भारत 2023 INDIA

वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE

INDIAN OVERSEAS BANK

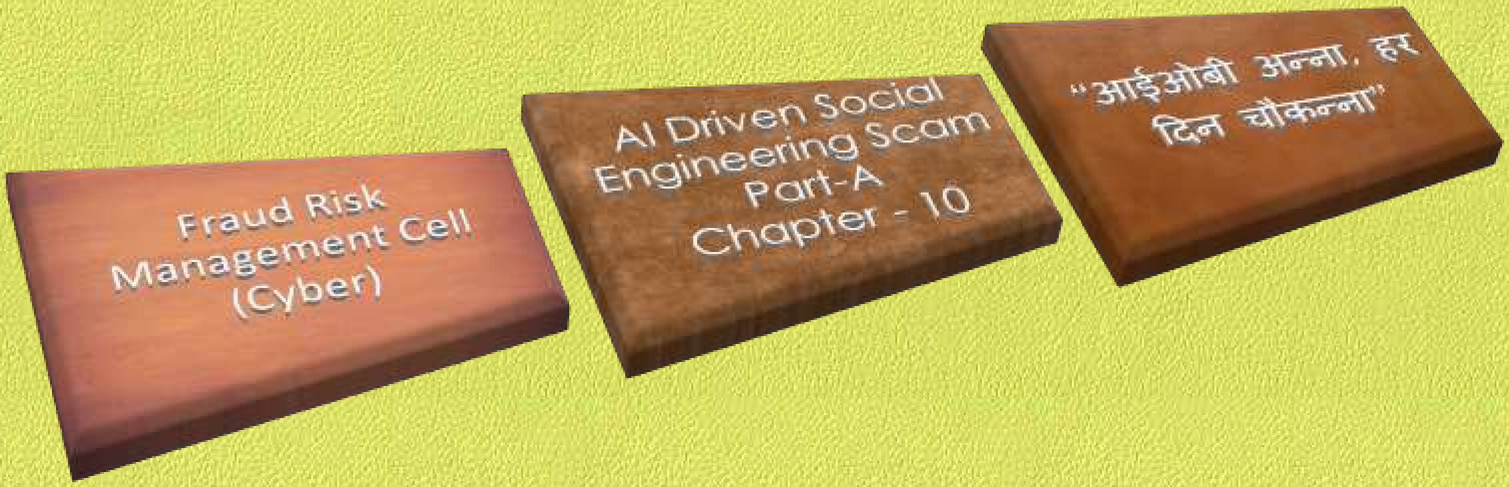
PRESENTS

AWARENESS INCIDENTS BY

IOB ANNA…

(Chapter 10)

(READ IT……….LEARN IT…………USE IT)


Fraud Risk Management Cell (Cyber)
AI Driven Social Engineering Scam Part-A Chapter - 10
“आईओबी अन्ना, हर दिन चौकन्ना”

AI DRIVEN SOCIAL ENGINEERING SCAM

Social Engineering Scam is a cybersecurity scam that relies on the psychological manipulation of human behavior to disclose sensitive data, share credentials, grant access to a personal device or otherwise compromise their digital security. Social engineering exploit peoples’ emotion, instinct, and trust by impersonating an authority figure such as family, friends, government official, boss, client, or co-worker. In advancement of AI technology, cybercriminals are using artificial intelligence (AI) to launch more sophisticated social engineering attacks, and result of that it is becoming increasingly difficult to distinguish between what is real and what is AI-generated. Apart from that as the landscape of commerce continues its steady shift towards online platforms, customers routinely divulge their financial details to various eCommerce entities. This prevalence makes the sector a hotbed for phishing, smishing, and other social engineering tactics. They employ fake phone calls, crafty phishing emails, counterfeit web pages, deceptive chat messages, and even malicious apps.

Four Distinct Phases or Sequential Deceptive Tactics Used For Social Engineering Scams:

1. Reconnaissance or Information Gathering.
2. Building Trust or Creating Urgency or Manipulation.
3. Exploitation.
4. Covering Tracks Or Erasing Digital Footprints

Types of Social Engineering Frauds:

1. **PHISHING:**

   Phishing is One of the most common forms of social engineering scams. Phishing is a deceptive practice where a fraudster sends emails or messages disguised as a reputable entity, typically luring the individual into providing their financial and confidential information. Phishing manifests in various forms, including email phishing, spear phishing and business email compromise (BEC). These deceptive techniques aim to trick people into divulging sensitive data or unknowingly downloading malware.

