PHISHING AWARENESS

W.M. CHANDU DISSANAYAKE

CA/S3/6378

AGENDA

Introduction to Phishing

Types of Phishing Attacks

Examples for Phishing Attack Types

How Phishing Works

Common Signs of Phishing Emails

Consequences of Falling for Phishing

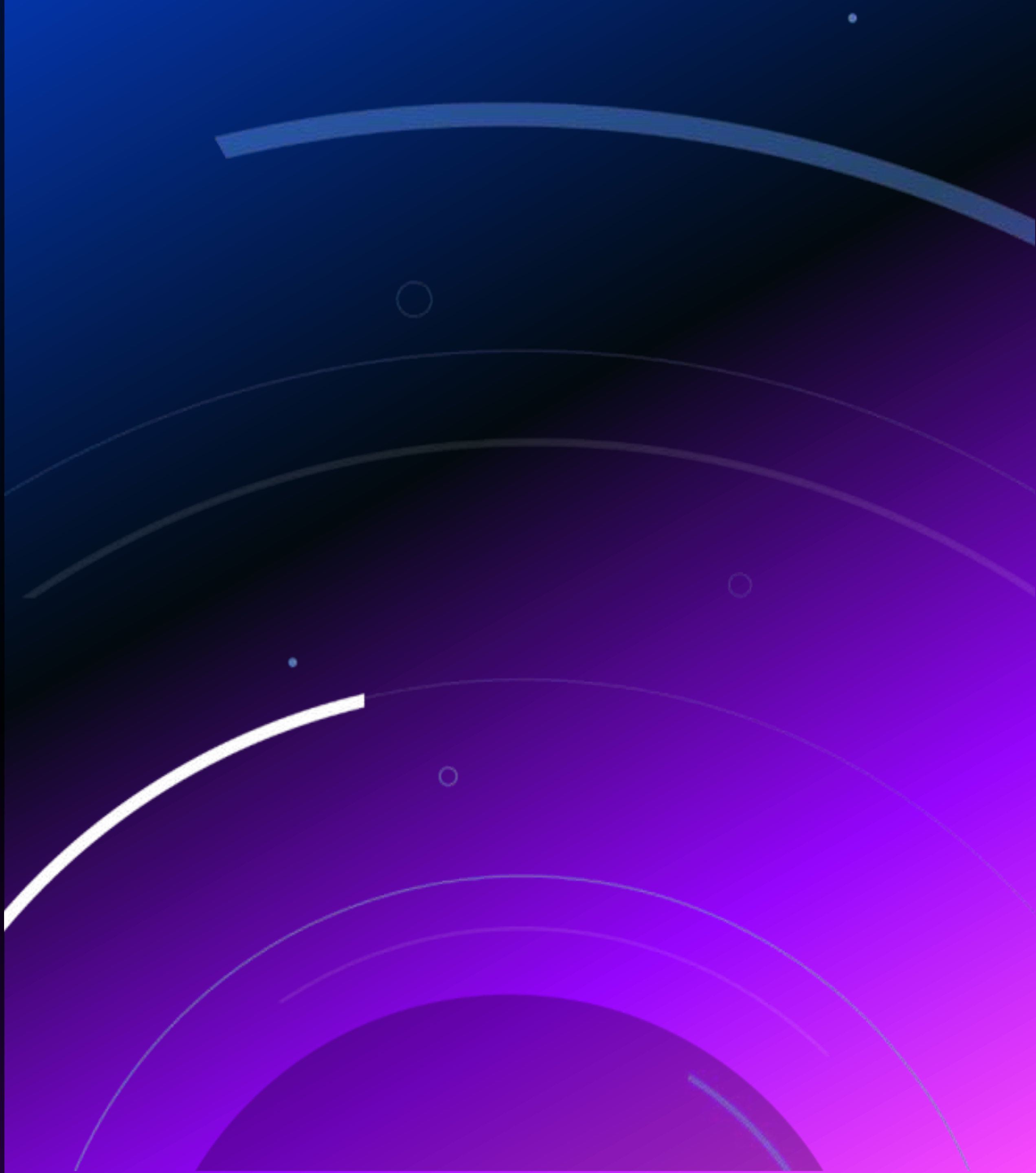
How to Protect Ourself from Phishing

Exploration about Phishing Attacks

Findings from Exploration

