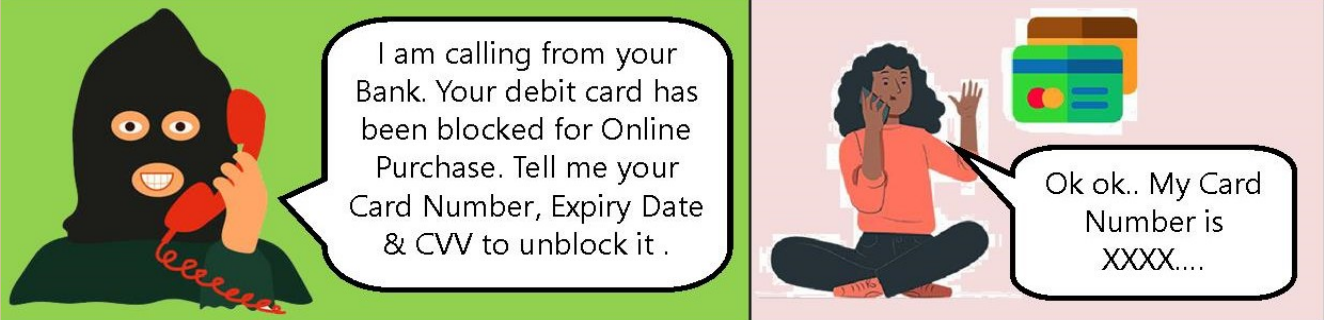
## Follow Below Steps



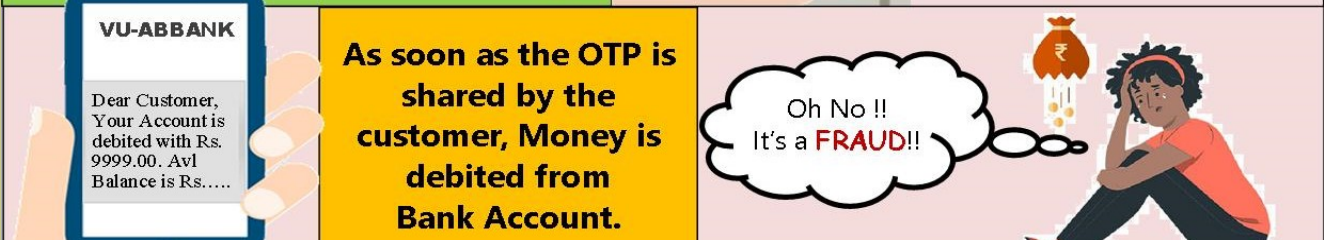
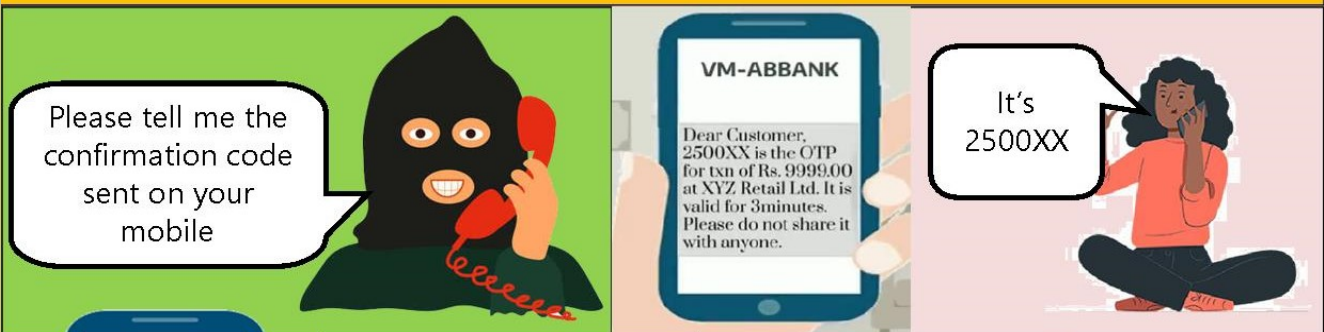
# Phishing through Phone calls (Vishing)

Vishing or "voice phishing," involves the use of phone calls by cybercriminals who pose as legitimate individuals or organizations to trick individuals into revealing sensitive information.

## How Vishing Attack Works ?



**Fraudster initiates Online Transaction using the card details shared by the user.**



## Preventive Measures

Do not share personal or financial information with any unknown caller under any circumstances.

If you receive a suspicious call, verify the caller's identity by independently contacting the organization.

Be skeptical of urgent or threatening requests. Do not succumb to the pressure tactics created by fraudster to manipulate victims.

If suspicious call is received in the name of any organization, immediately report it to the organization for investigation and further action.

# Phishing through SMS (Smishing)

## What is Smishing ?

It is a type of phishing attack in which scammer tries to get your personal information using text message



You receive an attractive SMS with link claiming heavy discount offer, free gift etc.

When you click the link, it would redirect you to suspicious website

It may lead to malware getting downloaded into your system and eventually, compromise your data

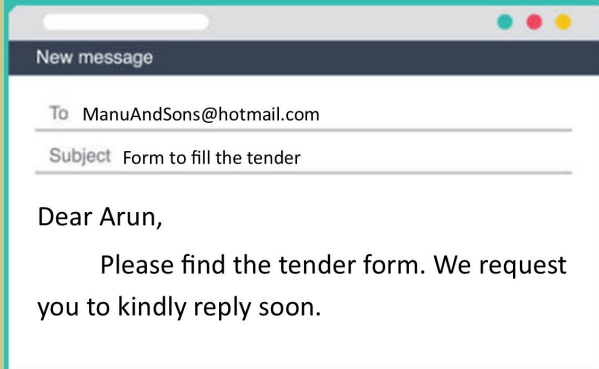
- => Avoid clicking unknown links received through unsolicited messages & senders.
- => Always verify the authenticity of the message & sender.



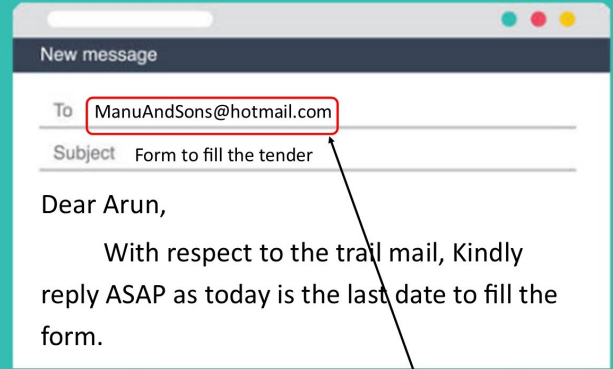
# Spear Phishing

Spear phishing is a targeted form of phishing, where attackers focus their efforts on specific individuals or groups. They tailor messages to suit the recipient's interests, job roles, or relationships, making the emails appear more convincing and personalized.

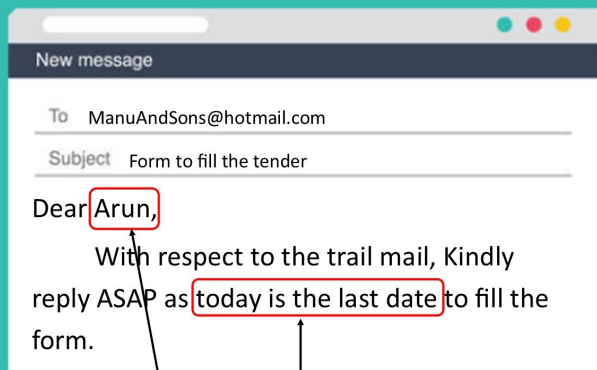
## Modus Operandi



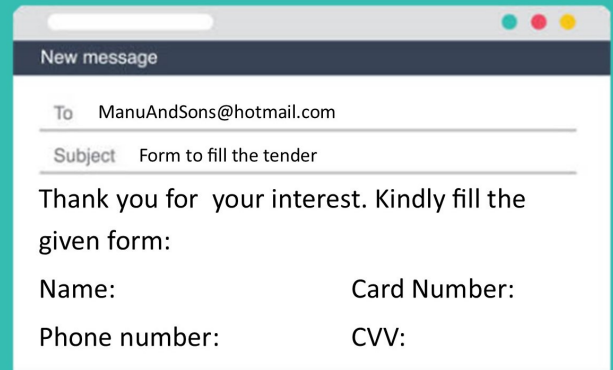
Employee of a reputable organization receives mail from a fraudster



The email seems to be from a legitimate organization or enterprise



The mail addresses a person or shows a sign of urgency



It prompts user to give away sensitive information to steal data or to attack organization's network

## How to Avoid such Scam ?

Verify with the source whether it has definitely come from the said person

Check the tone, spellings, urgency or unusual request for some information

Observe if the request made by sender is familiar one or is it fishy

Cross verify with other colleagues if they have received similar mails

# Anatomy of a Phishing Attack

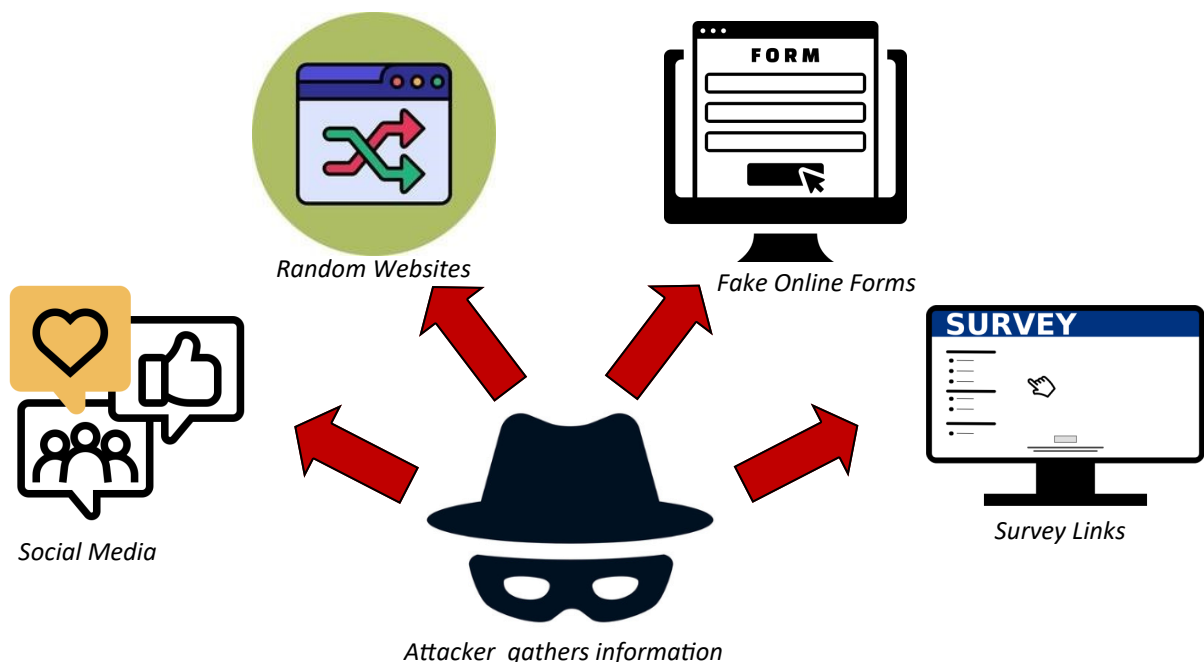
In the ever-evolving landscape of cyber threats, phishing attacks stand out as a persistent and global menace. Understanding the anatomy of a phishing attack is crucial for individuals and organizations to fortify their defenses and protect against these deceptive schemes. In this section, we delve into the inner workings of a phishing attack, examining its lifecycle, the various attack vectors employed, and the artful use of social engineering tactics. By dissecting the anatomy of a phishing attack, employees shall equip with the knowledge and awareness needed to recognize, thwart, and defend against this cunning cyber threat effectively. Let us embark on this journey to unmask the deceptive techniques of phishing and fortify our resilience against its dark art.



