14

ASSIGNMENT

R.AISHWARYA REDDY

CYBERSECURITY

HTNO- 2406CYS121

QUESTION 1

1. Choose a fake profile on any social media platform of your preference and identify the red flags signaling its fraudulent nature.

In general, fraudulent social media accounts can be easily detected by certain red flags. Some indications include:

No Posts in the Account: If an account has no posts or activity, it raises suspicion about its legitimacy.

Unreadable Name: Accounts with unreadable or unusual names may be fraudulent.

Impersonation of Celebrities or Influential People: Fraudsters may copy or impersonate well-known personalities with fake posts to deceive users.

Unauthorized Direct Messages: Fraudulent accounts may send unsolicited direct messages, often promising unrealistically good opportunities.

Promises Too Good to Be True: Fraudulent accounts often make promises that seem too good to be true, such as guaranteed success or financial gains.

Creating a Sense of Urgency: They may use tactics like creating a sense of urgency or offering gimmicks to prompt users to click on links or take immediate action.

Direct Interactions: Legitimate businesses may also copycat direct interactions, sending messages that appear authentic but aim to deceive.

Vague or Unrealistic Promises: Messages containing vague promises, such as becoming a model or lucrative investment opportunities, are often indicators of fraud.

High Follower Count in New Accounts: Some fraudulent accounts may have a surprisingly high follower count despite being new, indicating that they have likely acquired fake followers.