   Phishing and Spear Phishing are the most common types of social engineering attacks. It involves an attempt to access personal information such as credentials by acting as an authentic identity to fool individuals. The difference between them is that phishing attacks are usually targeted towards many people while spear phishing attacks are targeted towards single individuals.

   Attackers usually send spoof emails or instant messages to the victim. These emails and messages often instill a sense of urgency to manipulate victims into responding quickly. Victims are usually steered towards thinking that the phishing emails or messages are real and are often asked to insert their sensitive details to a fraudulent website designed to look exactly like a legitimate site. The consequences of a successful phishing attack can be far-reaching, ranging from financial losses to reputational damage and compromised data security.

2. **WHALING:**

   A whaling attack is a type of phishing attack that also leverages personal communication to gain access to a user's device or personal information.

   The difference between phishing and whaling has to do with the level of personalization. While phishing attacks are not personalized and can be replicated for millions of users, whaling attacks target one person, typically a high-level executive. This type of attack requires a significant amount of research on that individual, which is usually done by reviewing their social media activity and other public behavior.

   Though whaling attacks require more planning and effort initially, they often have huge payoffs as the targets have access to high value data or the financial resources needed to advance a ransomware attack.

3. **BUSINESS EMAIL COMPROMISE (BEC):**

   Business Email Compromise (BEC) is a social engineering tactic where the attacker poses as a trustworthy executive who is authorized to deal with financial matters within the organization. In this attack scenario, the scammer closely monitors the executive's behavior and uses spoofing to create a fake email account. Through impersonation, the attacker sends an email requesting their subordinates make wire transfers, change banking details, and carry out other money-related tasks. BEC can result in huge financial losses for companies. Unlike other cyber scams, these attacks do not rely on malicious URLS or malware. BEC attacks are carried out strictly by personal behavior, which is often harder to monitor and manage, especially in large organizations.

4. **SMISHING / SMS-PHISHING:**

   SMS-phishing, or smishing, is a social engineering attack conducted specifically through SMS messages. In this attack, scammers attempt to lure the user into clicking on a link which directs them to a malicious site. Once on the site, the victim is then prompted to download malicious software and content. Smishing attacks have increased in popularity amongst criminals as people spend more time on mobile devices. While users have become savvier at detecting email phishing, many people are far less aware of the risks associated with text messages. A smishing attack requires little effort for threat actors and is often carried out by simply purchasing a spoofed number and setting up the malicious link.

5. FAKE EMAILS FROM TRUSTED PEOPLE:

Another social engineering attack involves offenders posing to be someone that the victim knows and sending legitimate-looking emails to the victim. Victims are usually trapped into thinking that their trusted person is in need, thus sending over financial details or even money to the offender.

6. CLICKBAIT:

Clickbait is the technique of trapping individuals to click on website links with tempting headlines. Cybercriminals place these links in legitimate sites with similar content, so victims get trapped into clicking the link. Attackers often send enticing advertisements related to games, movies, or other websites. Victims are fooled into thinking that these advertisements are legit, and clicking these links installs executable commands or malware in the system.

7. SENDING DOWNLOADABLE CONTENT:

Another form of social engineering attack is sending files containing music, movies, games, or documents that are too good to be true. A newbie on the internet gets fooled into thinking that they have obtained the files they were looking for, when in fact, these fake files have malware embedded in them.

Some Helpful Dos & Don'ts For Consideration & Adaption

Dos	Don'ts
Check the validity of the source. Pay close attention to the email header and spelling and grammar mistakes, as this is a common sign of a scam.	**Click a link or download files from an unfamiliar or suspicious sender.** Hover your curser over the link to check its validity (without clicking).
Regularly update and patch your operating system and applications to reduce the risk of known vulnerabilities.	**Share your personal information**, including account numbers, passwords, or credit card details.
Remain vigilant when contacted by third parties. Keep in mind that reputable organizations will never ask users to share passwords or log in credentials.	**Respond to urgent requests.** Scammers will often instil a sense of immediacy to prompt action.
Install a pop-up blocker and spam filter. This will detect many threats and even stop infected emails.	**Insert an unknown USB or other device** into your computer.
Invest in cybersecurity software. This should be from a reputable security vendor and updated regularly.	**Allow another user to access** your personal device or accounts.
Use a password manager. This tool will automatically enter a saved password into a valid site.	**Login on the spoofed site, else** saved credential gets compromised.
Only access URLs that begin with HTTPS for secure browsing.	
Enable multifactor authentication (MFA) to reduce account compromise.	
Log in via your account or official website.	
Encouraging a culture of scepticism and critical thinking before sharing sensitive information	
Staying informed about the latest cyber fraud threats and tactics through reliable sources.	