## Phishing Attack Lifecycle

The success of a phishing attack lies in its methodical execution, following a well-defined lifecycle that allows cybercriminals to ensnare their victims effectively. Understanding the stages of the phishing attack lifecycle is essential for individuals and organizations to identify warning signs, disrupt the attack chain, and safeguard against falling victim to this pervasive threat.

**1. Reconnaissance:** In this initial phase, attackers conduct thorough research to identify potential targets and tailor their phishing campaign accordingly. They may gather information from publicly available sources, social media, random websites, fake online forms, survey links etc.



# Phishing Attack Life Cycle.....contd.

**2. Lure Creation:** Armed with the gathered intelligence, attackers craft compelling lures, such as fraudulent emails or messages, designed to attract the attention and trust of the intended victims. Lures often play on emotions like fear, curiosity, or urgency to provoke immediate action.

**3. Delivery:** The attackers disseminate the crafted lures to their targets using various delivery methods, such as mass email



campaigns, social media posts, or even instant messaging platforms. By employing multiple channels, they cast a wide net, aiming to reach as many potential victims as possible.

**Common Signs of PHISHING**

- Seems **URGENT** !!
- Provokes **FEAR** !!
- Spelling **MISTAKES** !!
- Too **GOOD** to be **TRUE** !!

**4. Deception and Social Engineering:** At the core of the phishing attack lifecycle lies the artful manipulation of human psychology through social engineering tactics. Attackers skilfully deceive recipients into believing the lures are legitimate, exploiting trust and authority to persuade them to take the desired actions.

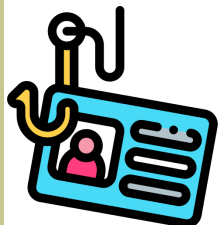


## Link



**5. Action by the Victim:** Upon receiving the phishing lure, victims may unknowingly click on malicious links, download infected attachments, or divulge sensitive information, falling prey to the attackers' deceptive scheme.

**6. Data Harvesting:** As victims unwittingly respond to the phishing attack, attackers harvest the obtained data, which may include login credentials, financial information, or other sensitive data, depending on their objectives.



**7. Exploitation:** Armed with the harvested data, cybercriminals may proceed to exploit the compromised accounts or launch secondary attacks, such as identity theft, financial fraud, or further phishing campaigns.



**8. Post-Exploitation Activities:** After achieving their goals, attackers may cover their tracks to avoid detection and maintain prolonged access to compromised systems or accounts.



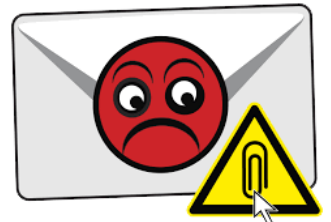
# Phishing Attack Vector & Common Entry Points



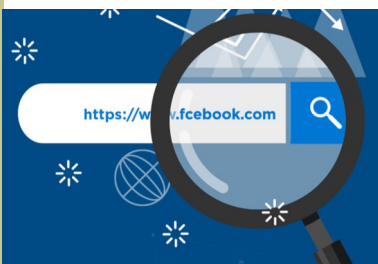
Phishing attacks are characterized by their versatility, with cybercriminals employing a diverse range of attack vectors and entry points to ensnare their victims. Understanding these attack vectors and common entry points is essential for individuals and organizations to identify potential vulnerabilities and implement robust defenses against phishing attempts. In this section, we explore the various avenues through which attackers execute their malicious schemes, shedding light on the deceptive tactics used to

breach security barriers and deceive unsuspecting victims.

⇒ **Deceptive Emails:** Phishing attacks often start with deceptive emails, where attackers impersonate trusted entities, such as banks, government agencies, or well-known companies. These emails may contain fraudulent requests, urgent alerts, or enticing offers, encouraging recipients to click on malicious links or disclose sensitive information.



⇒ **Malicious Attachments:** Cybercriminals may embed malware-laden attachments within phishing emails. Once opened, these attachments can infect the victim's system with viruses, ransomware, or other malicious software, granting the attackers unauthorized access to the victim's data or network.



⇒ **Spoofed Websites:** Phishing attacks frequently involve the creation of spoofed websites that closely mimic the appearance and functionality of legitimate sites. Unsuspecting users may be lured into entering their login credentials or personal information, unknowingly divulging it to the attackers.

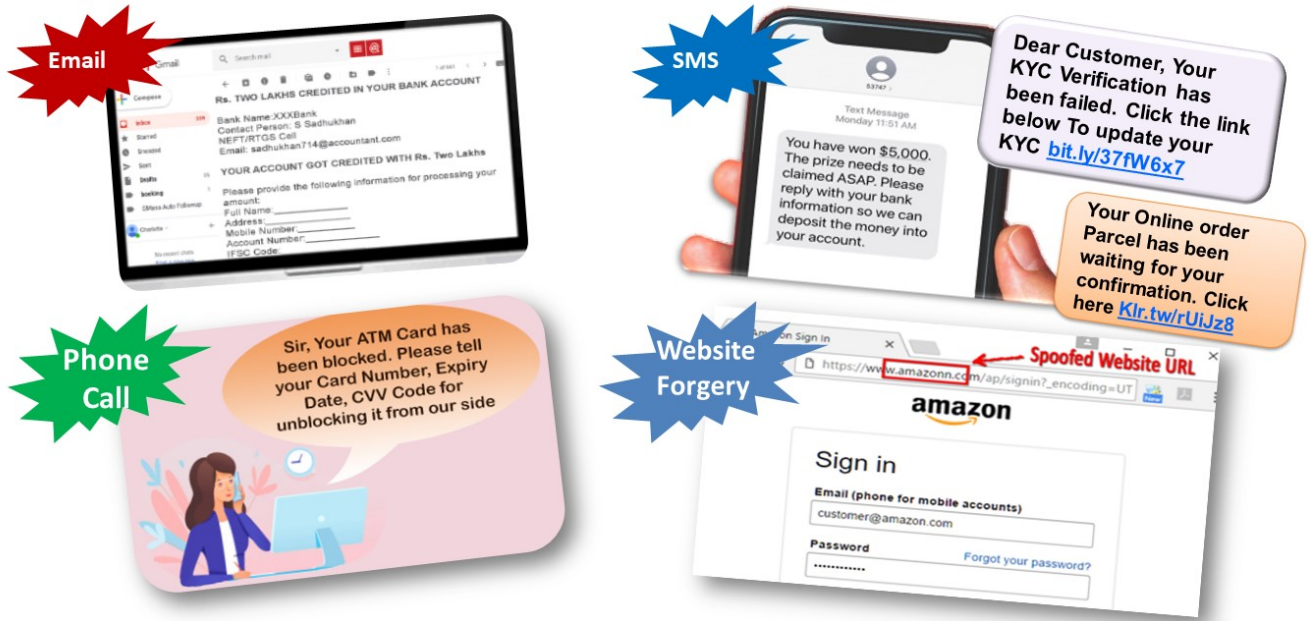
⇒ **Phishing Links in Messages or Posts:** Phishing links may be disseminated through various channels, such as social media, instant messaging, or online forums. Users may click on these links, thinking they lead to genuine content, but are directed to fraudulent sites instead.



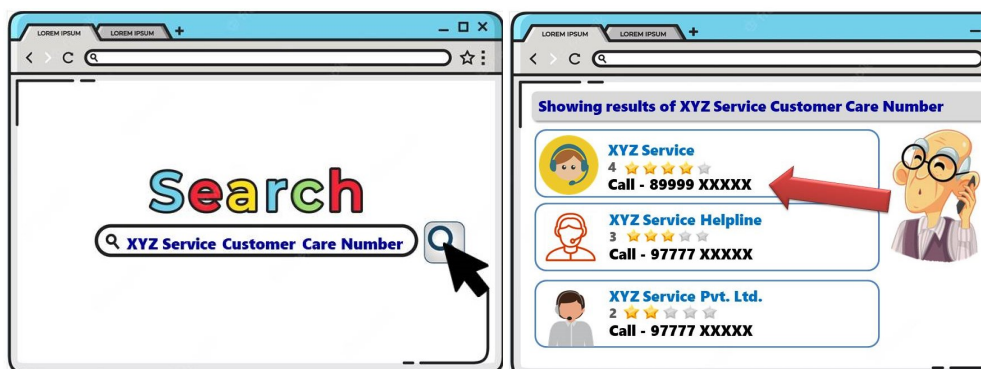
# Phishing Attack Vector & Common Entry Points

⇒ **SMS and Instant Messaging:** Phishing attacks extend to mobile platforms through SMS phishing (smishing) and instant messaging apps. Attackers send fraudulent messages, urging recipients to click on links or reply with sensitive information.

## Common Phishing Mediums



⇒ **Voice Phishing (Vishing):** Vishing attacks occur over phone calls, where attackers impersonate trusted entities, such as banks or customer support representatives, to trick victims into divulging sensitive information.