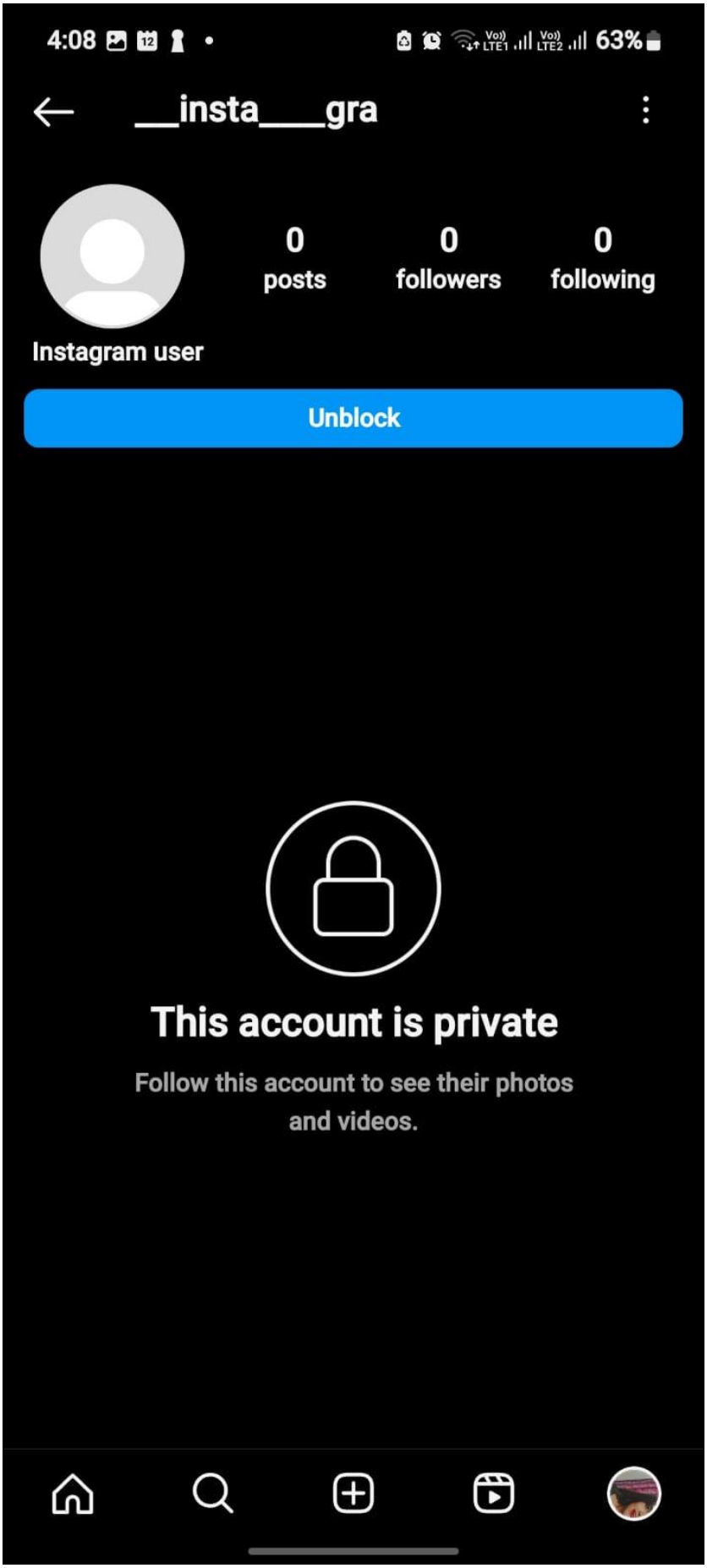
FAKE ACCOUNT NUMBER 1

The account below is a spam account from Instagram

It Has zero followers zero posts and no following

Name is uncommon

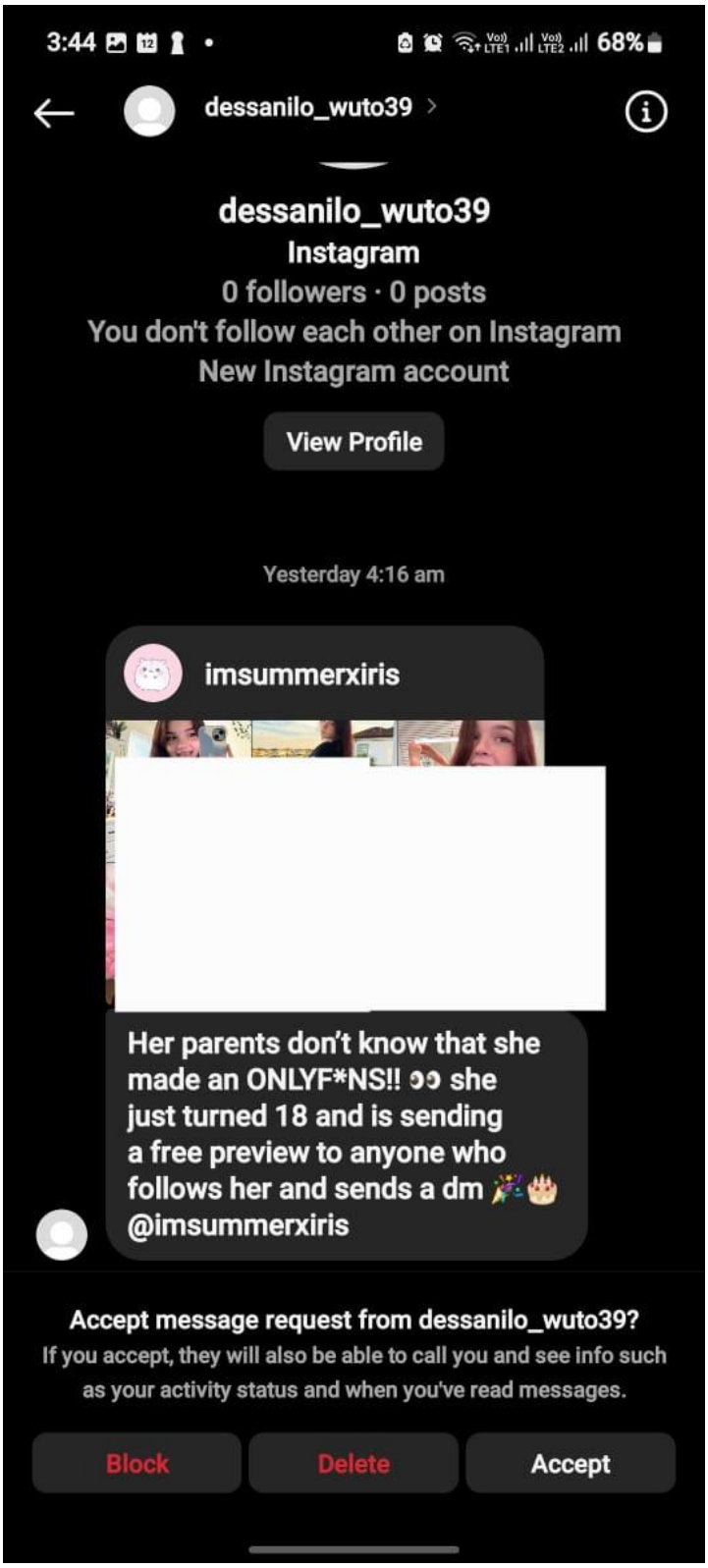
The account user sent follow request


4:08
63%
__insta___gra
0
posts
0
followers
0
following
Instagram user
Unblock
This account is private
Follow this account to see their photos and videos.