Real World Phishing Attack Scenarios

Conclusion



INTRODUCTION TO PHISHING

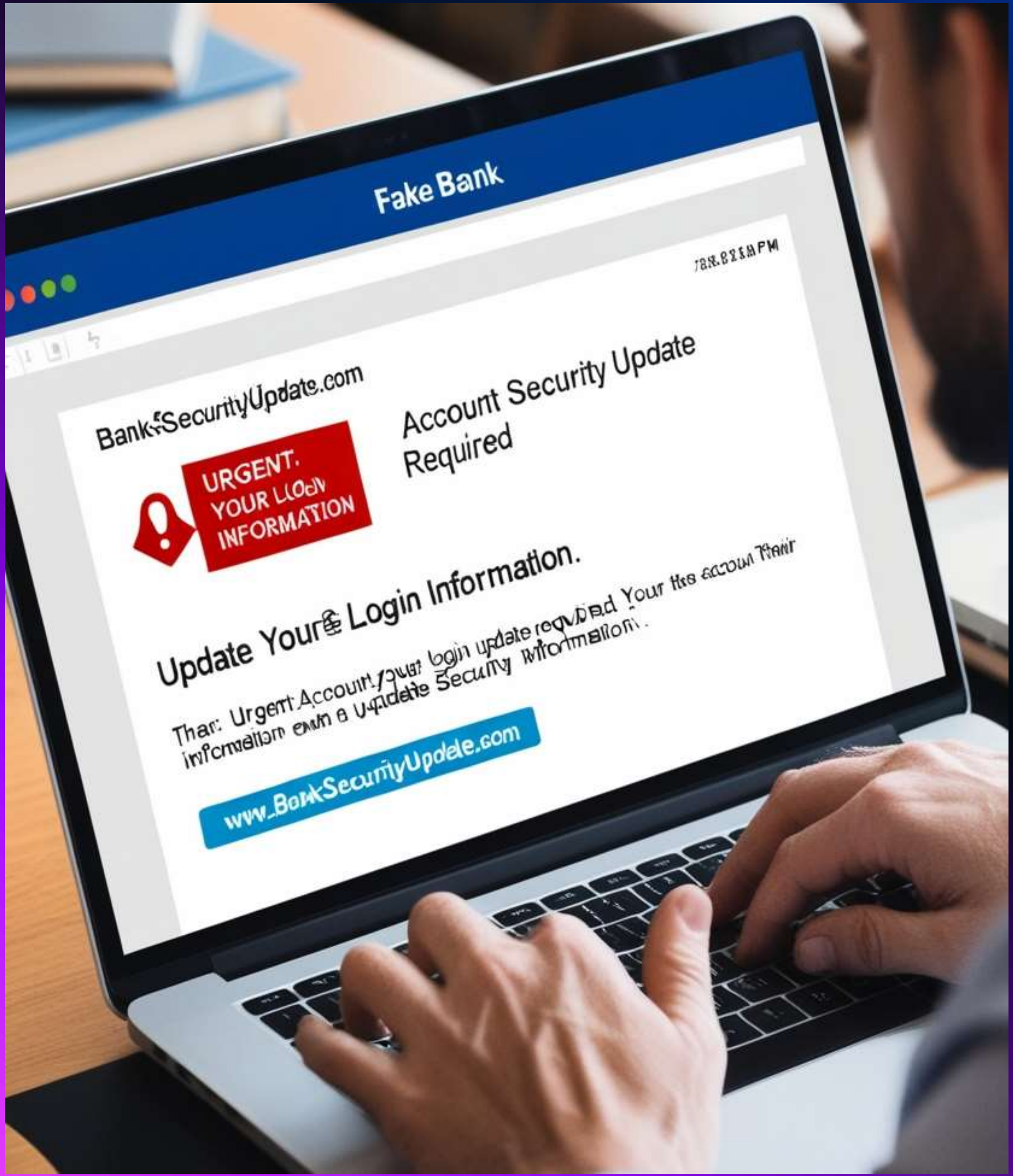
PHISHING IS A CYBER ATTACK WHERE ATTACKERS IMPERSONATE LEGITIMATE ENTITIES, TYPICALLY THROUGH FRAUDULENT EMAILS OR WEBSITES, TO TRICK INDIVIDUALS INTO REVEALING SENSITIVE INFORMATION LIKE PASSWORDS, FINANCIAL DETAILS, OR PERSONAL DATA FOR MALICIOUS PURPOSES.