### ⇒ Search Engine Manipulation:

Attackers may manipulate search engine results, ensuring that phishing websites appear among the top results for certain keywords, increasing the likelihood of users stumbling upon malicious sites.



# Social Engineering Tactics Exploited in Phishing

At the heart of every successful phishing attack lies social engineering—a cunning manipulation of human psychology to deceive and manipulate victims. Cybercriminals employ a variety of social engineering tactics to craft persuasive and convincing phishing lures, exploiting trust, emotions, and vulnerabilities to trick recipients into taking the desired actions. In this section, we explore the diverse social engineering tactics commonly employed in phishing attacks, illuminating the artful techniques used by attackers to compromise individuals and organizations.

- ◆ **Fear and Urgency:** Attackers often exploit fear and urgency to prompt immediate action from their victims. Phishing emails may threaten account closures, impending fines, or security breaches, compelling recipients to respond without critically evaluating the legitimacy of the message.
- ◆ **Curiosity and Clickbait:** Phishing lures that evoke curiosity or offer enticing clickbait content entice recipients to click on links or download attachments. By triggering curiosity, attackers capitalize on recipients' natural inclination to explore novel or intriguing topics.
- ◆ **Authority and Impersonation:** Attackers impersonate authoritative figures, such as CEOs, government officials, or trusted colleagues, to elicit compliance from recipients. Emails appearing to come from higher-ups or reputable sources can bypass normal skepticism and encourage victims to comply with the attacker's requests.
- ◆ **Empathy and Personal Appeals:** Phishing attackers may exploit empathy by crafting messages that evoke sympathy or support for a cause, encouraging recipients to act altruistically or provide sensitive information to help someone in need.

## Social Engineering – Red Flags



Your 'friend' sends you a strange message.



Your emotions are heightened.



The request is urgent.



The offer feels too good to be true.



You're receiving help you didn't ask for.



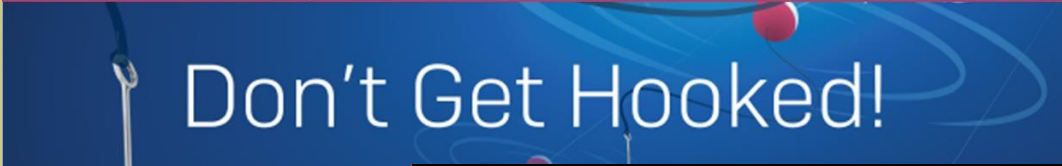
The sender can't prove their identity.

# Social Engineering Tactics Exploited in Phishing

- ◆ **Reward and Incentive:** Phishing emails promising rewards, prizes, or exclusive offers can tempt recipients into clicking on malicious links or submitting personal data to claim the purported benefits.
- ◆ **Scarcity and Limited Time Offers:** By creating a sense of scarcity or limited-time offers, attackers create a sense of urgency, encouraging recipients to take immediate action before the opportunity vanishes.
- ◆ **Trust and Familiarity:** Phishing lures often mimic well-known companies, banks, or social media platforms, leveraging recipients' trust in familiar brands. Attackers exploit this trust to encourage recipients to interact with the fraudulent content.
- ◆ **False Sense of Security:** Phishing attackers may craft messages that falsely reassure recipients of their authenticity, claiming security measures or verification processes to gain the recipient's trust.
- ◆ **Phishing as a Helpdesk or IT Support:** Cybercriminals may pose as IT support or customer service representatives, offering to assist recipients with technical issues. By exploiting the trust placed in support personnel, attackers can extract sensitive information under the guise of assistance.



## Stay One Step Ahead: **Be Phish-Savvy**



<b>P</b>	<b>Promises</b> Offering unbelievable things?
<b>H</b>	<b>Harassment</b> Pressurising you to act?
<b>I</b>	<b>Instinct</b> Does it feel wrong?
<b>S</b>	<b>Sense of Urgency</b> Making you rush?
<b>H</b>	<b>Hit DELETE</b> After reporting the email !

# Recognizing Phishing Attempts

Recognizing phishing attempts is crucial to protect ourselves and our organization from falling victim to these deceptive attacks. Always err on the side of caution. If you are unsure about an email's legitimacy, verify its authenticity through official channels or by contacting the sender directly using contact information from a trusted source.

## Identifying Suspicious Emails

- ⇒ **Unknown Sender:** Be cautious of emails from unknown senders or email addresses that look unfamiliar or misspelled.
- ⇒ **Unusual Subject or Greeting:** Be wary of emails with vague subjects or generic greetings like "Dear User/Customer" instead of addressing you by your name.
- ⇒ **Urgent or Threatening Language:** Suspicious emails may use urgent or threatening language, pressuring you to take immediate action.
- ⇒ **Spelling and Grammar Errors:** Phishing emails often contain spelling and grammar mistakes, which are uncommon in communications from reputable organizations.

### Be suspicious of...



Hyperlink to fake website



Unofficial "From" address



"Urgent" request or threat



Email containing attachment



Ask for sensitive information

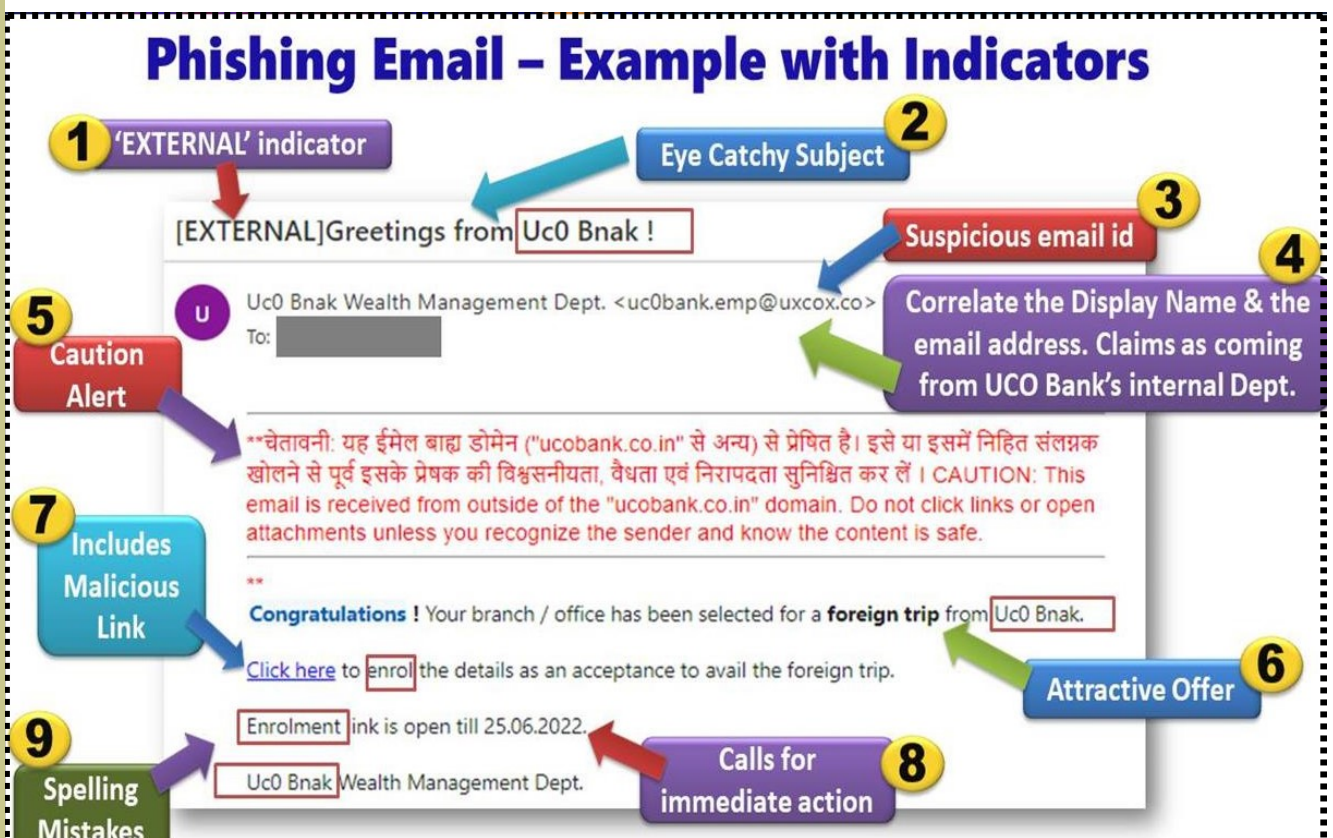


Generic subject line & intro message



- ⇒ **Mismatched URLs:** Hover your mouse over links in the email to check the actual URL. If it doesn't match the displayed text or seems unrelated to the sender or the email's content, it might be a phishing attempt.
- ⇒ **Requests for Personal Information:** Be cautious of emails asking for sensitive information like passwords, Personally Identifiable Information or financial credentials etc.
- ⇒ **Unexpected Attachments:** Do not open attachments from unknown senders or unexpected sources, as they could contain malware or viruses.
- ⇒ **Too Good to Be True Offers and Prizes:** Be cautious of emails promising extraordinary opportunities, significant financial gains, offering prizes, gifts or rewards that sound too good to be true.
- ⇒ **Impersonation of Trusted Entities:** Phishing emails may impersonate well-known companies, government agencies, or financial institutions to gain trust.
- ⇒ **Uncommon Requests from Contacts:** If you receive an email from someone you know but the content seems unusual or out of character for them, verify the message's legitimacy through another communication method.
- ⇒ **Pressure Tactics to Click on Links:** Suspicious emails often pressure you to click on links or download files by claiming it's urgent or essential.
- ⇒ **Emails from Misspelled Domains:** Phishing emails may use domain names with slight misspellings or extra characters to mimic legitimate websites.