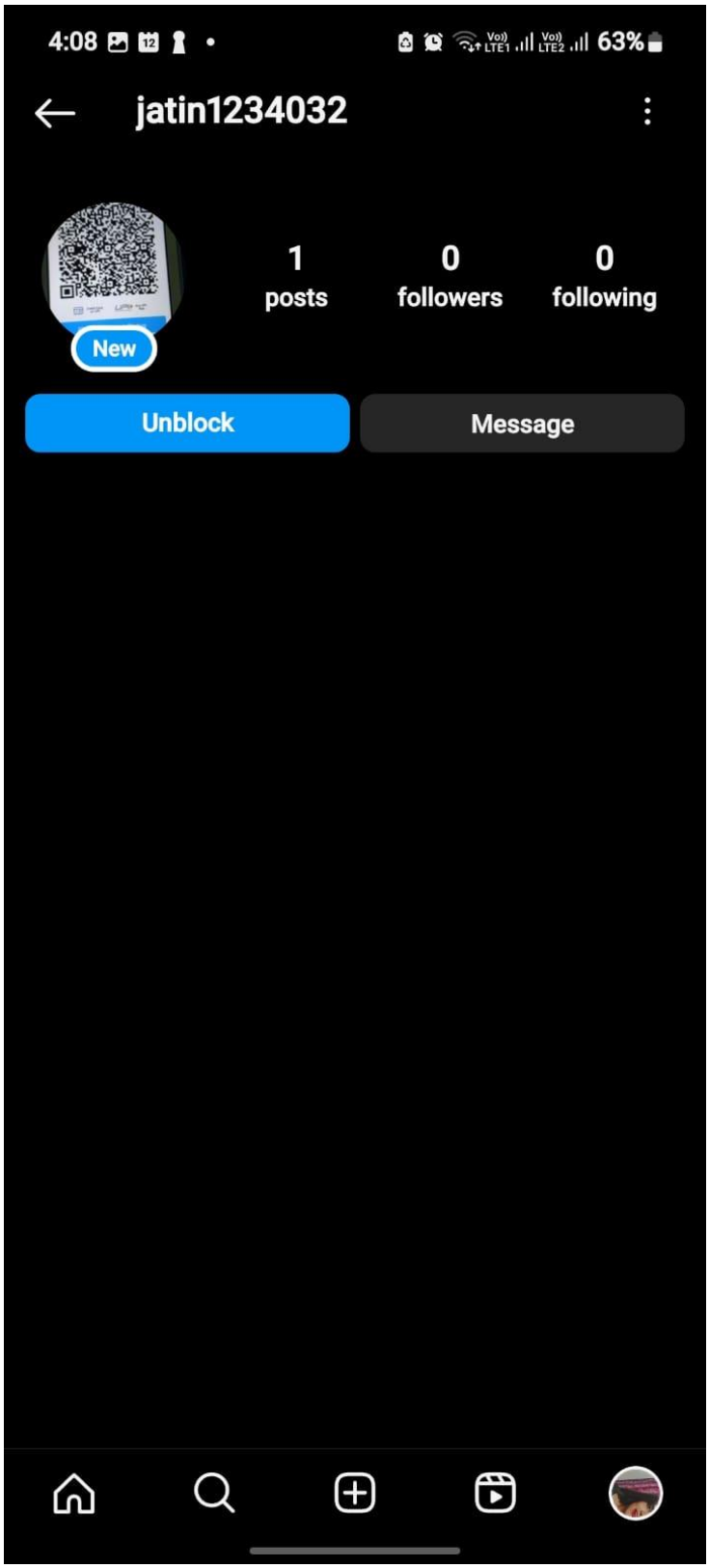
Second account

This account owner sends direct messages to people without any relevance

The message contains explicit content which is 18+ the account uses another accounts post



The third account has zero followers and the display image has a suspicious QR code



QUESTION 2

Outline the objectives and demographics of Interpol's International Child Sexual Exploitation Database.

Child Sexual Abuse Material consumption is considered as the viewing or downloading of any images or videos that show a child engaged in or depicted as being engaged in explicit sexual activity. Contact offenses are those which involve direct contact of a sexual nature with a child. Prevention initiatives exist globally to tackle both.