TYPES OF PHISHING ATTACKS

- Email Phishing: Most common type, involving fraudulent emails.
- Spear Phishing: Targeted at specific individuals or organizations.
- Whaling: Phishing attacks on high-profile individuals like executives.
- Smishing: Phishing via SMS or text messages.
- Vishing: Phishing via voice calls.
- Angler Phishing: Phishing targets victims via social media platforms.

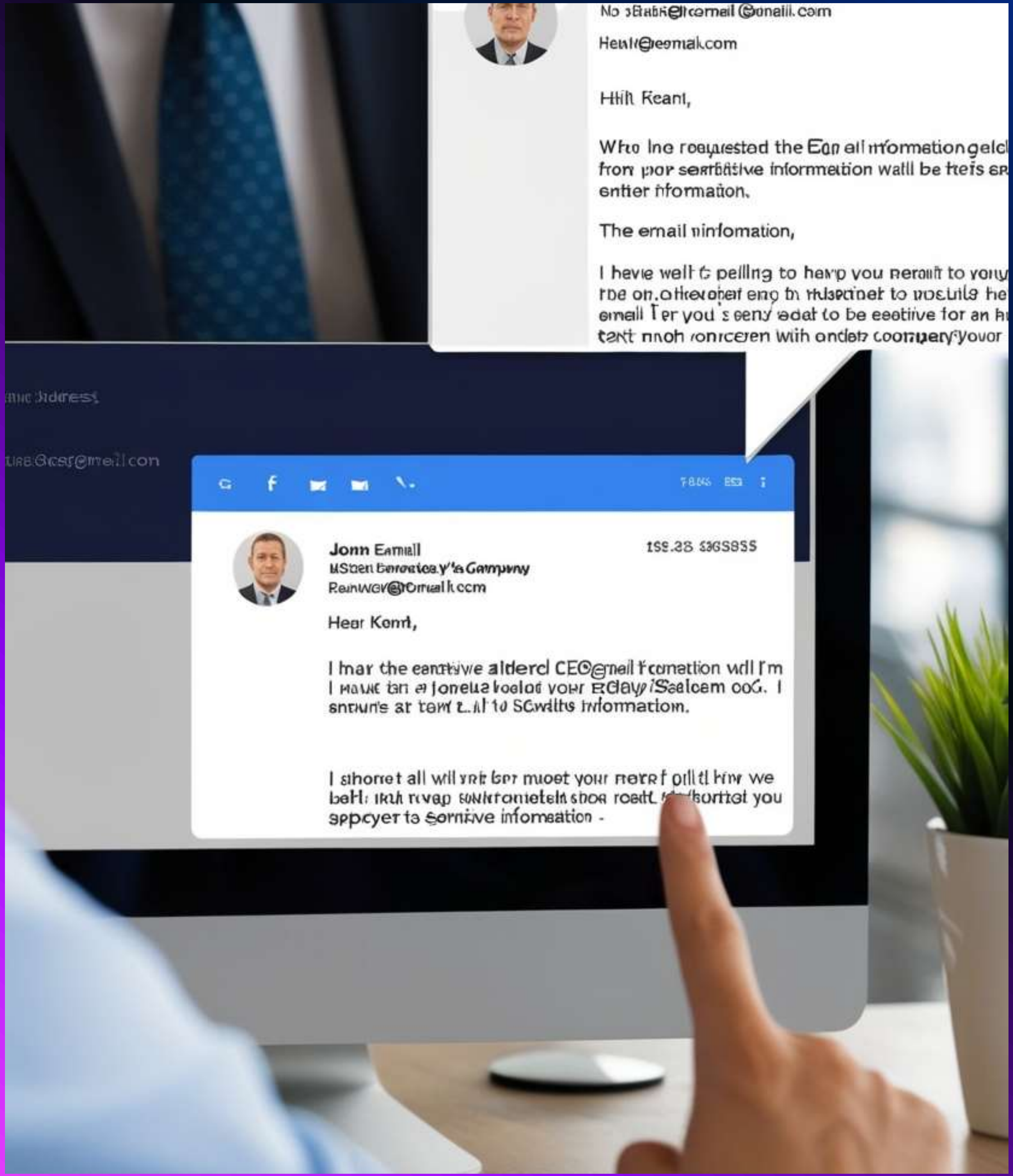
EXAMPLES

FOR PHISHING ATTACK TYPES



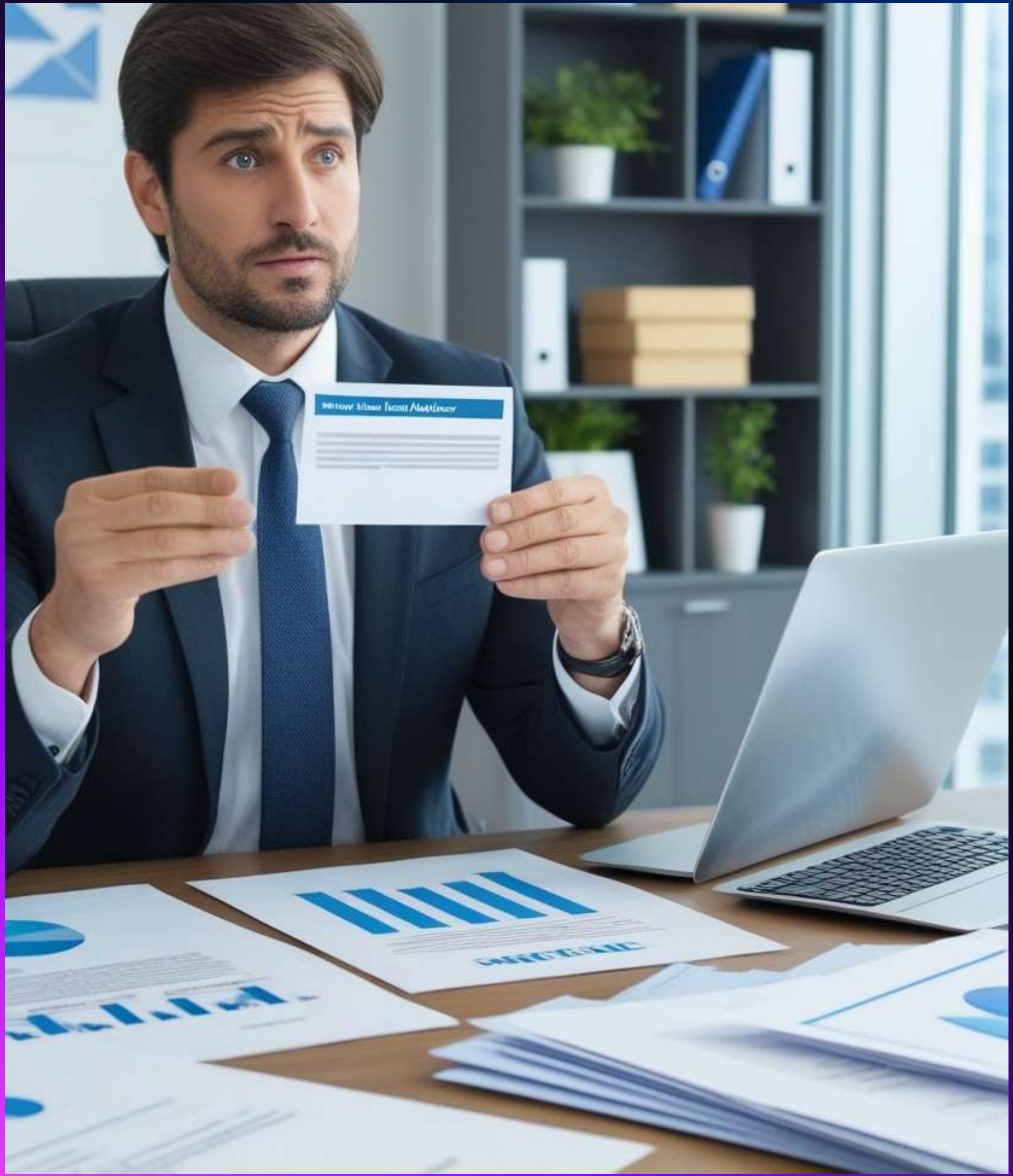
EMAIL PHISHING

As an example for this phishing type, imagine we receive an email claiming to be from our bank, asking us to click a link and update our password. The link leads to a fake website that steals your login information.