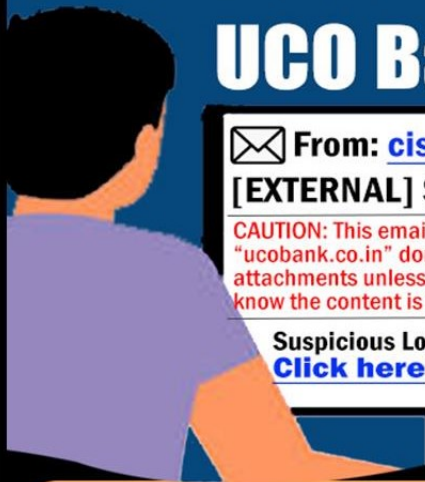
## Phishing Email – Example with Indicators



The diagram illustrates a phishing email with the following indicators:

- 'EXTERNAL' indicator:** Points to the subject line "[EXTERNAL]Greetings from Uc0 Bnak !".
- Eye Catchy Subject:** Points to the subject line "[EXTERNAL]Greetings from Uc0 Bnak !".
- Suspicious email id:** Points to the sender's email address "<uc0bank.emp@uxcox.co>".
- Correlate the Display Name & the email address. Claims as coming from UCO Bank's internal Dept.:** Points to the sender's name "Uc0 Bnak Wealth Management Dept." and the email address "<uc0bank.emp@uxcox.co>".
- Caution Alert:** Points to the red text "CAUTION: This email is received from outside of the 'ucobank.co.in' domain. Do not click links or open attachments unless you recognize the sender and know the content is safe."
- Includes Malicious Link:** Points to the link "Click here to enrol" in the body text.
- Attractive Offer:** Points to the text "Congratulations ! Your branch / office has been selected for a foreign trip from Uc0 Bnak."
- Calls for immediate action:** Points to the text "Enrolment link is open till 25.06.2022."
- Spelling Mistakes:** Points to the misspelled name "Uc0 Bnak" in the footer.

## Email appearing from UCO Bank ?



✉ From: [ciso1offc@uco0bnak.in](mailto:ciso1offc@uco0bnak.in)  
[EXTERNAL] Security Alert !  
CAUTION: This email is received from outside of the "ucobank.co.in" domain. Do not click links or open attachments unless you recognize the sender and know the content is safe.  
Suspicious Login detected in this Email.  
[Click here](#) to confirm your password.

**DON'T FALL  
FOR THE  
PHISHING  
BAIT !**

### WHAT SCAMMERS NEED FROM YOU ?



Passwords



Financial  
Information



Identity



Money

### BEWARE OF



Suspicious Email  
Senders



Unknown  
Links



Attachments



**Before responding, examine  
Email address closely even  
if the mail appears to be  
from UCO Bank !**

**ANYTHING SUSPICIOUS ? PAUSE & THINK..**  
**Report Suspicious Emails to [ciso.office@ucobank.co.in](mailto:ciso.office@ucobank.co.in)**

Report Cyber fraud Incident to <https://www.cybercrime.gov.in>  
or call **1930** for assistance

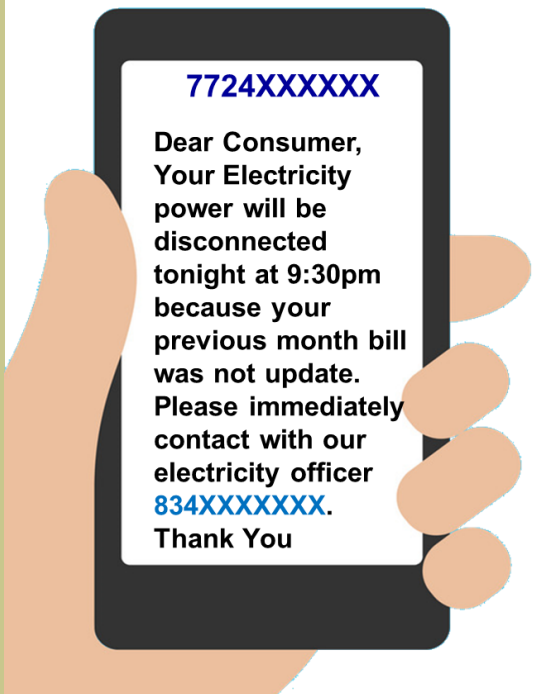
# Spot Fake SMS



Fake SMS messages, also known as Smishing (Phishing through SMS), attempt to deceive users into providing sensitive information or clicking on malicious links via text messages. Here are some indicators that can help you identify fake SMS messages:

⇒ **Unknown Sender:** Be cautious of the messages received from unknown or unexpected senders with 10 digit mobile number or suspicious sender ID.

⇒ **Suspicious Links:** Avoid clicking on links. It may redirect you to fake website for capturing your personal / sensitive information or may lead to download malware into your device.

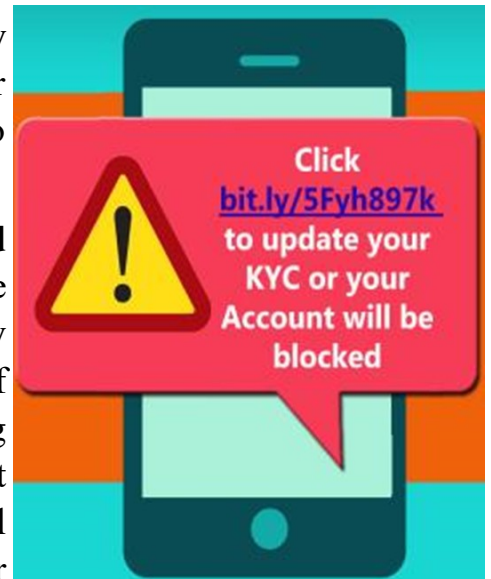


⇒ **Urgency and Fear Tactics:** Fake SMS messages may create a sense of urgency, warning you of account suspensions, bill payments, or other consequences if you don't respond immediately.

⇒ **Shortened URLs:** If the SMS contains shortened URLs / links, avoid clicking on them directly. Instead, use a trusted App/website to check the link's destination.

⇒ **Generic**

**Greetings:** Fake SMS messages may use generic greetings like "Dear Customer" or "Valued User" instead of addressing you by your name.



**50000 Reward Point credited on your ABC Account. Click here to redeem:**

[bit.ly/86dY9w3](http://bit.ly/86dY9w3)

# Spot Fake SMS.....contd.



**Beware of FAKE Messages on Income Tax Refund**

Dear , your income tax refund of Rs.16,988 has been approved and your bank a/c will be credited shortly. Do kindly verify your a/c no 5XXXXX6755. If the same is incorrect, quickly follow the link below to update your bank record on file. <https://bit.ly/2Kvr2ls>

- ✗ Do not respond such messages & Avoid clicking on any unknown link
- ✗ Never share personal / sensitive / financial information with anyone or random websites / apps
- ✔ Visit your nearest Bank Branch or refer Bank's official Apps / online eBanking portal for account related queries / information

From: IncomeTaxDept <admin@tradesigner.com>  
Sent: Tue, 06 Jun 2023 10:14:36  
To: [Redacted]  
Subject: <Name> confirm your refund details and mobile verification FRM81HJ812023

**FAKE**

e-Filing Anywhere Anytime  
Income Tax Department, Government of India

Dear <Name>

We are pleased to announce that the Tax Office has completed its tax audit. You are eligible for a overdue refund of Rs 41,542.81 but your account information in your database is incorrect. Please follow the steps outlined below to complete and submit your request. Make sure to enter the correct credentials.

Submit a refund request by clicking on the link below.

**Proceed**

**Be vigilant and skeptical about unsolicited emails claiming to be from the Income Tax Department**

**Do not click on any links provided in unsolicited emails. Always check the sender's email address carefully.**

⇒ **Spelling and Grammar Errors:** Messages with spelling mistakes or poor grammar are potential indicators of Smishing attempts.

⇒ **Unusual Requests:** Be wary of SMS messages requesting personal information, passwords, PINs, or financial details. Legitimate organizations typically do not request such information via text message.

BV-XXXUSER

Hello Applicant, your MSME Business Loan of **Rs.4085999** under Mudra Yojana has been sanctioned. Verify details on

Link: <http://tiny.cc/XXXdata>

⇒ **Unsolicited Offers and Prizes:** Be skeptical about unsolicited SMS messages offering quick & easy loans, quick high return on investment, unexpected lotteries, prizes, rewards or gifts which are too good to be true.

⇒ **Misspelled Brands:** Phishing SMS messages may use brand names with misspellings or extra characters to mimic legitimate organizations or companies.

## HOW TO SPOT A FAKE MESSAGE ??



**Suspicious sender with ten (10) digit mobile no.** → 789XXXXXXX

**Spelling or grammatical errors** → trackking code

**Sense of urgency** → Confirm the shipping address now, click

**Unexpected message** → GK3NPL3R is waiting for you.

**Malicious link** → [bit.ly/kl8uIP](http://bit.ly/kl8uIP)

# Indicators of Fake Website

Spotting fake websites is crucial to protect ourselves from falling victim to phishing attacks and other online scams. Here are some indicators to identify fake websites:

## INDICATORS OF MALICIOUS WEBSITE (PHARMING)



- Whether “s” is missing after “http”
- Check the verified indicators such as ‘lock sign’
- Check the spelling of Organization
- Check substituted letters , numbers , odd character or symbol appearing before the Organization name

- Fake Logo
- lack of “Contact us” section
- spelling & grammatical errors
- Low resolution images
- Incomplete design & information



## POP-UP MENACE



**A Phishing scam** may direct you to a legitimate website. But pop-up windows are used to reel in vulnerable targets

- **Pop-up Windows** may ask to enter your credentials
- **Do not click or respond to unwanted Ads / Pop-ups**

## BROWSER SECURITY INDICATOR

- **Make sure your own connection is secure / encrypted**
- **Do not forcefully enter into an website for which browser shows “connection is not secure” error**



# Indicators of Fake Website .....contd.

## Sample Phishing Website Indicators

**1** Not secure indicator - 'http'

**2** Suspicious URL

**3** Different Color of our Bank's Logo and wrong Hindi Tagline

**4** Multiple Spelling Mistakes

**5** Asking for Sensitive Info

UCO BANK (A Govt. of India Undertaking)  
Honours Your Trust

Enter Details Here

Name: Enter Employee Name  
PF No.: Enter PF Number  
Branch Id: Enter Branch Id

Enrol

Uco Bank | 2014 | Hunan Resource Management | Tested with Internet Explorer 9+, Firefox, Chrome.



Scammer copies (spoofs) the website of a well-known business.



The unknowing victim mistakes the spoofed website for the real thing.



Scammer steals information from the victim without their knowledge.

## SPOT THE DIFFERENCES

**1** UCO Bank's Logo is modified

**2** Different Background color

**3** Hindi Tagline is missing

**4** Second tagline is altered

# Best Practices for End-Users - Email Security

In today's digital landscape, end-users play a vital role in ensuring their own cyber security and safeguarding sensitive information. Cyber threats, especially phishing attacks, have become more sophisticated, making it crucial for individuals to adopt best practices to protect themselves from online risks. This section provides an overview of essential best practices for end-users, empowering them to navigate the digital realm with confidence and maintain a secure online environment.