The key to preventing social engineering is a "defense in depth" approach that combines human alertness, measures to prevent the transmission and execution of harmful content, robust antivirus technology, and strong authentication as a last line of defense, in case an attack succeeds. It is impossible to 100% prevention of social engineering attacks from taking place, but however, a multi-layered security approach can counter this menace. Proactivity & Awareness is key against dynamically evolving social engineering scam tactics.

INCIDENT

Mrs. Pushpa is a senior citizen and having a good family. She is very tech savvy person and spending lot of time of social media for interaction, online post etc. One day she was having issue with her banking account, and she was not able to resolve it so for the help she posted the issue on bank's social media page for help. She has posted her mobile number to contact. Later she received a call from perpetrator.

Hello Madam, I am Rahul here, sorry for inconvenience. I will help to resolve your issues. First you register your complaint and for that I am sending you a link on WhatsApp, you have to download and register your complaint first with required details. After completion you contact me for resolution of your issue.

Perpetrator already gathered the information about Mrs. Pushpa from online and regularly keep an eye on Mrs. Pushpa's online activity through social media. When Mrs. Pushpa put a post on Bank's social media webpage, perpetrator sensed the opportunity to dupe Mrs. Pushpa. He called Mrs. Pushpa and asked little-2 information in a familiar way as he was already following from her social media Posts.

Mrs. Pushpa never think twice about the other possibility because perpetrator talked very nicely to her. She followed the instruction and click on the link received on WhatsApp and download a app. She installed app and fill all the details along with bank details, User ID, Password and OTPs. She doubted on these personal details and called the perpetrator before submitting the form.

Hi Rahul, I have downloaded app as you instructed but it required some personal detail whether it is necessary.

Madam, I understand your concern but don't worry about that. All the details are safe and secure and as per bank's grievance redressal process. Please fill the details so I can resolve the issue.

This time also perpetrator convinced Mrs. Pushpa with lucrative and crafty manner and result of that she agreed to fill the form on the app.

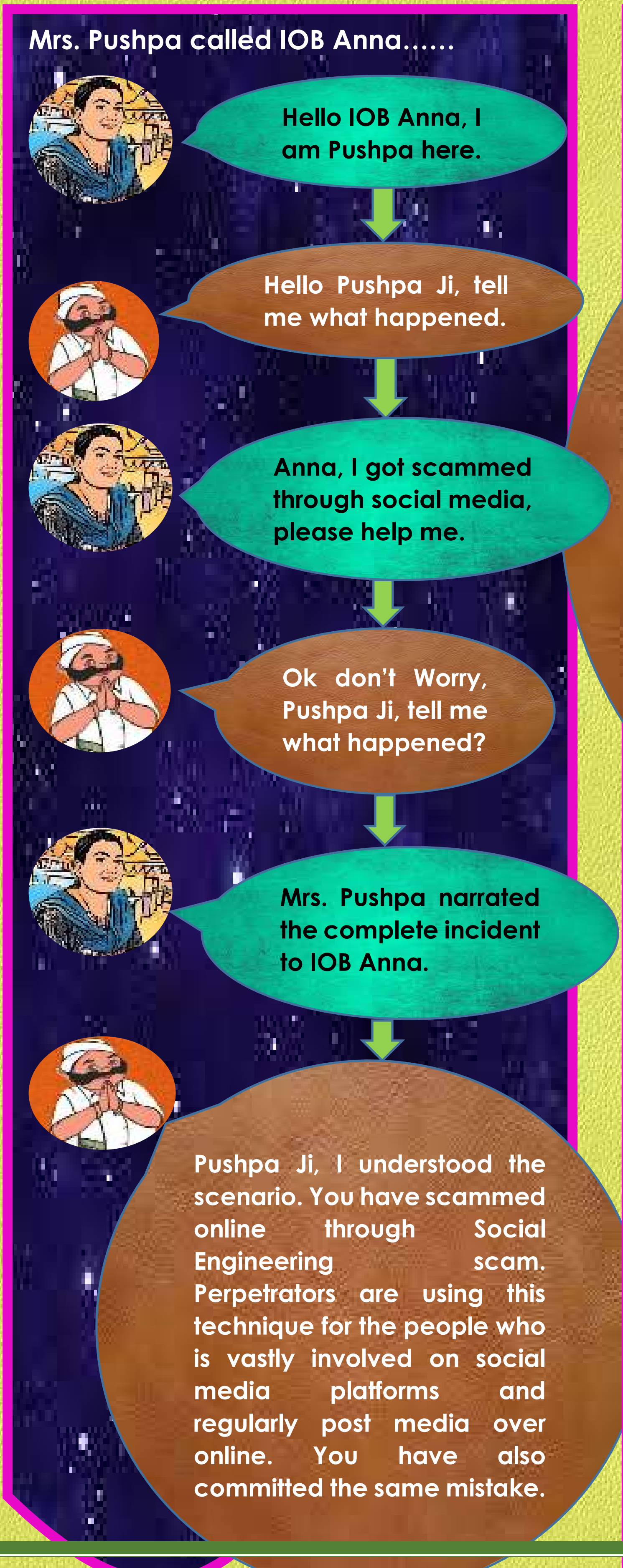
Ok Rahul, I feel something wrong, that is why I called you. Now I am ok. I have submitted the form now you can check.