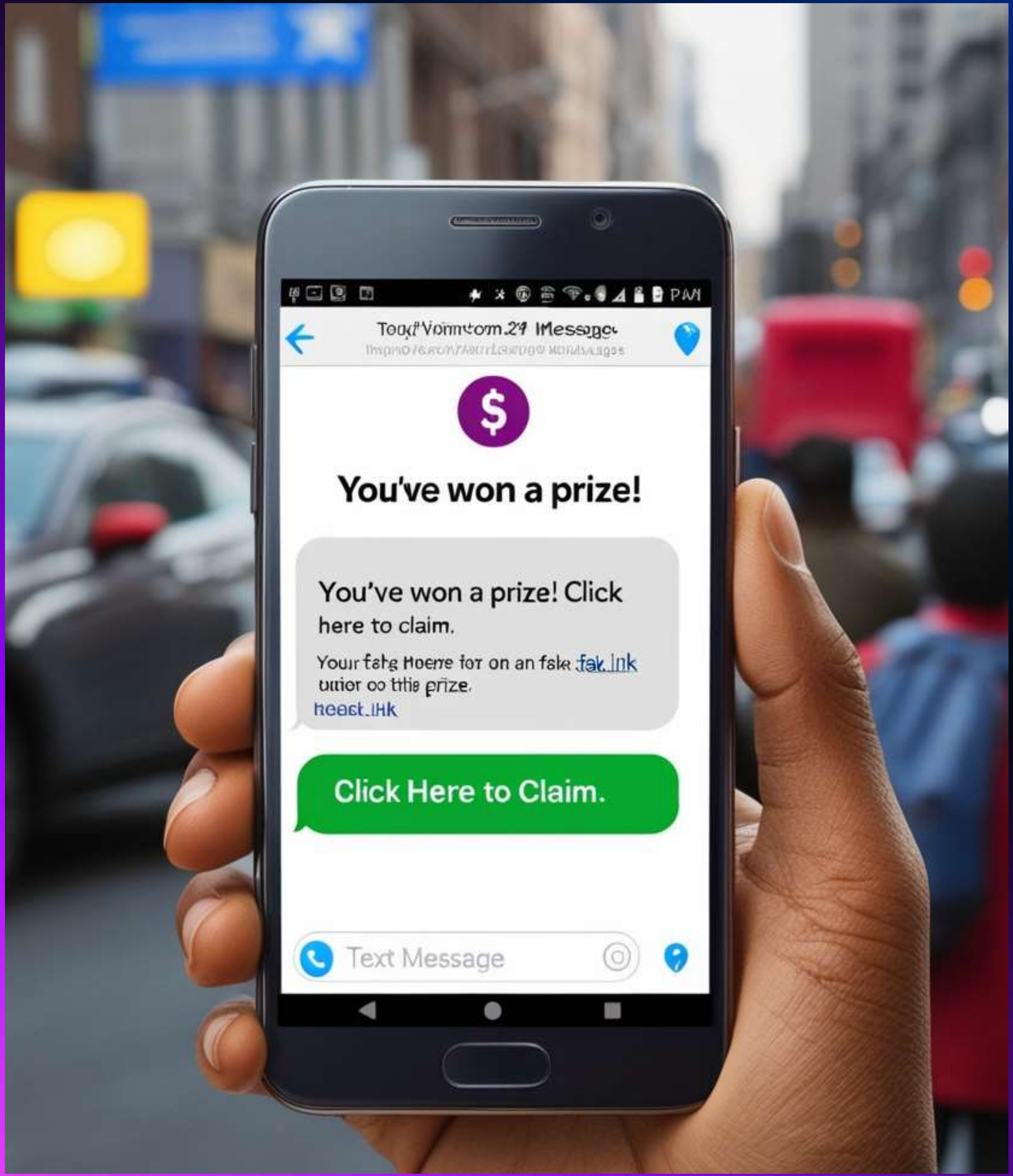
SPEAR PHISHING

As an example for this phishing type, imagine an employee gets an email from what seems to be their boss, asking for sensitive company information. The email looks legitimate but is actually from a hacker targeting the specific employee.



WHALING

As an example for this phishing type, imagine a CEO receives an email that looks like it's from the company’s lawyer, asking for confidential business documents. The attacker specifically targets high-level executives with this approach.



You've won a prize!