## HOW TO AVOID EMAIL PHISHING ?

	<p><b>1</b> Do not open emails from unknown or untrusted senders.</p>		<p><b>4</b> Do not reply to suspicious requests.</p>
	<p><b>2</b> Avoid responding or clicking links on unsolicited or spam email.</p>		<p><b>5</b> Do not rely on any information in the email from untrusted senders.</p>
	<p><b>3</b> Do not open or download email attachment from unknown or untrusted senders.</p>		<p><b>6</b> Do not share sensitive information through email.</p>





### Best Practices

- ✓ Always ignore suspicious calls, messages, emails or links
- ✗ Avoid clicking on unknown links & do not open or download unknown attachments / files from untrusted sender
- ✓ Examine Email / SMS sender address closely. UCO Bank's Official Email domain is "[@ucobank.co.in](mailto:@ucobank.co.in)" & legitimate SMS sender address will contain "**UCOBANK**" / "**UCOPPC**" / "**UCORWD**"
- ✗ Never reveal any personal / sensitive information on random websites, forms, documents or at the behest of any stranger
- ✗ Do not fall prey to attractive offers, deep discounts etc. which are too good to be true

# Best Practices for End-Users - Password Security

Password security plays a crucial role in preventing phishing attacks and protecting against unauthorized access to personal accounts and sensitive information. By adhering to strong password security practices, individuals can significantly reduce the risk of falling victim to phishing attacks.

## Password Safety Practices

-  Create complex passwords with combination of letters, numbers and special characters to prevent their guessing or cracking by fraudsters / adversaries
-  Avoid using dictionary words, family name, vehicle number, personal or office information etc. in your password
-  Change default password immediately & avoid setting passwords like Uco@..., Ucobank@... or any other passwords which can be easily guessed
-  Never select 'YES' when any Application, Website, Browser etc. asks to remember your password



Password are like socks, change them regularly



Never write passwords on paper or on devices



Memorize your password



Beware of Shoulder Surfers at public places while entering passwords



Making password complex increases difficulty of attacks & are hard to guess



Use different passwords for different accounts

Passphrase

**My Car is Blue**

Password

**mYc@RI5b!Ue**

If hard to remember password, switch to passphrase



Never share password with anyone



# Best Practices for End-Users - Desktop Security

Desktop security is a crucial aspect of overall cyber security, as it involves protecting computers and their data from various threats and unauthorized access. Desktop security is a continuous process, and maintaining a proactive approach to cyber security helps protect sensitive information, prevent data breaches, and ensure the overall integrity and privacy of the system.

## Cyber Hygiene Practices for Desktop Security

**Avoid leaving system unlocked or unattended. Always lock it by pressing  + L key together**




**Do not write confidential information such as Username or Password anywhere**




**Avoid using common or easy to guess Password**



**Ensure Antivirus is installed & updated in your system**



**USB is blocked**

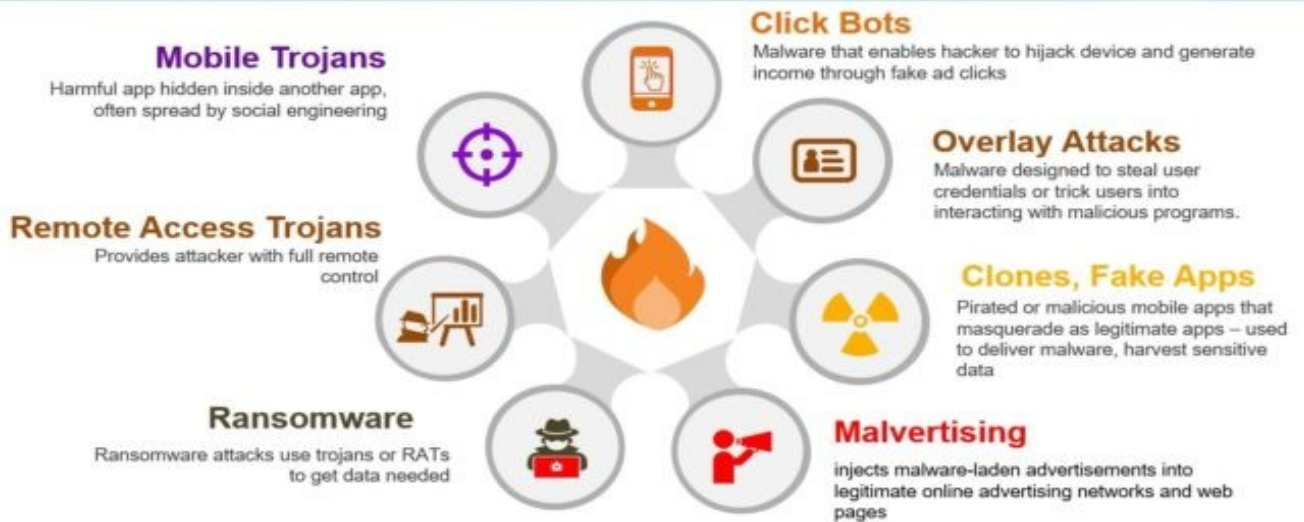


**Access Internet at Branches / Offices through Bank's **PROXY** Server**

# Best Practices for Mobile Malware Protection

Phishing, a prevalent cyber threat, has extended its reach to mobile devices through the use of mobile malware. As smartphones and tablets become integral to our daily lives, cybercriminals exploit this trend by deploying malicious software to target unsuspecting users.

## Malware Examples – What Makes Them So Harmful



## Do's & Don'ts for Mobile Malware Protection

A Mobile security breach can give hackers access to users' personal information, other critical information like banking information, current location, and lots more



# QR Code Scams & Best Practices

QR codes, once a convenient way to quickly access information or websites, have become an avenue for cybercriminals to perpetrate phishing attacks. QR code phishing is a growing concern as attackers leverage these scannable codes to trick unsuspecting users into visiting malicious websites, downloading malware, or revealing sensitive information. With the rising popularity of QR codes in advertising, promotions, and mobile payments, it is vital to recognize the risks posed by QR code phishing and adopt preventive measures to protect against this stealthy form of cyber threat.

## Cyber Threats hiding in QR codes



### QRLjacking

Fraudsters leaving malicious QR codes on public places like walls, buildings and also computer screens that direct users to a malicious site.



### Quishing

Fake QR Code directs unsuspecting victims to a fake version of a popular website and prompts users to enter their login details.



### Free Wi-Fi set up

Cybercriminals often set up free Wi-Fi network for anyone that scans the QR Code. By this network fraudsters can silently steal sensitive information.



### UPI related

Fraudsters sent malicious QR Code through Social Media, Emails, SMSs prompting for "SCAN & WIN Money". Scanning leads to debit money from account.

## How to Avoid such frauds ?



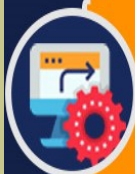
Never scan QR Code for receiving money



Do not scan QR Code received from untrusted sources



Use reputable service or App for generating QR Code



Disable 'Open Website Automatically' option or other equivalent setting in QR Code Scanner App



While making payment through QR Code, always verify UPI/VPA address before payment approval

# Best Practices to secure Biometric Information

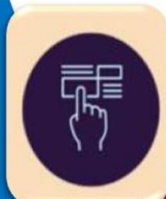
Biometric authentication, such as fingerprint scans, facial recognition, and iris scans, offers a convenient and secure way to access devices and applications. However, cybercriminals have found ways to exploit this advanced security feature through biometric phishing. Biometric phishing, also known as biometric spoofing or presentation attacks, involves tricking biometric systems to gain unauthorized access to protected data or accounts. This emerging threat poses unique challenges, as attackers target the very mechanisms designed to enhance security.

## Best Practices to Secure Biometric Information

Lock your Biometrics and Aadhaar through Official UIDAI website or the mAadhaar App



Generate the 16-digit Virtual ID (VID) number from official UIDAI website & use it in the place of original Aadhaar number



Generate and use 12-digit Masked Aadhaar from UIDAI portal to protect your Aadhaar information



Never reveal your Biometrics, Aadhaar or OTP etc. at unknown or unauthorised places including Social Media



If mobile number, email id etc. which are linked with the Aadhaar are changed/modified, update them at UIDAI portal or by visiting nearest Aadhaar Enrolment Centre



Frequently check UIDAI portal to verify your authentication and implement new security features if introduced

# Best Practices for End-Users - UPI Safety

Unified Payments Interface (UPI) has revolutionized the way people conduct digital transactions, providing a convenient and fast way to transfer money. However, with its popularity, cybercriminals have devised sophisticated phishing schemes targeting UPI users. Phishing using UPI involves deceptive tactics to trick individuals into divulging their UPI credentials, such as UPI PIN or mobile app login details. These malicious campaigns exploit users' trust in the UPI system and aim to gain unauthorized access to their bank accounts or conduct fraudulent transactions. and best practices to safeguard against falling victim to such scams.

## Beware of these UPI scams

- Fake Offers
- Phishing Links
- Request Money
- QR Code Scams
- Remote Screen Monitoring
- Scams using UPI PIN & OTP



## Safety precautions while using UPI



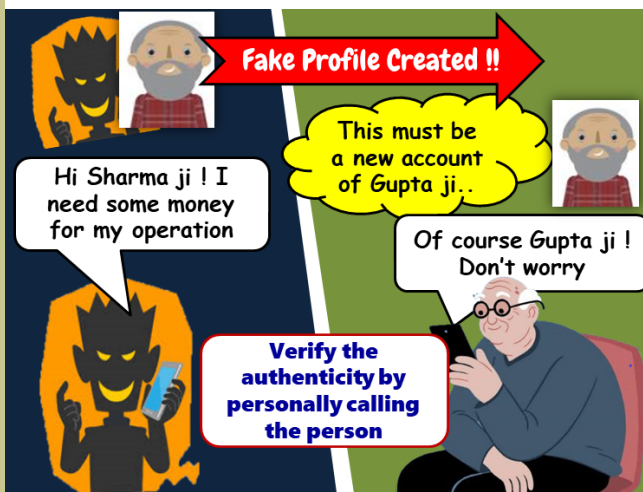
- ✓ **Keep your UPI PIN confidential.**
- ✓ **Do not download unverified third-party apps. Always use App provided by your own Bank.**
- ✓ **Do not respond to unverified messages or calls from individuals claiming to be bank representatives.**
- ✓ **Do not use UPI PIN for receiving money. UPI PIN is only used for payments.**
- ✓ **Do not fall prey to fraudulent lucrative advertisement offers which ask for UPI PIN.**
- ✓ **Do not scan any QR Code received from unidentified source.**

# Avoid Phishing at Social Media Platforms

Social media platforms have become an integral part of modern communication, networking, and sharing. However, their widespread popularity has also attracted cybercriminals who exploit social media for phishing attacks. Social media phishing is a deceptive practice where attackers use various tactics to manipulate users into revealing sensitive information, such as login credentials, personal details, or financial data. By impersonating trusted individuals or organizations, scammers trick users into clicking malicious links, downloading malware, or providing confidential information. This section explores the types of social media phishing, the techniques employed by cybercriminals, and essential best practices to safeguard against falling victim to these crafty online scams.