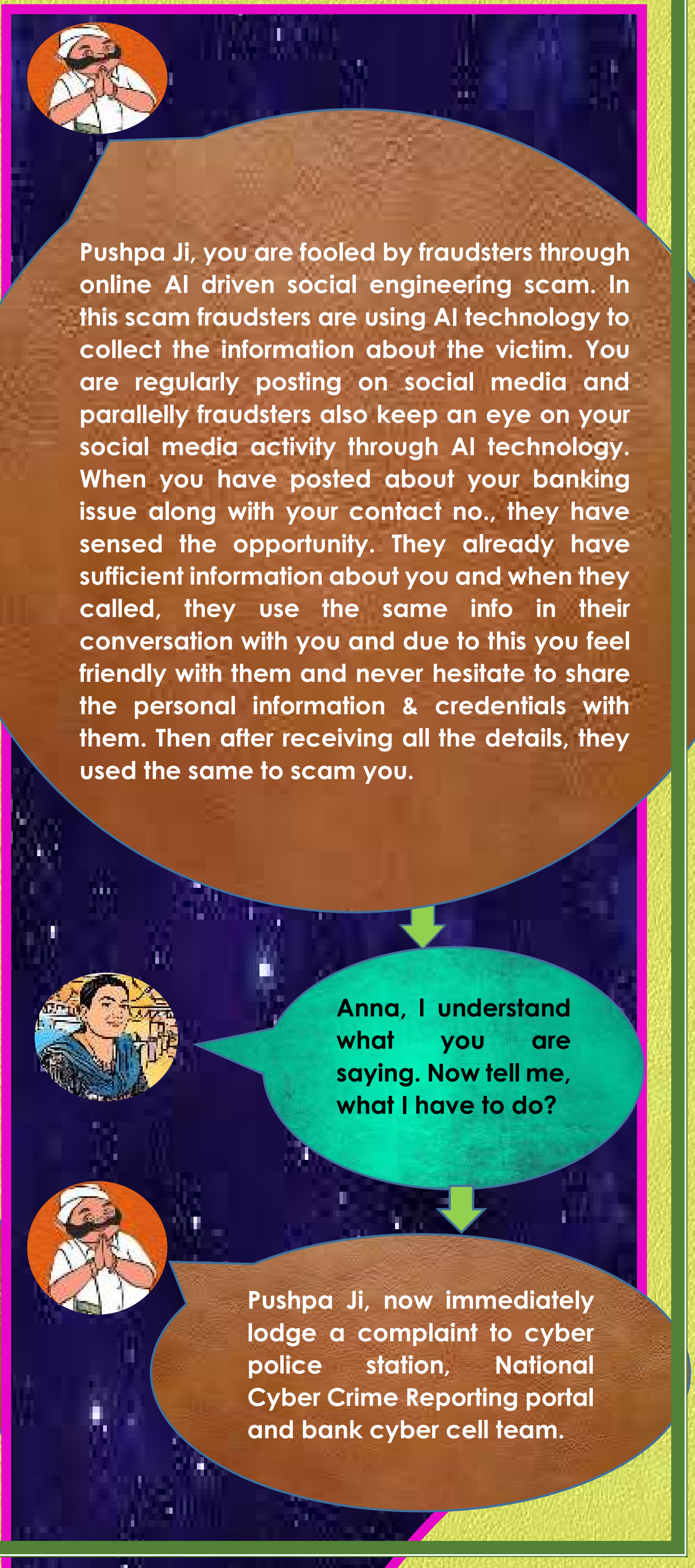
Ok Madam. I will check your complaint came back to you after some time. Don't worry we will resolve the issue. Then Rahul disconnected the call.