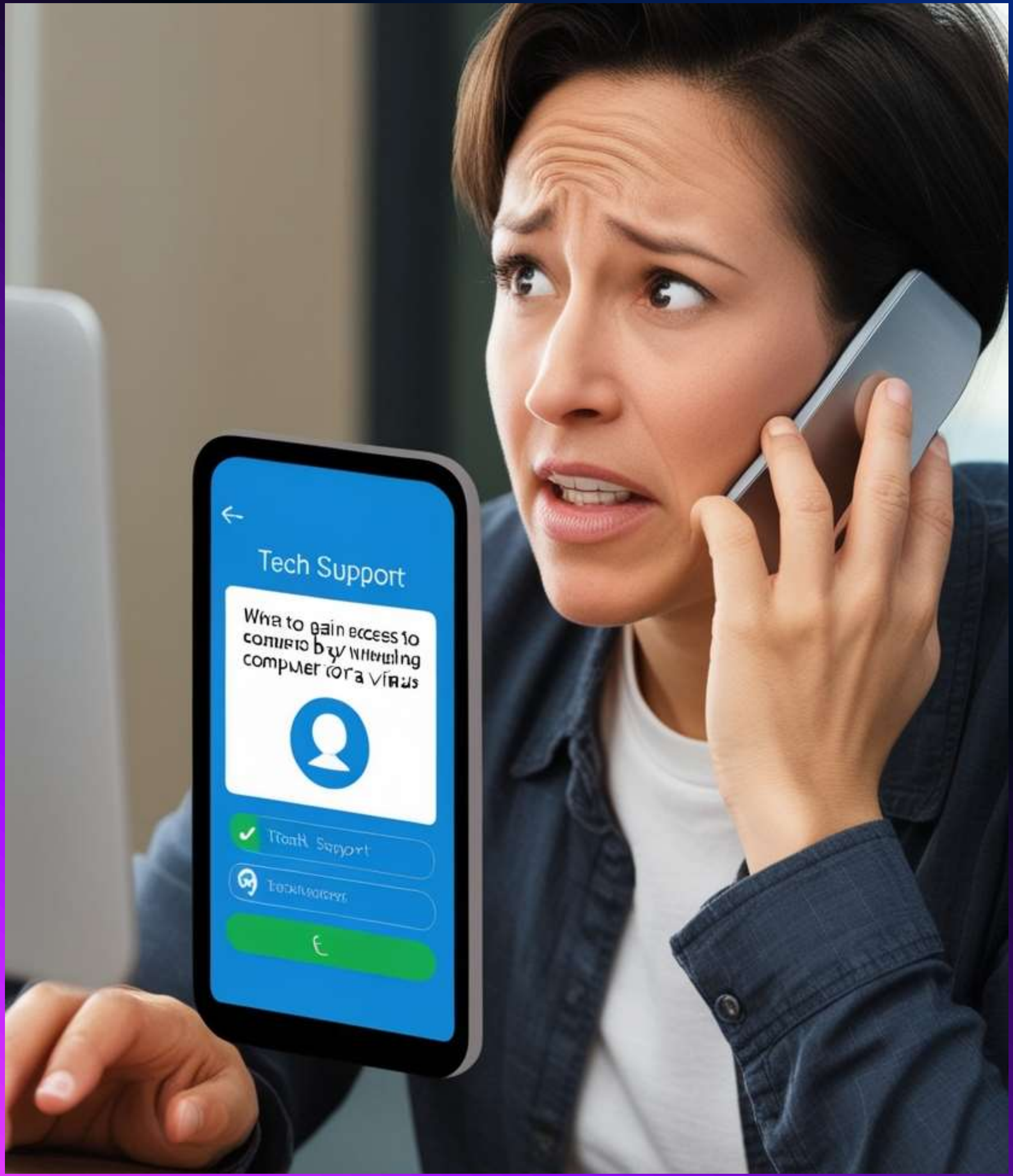
You've won a prize! Click here to claim.