## Types of Social Media Phishing:

**Phishing Links:** Attackers post malicious links disguised as enticing content on social media platforms, leading users to phishing websites designed to steal login credentials or infect devices with malware.



**Fake Profiles:** Cybercriminals create fake profiles impersonating trusted individuals, brands, or organizations to gain users' trust and extract sensitive information through private messages or posts.

**Contest Scams:** Scammers entice users with fake contests or giveaways, requiring participants to share personal information to claim prizes that do not exist.

**Fake Ads:** Cybercriminals create deceptive advertisements that appear legitimate and enticing, leading unsuspecting users to malicious websites or fake login pages, where sensitive information is harvested.

### Xiaomi Mi 11X Pro



## AVOIDING PHISHING ATTACKS

### ON Social Media

- ^ Never click on random advertisements / Pop-ups / links while scrolling through your social media as it may redirect you to malicious websites.
- ^ Avoid accepting friend request from strangers, and keep your friend list private to refrain fraudsters from reaching out to you / your known ones.
- ^ Avoid joining unknown groups on social media. Fraudsters often create groups / accounts promising "too good to be true" job offers, investment opportunities etc.

**50% Off**

**UNKNOWN**

**1**

# Avoid Phishing at Instant Messaging Platforms


Phishing through instant messaging platforms is a crafty cyber strategy that capitalizes on the widespread use of messaging apps like WhatsApp, Telegram etc. Attackers employ messages containing malicious links or attachments, posing as trusted contacts or reputable sources, aiming to trick recipients into revealing personal /sensitive / financial information or downloading malware and thereby leading to identity theft or financial loss. This evolving threat underscores the importance of verifying sender identities, avoiding suspicious links, and maintaining cyber security vigilance in the realm of instant messaging. Here's how these attacks are conducted:


## Impersonation:

- ⇒ Attackers create fake profiles that closely resemble trusted contacts, organizations, or known entities.
- ⇒ They use profile pictures, names, and information similar to the legitimate ones to deceive recipients.


## Beware of WhatsApp Impersonation Scam

**Mr. Chandu was working at ABC Company in the post of Finance Manager. One day, he received a WhatsApp message from his Boss.**





**Mr. Chandu immediately went to the office of Boss Secretariat and depicted the total scenario to the Secretariat.**



Now a days, fraudsters are impersonating Senior Officials / Top Management of Organizations with their photo and sending out fake messages through WhatsApp, Telegram, SnapChat etc by asking for urgent monetary favours from their colleagues.

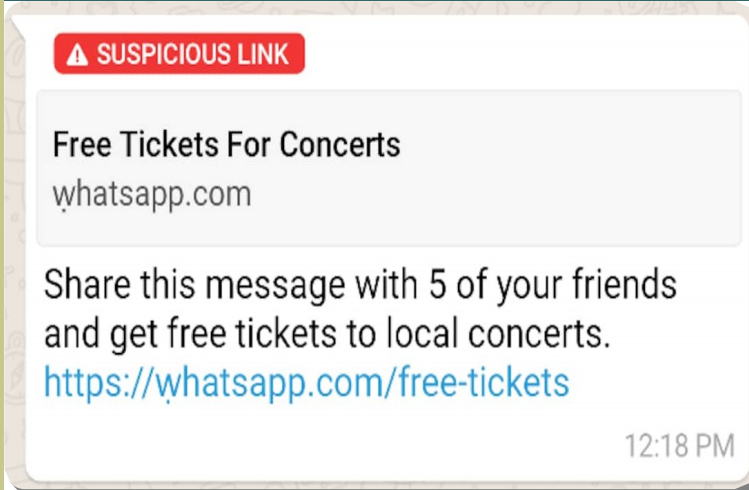
### Warning Signs

- ⚠ Pretends to come from senior officials / top management of the organization
- ⚠ Asks for urgent monetary favours like money transfer to anonymous account, buy gift cards etc.
- ⚠ Pressurizes for immediate action
- ⚠ Informs about the non availability of the concerned official / top management for a certain period over phone

### Safety Precautions

- ✗ Do not trust messages from unknown WhatsApp number
- ✗ Never carry out monetary transaction or purchase gift cards at the behest of any stranger
- ✓ Always verify the authenticity of the message by calling the person concerned or confirm from known trusted sources

# Avoid Phishing at Instant Messaging Platforms



## Malicious Links:

- ⇒ Attackers send messages containing links to malicious websites that closely resemble legitimate ones.
- ⇒ These websites often imitate well-known platforms or services and prompt users to enter personal information, such as login credentials or payment details.

## Gifts and Prizes:

- ⇒ Attackers promise fake rewards, prizes, or exclusive offers to lure users into sharing personal information. These messages exploit users' desire for discounts or freebies.

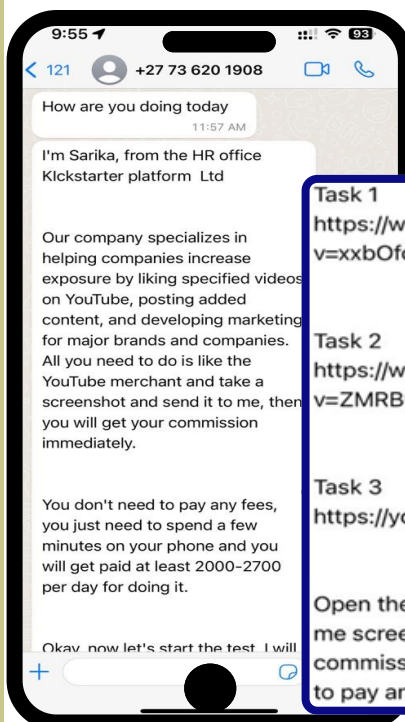
## Attachments with Malware:

- ⇒ Attackers send seemingly harmless attachments, such as documents, images, videos or files with malicious extensions like .APK, .EXE etc. Once downloaded, these attachments may contain malware that compromises the recipient's device.



**Beware of random "APK" files**

Never download Application or document by clicking on random "APK" files received on WhatsApp / SMS / Email.



## Fake Offer & Customer Support:

Task 1  
<https://www.youtube.com/watch?v=xxbOfoDKd8g>

Task 2  
<https://www.youtube.com/watch?v=ZMRBGiLXjUM>

Task 3  
<https://youtu.be/0xkb5hb9DqQ>

Open the video, click LIKE, send me screenshot, after that, your commission will be paid, no need to pay anything

- ⇒ Attackers pretending to be customer support representatives from trusted organizations, offer assistance and request sensitive information under the guise of resolving an issue.
- ⇒ Fraudster posing as representative of advertising company offers task-based part-time job to unsuspecting user and lure them with lucrative deals on easy money earning through just clicking links / liking YouTube videos.



# Avoid Phishing at Instant Messaging Platforms

## How to avoid such Scams ?



### Do's

- ✓ If a call or message claims to be from reputable organization, verify the authenticity through alternate & trusted communication such as by visiting organization's official website / apps, direct communication through phone calls, physically contacted to nearby Branches / Offices etc.
- ✓ Block and report suspicious numbers in instant messaging platform to avoid potential scams.
- ✓ Regularly update devices, operating systems & Apps to ensure the latest security patches are in place.
- ✓ Enable Multi-factor Authentication (MFA) to add an extra layer of protection to your account.



### Don'ts

- ✗ Entertain calls from unknown international numbers particularly from countries like +84 (Vietnam), +62 (Indonesia), +223 (Mali), GizChina etc.
- ✗ Share personal / sensitive / financial information to unknown callers
- ✗ Respond to Online quizzes, surveys, unknown forms/documents that request personal information.
- ✗ Reveal your information on random websites / Apps
- ✗ Overshare your information on Social Media Platforms
- ✗ Click on suspicious links from unknown messages, Emails, random Pop-up ads etc.

## Best Practices to Stay Safe at Instant Messaging Platforms

- ✗ Never respond calls, requesting personal or sensitive information / urge for immediate action / seem too good to be true, do not blindly follow instructions or engage in financial transactions.
- ✗ Never dial codes or send SMS from your number at the behest of strangers. Always check with your service provider before doing so.
- ✓ Be vigilant about call/SMS forwarding settings on your phone / SIM network service(s). If call/SMS forwarding features are enabled accidentally / unknowingly, immediately contact your mobile network provider (such as Jio, Airtel, etc.) from the official website / App to deactivate the same.
- ✗ Never click on any unknown link & do not share OTP, PIN, UPI PIN, password or any other personally identifiable / sensitive information with anyone.
- ✓ Beware of Urgent Requests for Financial Assistance by strangers. Always verify the sender's identity through an alternative communication channel before taking any action.
- ✓ Enable Two-factor authentication (2FA) for your accounts, including WhatsApp to add extra layers of security and thereby reducing the risk of unauthorized access & misuse.
- ✓ Regularly monitor your Bank account activities. If any unauthorized or suspicious transaction is noticed, immediately inform to your Bank / Branch. For UCO Bank, dial Customer Care / Helpline Number 1800 103 0123 for help / assistance.

# Case Studies on Phishing Attacks



In the evolving landscape of cyber threats, phishing attacks stand as one of the most pervasive and insidious. A case study delving into real-world instances of phishing attacks offers a glimpse into the tactics, techniques, and impact of these malicious campaigns. By analyzing actual scenarios where individuals and organizations fell victim to phishing, we gain valuable insights into the methods employed by cybercriminals to manipulate human psychology, exploit vulnerabilities, and breach security defenses.

## Case Study 1: "The CEO Fraud"

In this case study, a multinational corporation fell victim to a sophisticated spear phishing attack known as "The CEO Fraud." The attackers meticulously researched the organization and identified the CEO's name, email address, and key financial personnel. They then crafted an email that appeared to be from the CEO and used an almost identical domain name to the company's legitimate domain.