After call disconnected, Mrs. Pushpa received msg on the phone that Rs. 1,00,000/- debited from her account. She did not understand why amount debited. Then she calls the perpetrator also but his number was not reachable and she realizes that she got scammed through social media.

She called her relative and shared all the incident. After hearing the incident her relative advised her to contact cyber security expert IOB Anna for immediate help. Mrs. Pushpa called IOB Anna for the help.

Mrs. Pushpa called IOB Anna......


Hello IOB Anna, I am Pushpa here.
Hello Pushpa Ji, tell me what happened.
Anna, I got scammed through social media, please help me.
Ok don't Worry, Pushpa Ji, tell me what happened?
Mrs. Pushpa narrated the complete incident to IOB Anna.
Pushpa Ji, I understood the scenario. You have scammed online through Social Engineering scam. Perpetrators are using this technique for the people who is vastly involved on social media platforms and regularly post media over online. You have also committed the same mistake.


Pushpa Ji, you are fooled by fraudsters through online AI driven social engineering scam. In this scam fraudsters are using AI technology to collect the information about the victim. You are regularly posting on social media and parallelly fraudsters also keep an eye on your social media activity through AI technology. When you have posted about your banking issue along with your contact no., they have sensed the opportunity. They already have sufficient information about you and when they called, they use the same info in their conversation with you and due to this you feel friendly with them and never hesitate to share the personal information & credentials with them. Then after receiving all the details, they used the same to scam you.
Anna, I understand what you are saying. Now tell me, what I have to do?
Pushpa Ji, now immediately lodge a complaint to cyber police station, National Cyber Crime Reporting portal and bank cyber cell team.

Incident Overview by IOB Anna…….

- Mrs. Pushpa is the victim of AI driven Social Engineering scam.
- She posts her financial issue along with contact no. on social media platform where fraudster use the info for their benefit.
- She must visit only bank's official website but instead of that she talked with unknown person for resolution without verifying his identity.
- She clicked on unknown link and downloaded malicious app in her mobile and divulged her personal information and financial credentials on malicious mobile app.

Awareness Tips by IOB Anna…….

- The more information you have posted about yourself, the more likely it is that a criminal can target you for attack. Contain yourself to post more information on social media.
- Limit who can see your posts and information on social media. All platforms collect information about you from your activities on social media so visit your privacy settings to set restrictions.
- If someone appears from social media information and rushes you to provide some help, slow down and ponder before any action.
- Be suspicious of any unsolicited messages. If the links received on your messaging platform, do your own research before click.
- If you don't know the sender's identity, then downloading anything and divulging any personal and financial info is a big setback. Legitimate organizations will never ask you to share sensitive data.
- Use multi-factor authentication. This adds an extra layer of security to your financial activity over online.
- Make sure you are using an updated antivirus software.
- Keep yourself informed about new type of cyber frauds update yourself with their modus operandi. It will help you to recognize and avoid common cyber fraud threats.
- Please contact at Cyber Police Help Line No. 1930 in case of any cyber fraud.
- Please contact IOB cyber cell at 044 2858 4890 & IOB customer care at 1800 425 4445 or send mail at cybercell@iob.in in case of cyber fraud.

Human Firewall Is A Best Defence Against Cyber Fraud!!

इण्डियन ओवरसीज़ बैंक
Indian Overseas Bank
आपकी प्रगति का सच्चा साथी
Good people to grow with

"Protecting Personal Information is Every One's Personal Business, Because Personal Information is not Every One's Personal Business"

Social Engineering Bypasses All Technologies, Because in Social Engineering Scammers are breaching People not Technology!!

THANKS!