Your fahg Hoene for on an fske fak lnk utiior oo ttie prize.

heact.lHk

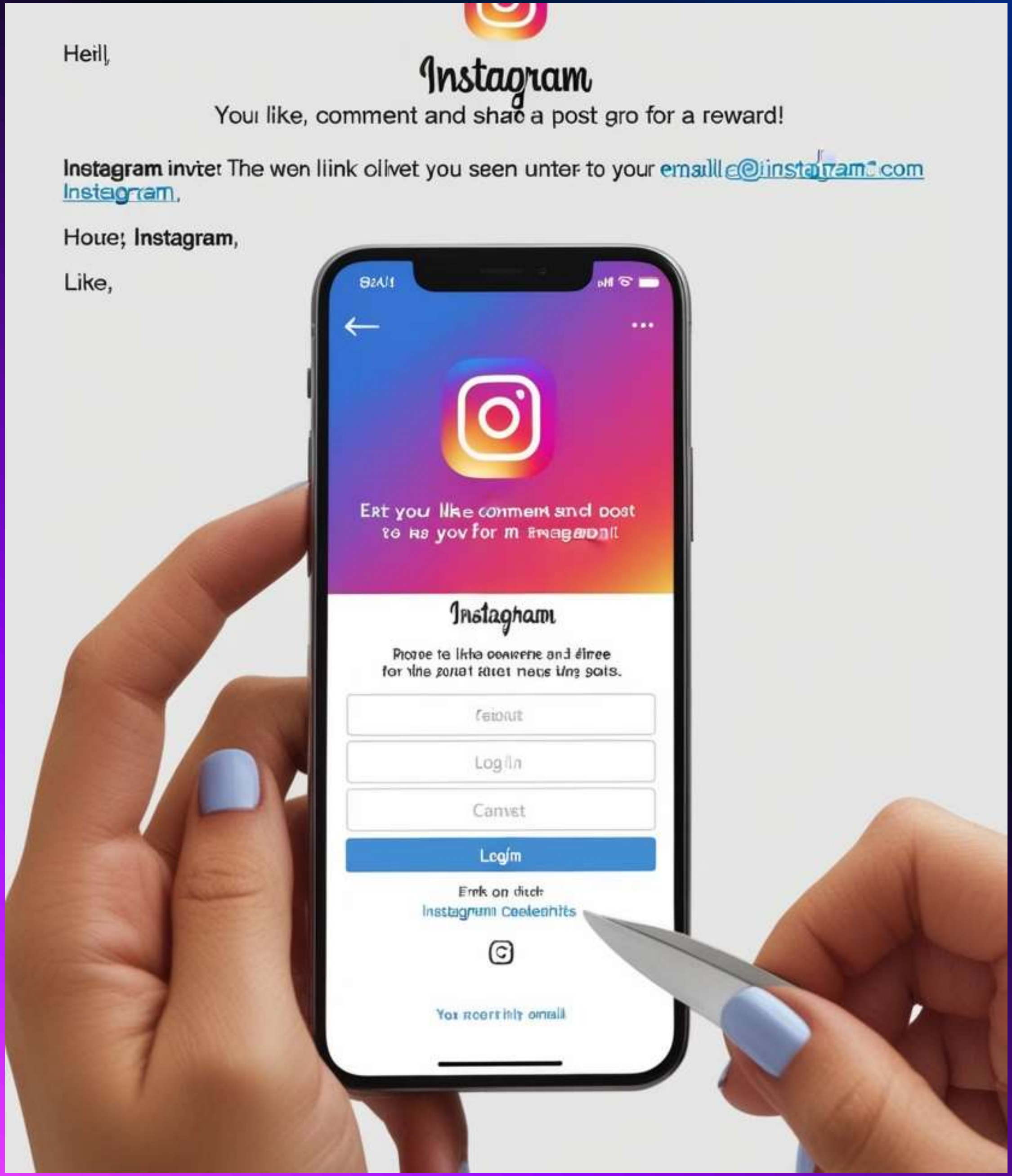
SMISHING

As an example for this phishing type, imagine that we get a text message saying you've won a prize and need to click a link to claim it. The link leads to a site that asks for personal information, which the attacker then steals.



VISHING

As an example for this phishing type, imagine that we receive a phone call from someone claiming to be tech support, saying our computer is infected with a virus. They ask us to provide access to your computer, allowing them to steal your data.