The fraudulent email was sent to the organization's CFO, requesting an urgent and confidential wire transfer to a foreign bank account to secure a lucrative business deal. The email leveraged authority, urgency, and confidentiality to dissuade the CFO from seeking confirmation or verification.

Unaware of the ruse, the CFO initiated the wire transfer, resulting in a substantial financial loss for the company. The attack was only discovered when the CEO inquired about the transaction days later, revealing that he had never sent the email.

### 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**

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

**To: Chandu Sur <chandu.sur@abc.co.in>**

**Subject: Urgent Payment instruction**

**creates urgency to act immediately**

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

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.

**asks for immediate action**

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

**requests for money transfer to unusual account number**

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

**MD & CEO ABC COO.**

**spelling of establishment may be changed**

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

# Case Studies on Phishing Attacks.....contd.

## Case Study 2: "The Tax Season Phish"

In a recent cyber attack, cybercriminals exploited individuals' fears and confusion regarding income tax procedures. They launched a widespread phishing campaign using fake emails and SMS messages, pretending to be from official tax authorities. The goal was to steal sensitive personal and financial information from unsuspecting taxpayers.

### Consequences:

- ⇒ Several taxpayers fell victim to the scam, divulging their confidential information under the guise of complying with tax regulations.
- ⇒ With the stolen data, the attackers could engage in identity theft, financial fraud, and unauthorized access to bank accounts.

## Beware of Fake Income Tax Return Email & SMS

From: IncomeTaxDept <admin@fradesigner.com>  
 Sent: Tue, 06 Jun 2023 10:14:36  
 To: [Redacted]  
 Subject: <Name> confirm your refund details and mobile verification FRM81HJ812023



**e-Filing** *Anywhere Anytime*

Income Tax Department, Government of India

FAKE

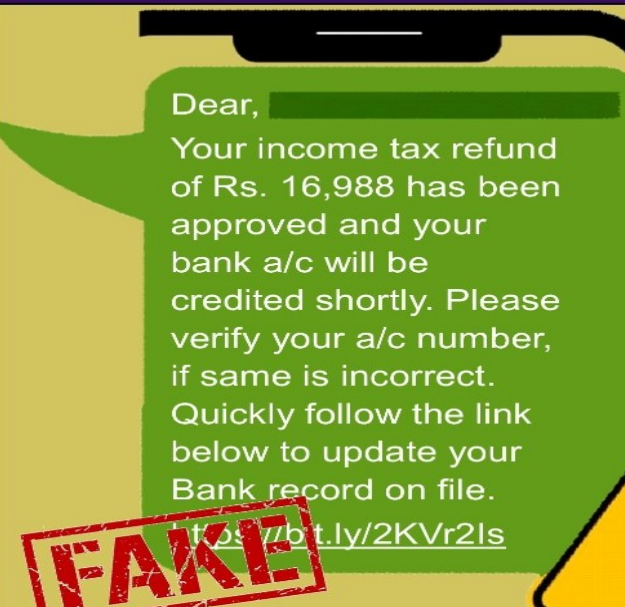
Dear <Name>

We are pleased to announce that the Tax Office has completed its tax audit. You are eligible for a overdue refund of Rs 41,542.81 but your account information in your database is incorrect. Please follow the steps outlined below to complete and submit your request. Make sure to enter the correct credentials.

Submit a refund request by clicking on the link below.


Proceed





Dear, [Redacted]  
 Your income tax refund of Rs. 16,988 has been approved and your bank a/c will be credited shortly. Please verify your a/c number, if same is incorrect. Quickly follow the link below to update your Bank record on file.  
<https://t.ly/2KVr2ls>

- ❌ Do not respond to such Emails and SMS & Avoid clicking on any unknown link
- ❌ Never share personal / sensitive / financial information with anyone or random websites / Apps
- ✅ Be vigilant and skeptical about unsolicited emails claiming to be from Income Tax Department
- ✅ Always check sender's email address carefully and verify the authenticity of the communication from official website



# Case Studies on Phishing Attacks.....contd.

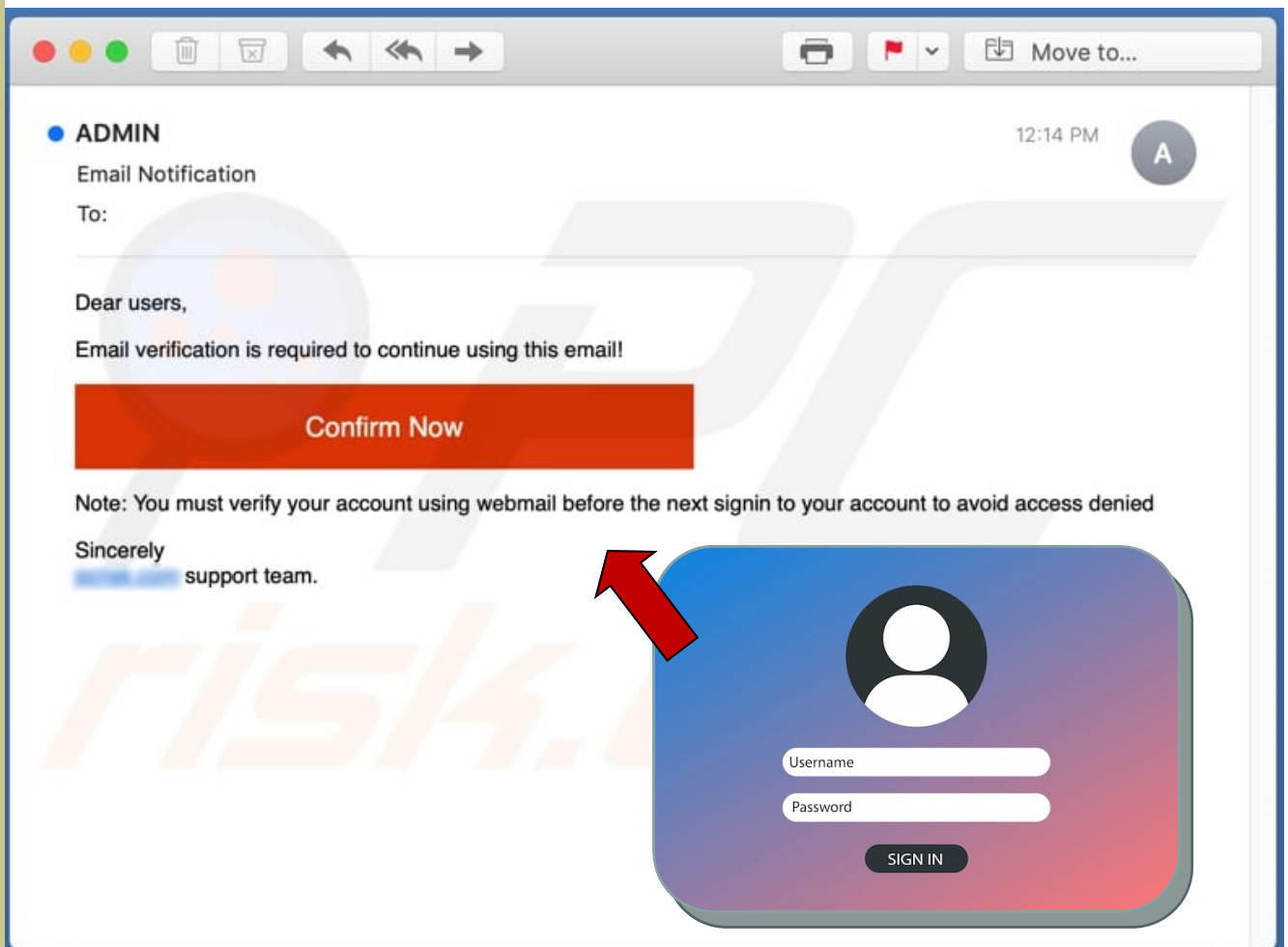
## Case Study 3: "The Credential Harvesting Campaign"

A leading educational institution faced a persistent and targeted phishing attack that aimed to harvest login credentials from faculty, staff, and students. The attackers sent out emails masquerading as a mandatory account verification process, warning recipients of potential account suspension if they failed to update their credentials.

The phishing emails were designed to mimic the institution's branding and included a convincing link to a fake login page. Unsuspecting recipients who clicked on the link unknowingly submitted their usernames and passwords, which the attackers immediately harvested.

With access to the stolen credentials, the attackers gained unauthorized entry to various academic and administrative systems. They used this access to launch further attacks, including identity theft, data breaches, and unauthorized grade changes.

The institution discovered the phishing campaign after an increase in reports of compromised accounts. An immediate response involved warning the campus community about the phishing attempt and advising them to update their passwords through the institution's official website. The incident prompted the institution to enhance its cyber security awareness training and implement multi-factor authentication to protect against future phishing attacks.



# Case Studies on Phishing Attacks.....contd.

## Case Study 4: "Scam through fake Loan Apps"

People looking for instant loans are first asked to download an aggregator app. This app then directs them to other apps that process the loan request after collecting Aadhaar, PAN details and a selfie of the applicant. After submission of the required data the loan is sanctioned immediately with levy of huge interest and processing charges. The applicant gets few days such as 1-2 weeks for repayment. This types of Apps also ask for access to the users' photo gallery and phone contact list.



If the borrowers fail to repay the amount on the due date, there are multiple harassment from lender's side like systematic abuse, blackmailing and threatening calls, sending fake legal notices to family members and relatives, leakage of personal data and morphed pictures in different media.

### Warning signs

! Offers instant hassle free loans without credit score

Lender is neither registered with the Govt. nor approved by RBI !

! Demands for advance payment in the name of instant loan approval



! Offers low interest rate initially but later demands usurious rates & opaque charges !

! Lack of company website, physical address or contact information

! Loan App asks for granting unnecessary permissions to access user's personal data, images, contacts, messages etc !

### Safety Precautions to Avoid such Scam


 Do not click on suspicious links received through Emails, SMS, WhatsApp, Social Media for availing loans

 Stay away from lenders who ask for any advance payment in the name of sanctioning of loans

 Never share sensitive personal or financial information with anyone

 Never download unknown Apps at the behest of any stranger. Always read users' reviews, ratings etc before downloading any App

 Avoid easy loan offers which are too good to be true

 Frequently review App Permissions and do not grant unnecessary permissions to apps

**Always apply loan from RBI approved Banking & Financial Companies.**  
**To apply loan from UCO Bank, visit our nearest Branch or refer official website [www.ucobank.com](http://www.ucobank.com)**

## Case Study 5: "Parcel Delivery Scam"

# Beware of Parcel Delivery Scam: Safeguard Your Data from Deceptive Tactics

Now a days, individuals awaiting parcels are defrauded by fraudsters through social engineering tactics.



## Modus Operandi of the Scam

- ⇒ Individual / citizen who is expecting courier / parcel, contacts a courier helpline number found through search engine.
- ⇒ Fraudster, with the guise of a courier service agent, cunningly gains the individual's trust and convinces to share the order number and tracking code under false pretenses.
- ⇒ By creating a sense of urgency, fraudster pressurizes the individual to quickly update the delivery address to receive the parcel promptly.
- ⇒ Fraudster then instructs the individual to download 'AnyDesk' App - a remote access tool & persuades for sharing the unique address code displayed within the App.
- ⇒ After that, using deceptive techniques, fraudster coerces the individual into accepting App permissions and security warning notifications for gaining control of the device remotely.
- ⇒ The fraudster sends a Google Form link to the individual through text message, asks to fill up the personal details & also encourages the individual for paying a small amount as "address verification charge" using debit or credit card.
- ⇒ During the payment process, the individual's personal information and card details are captured. Armed with this data and remote access to the victim's device, fraudster initiates unauthorized transactions and reads OTPs received during transactions, causing financial loss to the victim.



## Best Practices to Avoid such Scam

- ✗ Avoid searching Customer Care or Helpline number on search engine because fraudster may display misleading information/ads under spoofed / fake website to lure individuals.
- ✓ Always refer the official website or App of the organization to find legitimate Customer Care or Helpline number related information.
- ✗ Do not download any unknown App and never carry out financial transaction on unknown / random website or at the behest of any stranger.
- ✗ Never share sensitive personal / financial information, such as card details, financial credentials, OTP, PIN, UPI PIN with anyone or in any random forms / websites / social media platforms etc.
- ✓ Carefully review App permissions, notifications, security warnings etc. Do not grant unnecessary permissions to App which allow remote access.

# Case Studies on Phishing Attacks.....contd.

## Case Study 6: "Quid Pro Quo Phishing"

### QUID PRO QUO

### PHISHING!



Fraudster tricks individuals with a fake promise for revealing sensitive information

## Modus Operandi

Fraudster posing as helpful individual, gains the trust of user by offering assistance, technical support, or exclusive privileges

Entices victim with promises of rewards, discounts, freebies, or personalized services

Asks for sensitive information such as usernames, passwords, financial details, or personal data to process the offered benefits

Once user shares the information, fraudster may exploit them for malicious purposes like identity theft, financial fraud, or unauthorized access etc

## Cyber Security Best Practices

Be skeptical about random offers / discounts / ads which are too good to be true



### Tips to Stay Safe

Verify the legitimacy of the offer or request from official website/app

Avoid responding to unsolicited emails /calls / SMS / Links

Never share personal, sensitive & financial information with anyone

# Case Studies on Phishing Attacks.....contd.

## Case Study 7: "Scams with the help of Artificial Intelligence (AI)"

In an era where technology advances at an unprecedented pace, we find ourselves in a digital landscape where even cybercriminals harness the power of artificial intelligence (AI). AI-generated cyber scams have emerged as a new and potent threat that demands our vigilance and awareness.

These sophisticated scams utilize AI algorithms to craft convincing phishing emails, fraudulent websites, and even deepfake audio and video content. The attackers' aim is simple yet dangerous: to deceive users into revealing sensitive information, transferring funds, or taking immediate actions.

Beware of AI  
Voice-Cloning  
Scam

Scammers are employing **artificial intelligence** to replicate individuals voice, using which they dupe their family and friends

**!** Be mindful of unexpected calls asking for urgent financial help, even from people who you know very well

**✓** Always verify the concerned person's identity through alternate communication channel before taking any action

**Chatbot Scams**

Cybercriminals use AI-powered chatbots to impersonate customer support representatives or other legitimate agents, engaging victims in conversations that lead to disclosing sensitive data.

**Impersonation Attacks**

AI-generated profiles and social media accounts can impersonate real people or entities, building trust to extract personal information, credentials, or financial details.

Example of a Family Emergency Scam Call

Chhotu ?? Is that you?

Hi Grandpa, it's me.

Yes, it's me, Chhotu. Grandpa, I'm in trouble, and I need money for bail.

What happened?

Please don't tell Mom or Dad. I'll get in so much trouble.

Please help me!



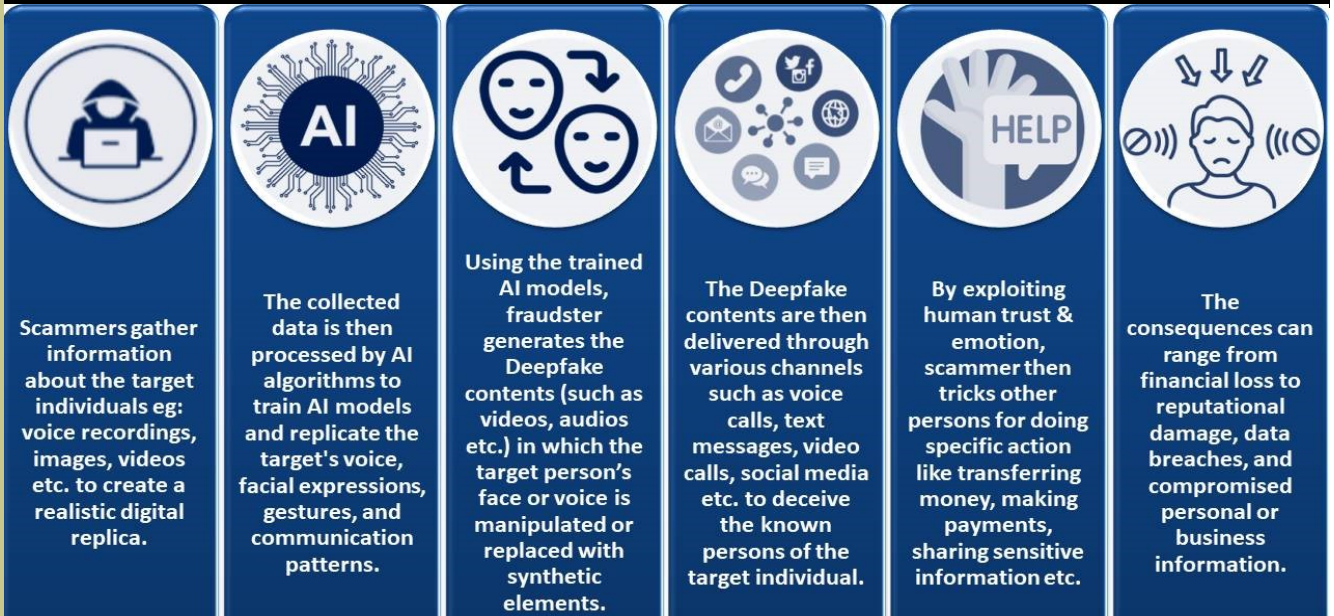
# Case Studies on Phishing Attacks.....contd.

## Beware of AI generated Deepfake Scams



AI-generated cyber scams represent a new and sophisticated avenue of threat in the digital landscape. Nowadays, with the power of Artificial Intelligence (AI), cybercriminals may create fake audio, video, or text content that convincingly mimics real person's voice, appearance or communication style, making it challenging to distinguish between genuine and fake.

### Modus Operandi of the Scam



### Deepfake Scams - Warning Signs & Precautionary Measures



**If you are a victim of Cyber Crime,  
Dial 1930 &  
register your complaint at  
<https://cybercrime.gov.in>**

## **The complainant must provide**

- ⇒ **Mobile Number**
- ⇒ **Name of the Bank and Account Number from which amount has been debited**
- ⇒ **Transaction details (ID and Date of Transaction)**
- ⇒ **Debit / Credit Card Number in case of fraud made by using Card**
- ⇒ **Screen shot of transaction or any other image related to fraud, if available**

**After reporting of complaint, the complainant will receive a system generated Log-in Id / acknowledgement number through SMS/Mail. Using the above Log-in Id / acknowledgement number, the complainant must complete the complaint registration on National Cybercrime reporting Portal ([www.cybercrime.gov.in](http://www.cybercrime.gov.in)) within 24 hours.**



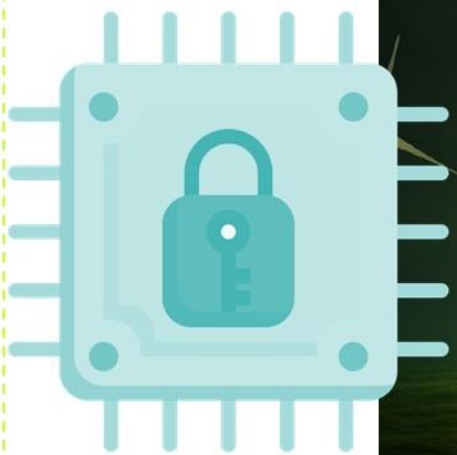
**In case of occurrence of any Cyber Incident like Phishing Email, Virus, Ransomware etc, report immediately to**  
**CISO OFFICE**  
Email at:  
[ciso.office@ucobank.co.in](mailto:ciso.office@ucobank.co.in)  
or Call at:  
**033-4455-7903**

# In Conclusion



As we conclude our expedition into the realm of phishing attacks and mitigation, we reflect on the knowledge gained and the empowerment achieved. The compendium "**Phishing and Countermeasures: A Comprehensive Guide to Identify & Avoid Phishing**" stands as a beacon of light amidst the shadows of cyber deception, guiding our readers to embrace vigilance, knowledge, and resilience in the face of this potent threat.

Armed with this compendium, we stride forward, prepared to thwart the deceptive tactics of the phishing predators and emerge victorious in the ongoing battle to safeguard our digital world. Together, let us raise the shield of awareness and wield the sword of knowledge to defend against the dark art of phishing.



Be a **CYBER JAGROOK** UCOites !

**STAY VIGILANT. STAY SAFE.**

# NEVER BE THE WEAKEST LINK AT THE CYBER SECURITY CHAIN



Keep Your Eyes Open

& Navigate the Digital Landscape with

## Cyber Security Awareness

Together we  
**Defend..**  
Together we  
**Prevail..**



CISO OFFICE

यूको बैंक  
(भारत सरकार का उपक्रम)



UCO BANK  
(A Govt. of India Undertaking)

सम्मान आपके विश्वास का

Honours Your Trust