Heill,
Instagram
You like, comment and shao a post gro for a reward!
Instagram invtet The wen liink olivet you seen unter to your emalll e@iinstagram.com Instagram.
Houe; Instagram,
Like,
82Al1
Ert you like conmem and post to Rs yov for m Imagaoalt
Instagram
Rcroe te likle ooakene and dinee for vine ponat sacet neos ling sots.
Feioait
Log in
Canvet
Logim
Erik on dick
Insstagrum Coelechits
You noortiniy omall

ANGLER PHISHING

As an example for this phishing type, imagine that a phishing email pretending to be from Instagram invites the user to click a link to like a post for a reward. When clicked, the link directs to a fake Instagram login page that looks legitimate. The user, believing it’s real, is prompted to enter their Instagram credentials, then stolen by the attackers.

HOW PHISHING WORKS

- Social Engineering: Exploit trust through manipulation.
- Impersonation: Pretend to be legitimate entities.
- Fake Websites: Direct users to realistic-looking fake sites to steal login credentials.
- Malicious Attachments: Contain malware that compromises the user’s device.

COMMON SIGNS OF PHISHING EMAILS

- Suspicious Sender Addresses: Random or slightly altered domain names.
- Urgent or Alarming Language: Creates a sense of urgency.
- Unusual Links or Attachments: Unfamiliar formats or prompts.
- Grammatical Errors: Often contains spelling and grammar mistakes.

CONSEQUENCES OF FALLING FOR PHISHING

- Identity Theft: Stolen personal information leads to identity misuse.
- Financial Losses: Loss of money due to fraudulent transactions.
- Data Breaches: Sensitive corporate or personal data being exposed.

HOW TO PROTECT OURSELF FROM PHISHING

- Verify the Source: Double-check email addresses and links.
- Two-Factor Authentication (2FA): Adds extra security to logins.
- Antivirus Software: Prevents malicious downloads from phishing emails.
- Update Software: Patch vulnerabilities attackers may exploit.

STUDY MORE ON PHISHING ATTACKS TO IDENTIFY ITS FUNCTIONALITY

- Most of the time, Hackers or Malicious Actors use operating systems like Kali Linux or Parrot OS to implement attacks.
- As common tools we can mention Shellphish and Zphisher.
- Tools like above help to clone phishing sites similar to the popular social media platforms or essential services platforms.
- Hackers can easily share the links of the clone sites to their targets.
- Those phishing sites looks legitimate and appeared to be as the original platforms. Thereby users directed to enter their credentials or sensitive information.

FINDINGS FROM EXPLORATION

- We need to think like a thief to protect ourselves from a thief. Likewise, we need to think like a hacker to protect ourselves within this cyber world.

- According to the exploration, the only main way to identify a phishing site is to check the site’s URL twice.

- As an example, imagine a site directed from a link sent by an unknown sender in Email, appeared to be an Instagram login page. We can check the URL twice. If it is original Instagram login page, the URL should be like *https://www.instagram.com/accounts/login/*. If it is not, it may be a phishing site.

REAL WORLD

PHISHING ATTACK SCENARIOS

GOOGLE AND FACEBOOK SCANDAL

- **Example:** In 2017, employees at Google and Facebook were tricked into transferring $100 million to fraudulent accounts through a phishing scam that posed as a legitimate business partner.
- **Lesson:** Phishing can fool even tech giants, proving the importance of strong verification processes and employee training.

TARGET DATA BREACH

- **Example:** In 2013, a phishing email led to a major breach at Target, exposing the credit card information of over 40 million customers. The breach started with phishing emails sent to third-party vendors.
- **Lesson:** Phishing can have devastating consequences when supply chains are compromised.

COVID-19 PANDEMIC SCAMS

- **Example:** During the pandemic, attackers sent fake emails pretending to offer COVID-19 relief funds or health updates. Many fell for these phishing scams, revealing personal and financial details.
- **Lesson:** Crisis situations like global pandemics are exploited by cybercriminals to launch phishing attacks.

SONY PICTURES HACK

- **Example:** In 2014, Sony Pictures suffered a major hack after employees fell for a phishing email, leaking confidential company information and causing significant financial loss.
- **Lesson:** Phishing attacks can lead to massive breaches of sensitive data and irreparable damage to reputation.

CONCLUSION

Phishing awareness is crucial for safeguarding personal and organizational data from cyber threats. By staying informed, recognizing phishing signs, and reporting suspicious activity, we can protect ourselves and others. Always be cautious before clicking links or sharing sensitive information.

THANK YOU

Name: Chandu Dissanayake

Student ID: CA/S3/6378

wmchandu2005c@gmail.com

Cyber Security Domain