FROM INHOPE: https://www.inhope.org/

As evidenced in the 2023 Global Threat Assessment of child sexual exploitation and abuse online, the volume of child sexual abuse material detected has increased by 87% from 2019. One concerning trend contributing to the sustained increase in the incidence of child sexual exploitation online is an explosion in Financial Sexual Extortion (FSE), with the number of reports of this crime having increased by 7200% between 2021 and 2022.

FROM https://www.weprotect.org/wp-content/uploads/FSE-Post-Event-Report-PA-Consulting.pdf

On 31 January 2024 CEOs from social media giants Meta (the parent company of Facebook and Instagram), X, Snapchat, Discord, and TikTok faced a US Senate Committee hearing where they were questioned over their platforms' efforts to protect young people from online abuse, including sexual exploitation. As the CEOs testified in front of the US Senate, PA Consulting (PA) held a cross-sector innovation forum co-facilitated with Plexal to explore some of the challenges and opportunities for tackling and preventing the alarming, growing abuse trend of financially motivated sexual extortion. The forum included opening addresses from sector experts Iain Drennan (WeProtect Global Alliance), Simon Bailey (representing Child Rescue Coalition), Ian Critchley QPM (National Police Chiefs' Council), Julie Dawson (Yoti), and Saj Huq (Plexal), who set out the challenges faced in today's digital age, and observations on the current response to FSE. Attendees then took part in facilitated workshops to explore a typical 'victim-perpetrator pathway', and an open group discussion to consider challenges and opportunities for early intervention. The workshop discussions focussed primarily around three areas for intervention, within which specific challenges and opportunities were identified:

1. PREVENT – how to prevent people from engaging in FSE (stopping the problem at source)

2. PROTECT – how to protect individuals from FSE (building high levels of defence and resilience)

3. PURSUE – how to pursue offenders through prosecution and disruption (relentless disruption and targeted action) The group discussion emphasised the shift required from cure to prevention, and how the ecosystem can maximise the use of innovation from small and medium-sized enterprises (SMEs).

Victim Identification and Rescue: The primary function of the ICSE database is to facilitate the identification and rescue of victims of child sexual abuse. This is achieved by enabling law enforcement agencies to meticulously analyze images and videos containing evidence of abuse. By leveraging advanced technology and data analysis techniques, investigators can swiftly identify and locate these vulnerable children. Prompt identification is imperative for ensuring the safety and well-being of the victims, as it enables law enforcement to take immediate action to rescue them from further harm.

Apprehension of Offenders: In addition to aiding in victim identification and rescue, the ICSE database plays a crucial role in apprehending perpetrators of child sexual exploitation. By employing sophisticated image comparison algorithms and facilitating seamless data sharing among law enforcement agencies worldwide, the database enables investigators to establish connections between cases that span international borders. This integrated approach enhances the capacity of law enforcement to identify and track down offenders, regardless of their geographical location. Ultimately, this concerted effort serves to hold perpetrators accountable for their reprehensible actions and bring them to justice.

Security Measures:

Restricted Access: Interpol uses a secure network (I-24/7) to restrict access to authorized investigators from member countries. Only trained personnel can upload and analyze content.

Data Encryption: The content itself is encrypted to ensure its confidentiality and prevent unauthorized access.

How Hackers Exploit the System (Even Without Direct Access):

Targeting Weak Points: Hackers may try to infiltrate other parts of law enforcement networks, hoping to find a vulnerability that grants access to the ICSE database.

Social Engineering: Hackers might use phishing emails or other tactics to trick law enforcement personnel into giving up their login credentials.

Insider Threats: In rare cases, a corrupt official within law enforcement might steal or leak data from the database.

Dark Web Marketplaces: Stolen content or newly created content can find its way to these platforms where it's bought and sold by abusers.

The Importance of International Cooperation:

Sharing Best Practices: Law enforcement agencies worldwide need to collaborate on improving security measures and sharing knowledge about “how to identify and prevent cyberattacks”.

Public Awareness Campaigns: Educating the public on online safety and how to report suspected child sexual abuse online can help reduce the creation and distribution of such content.

Additional Resources:

The National Center for Missing and Exploited Children (NCMEC): https://www.missingkids.org/home

Statistics from the National Centre for Missing and Exploited Children (NCMEC) point to an 87% volume increase in child sexual abuse material since 2019. A significant increase in new tactics by perpetrators, including through FSE, are a large part of this growth.

Children are particularly vulnerable; in a survey of over 1,500 victim-survivors, 46% were children. Financially motivated sexual extortion and coercion is highly traumatic for victims and has led to tens of children taking their own lives.

QUESTION 3

Identify five suspicious SMS/emails you've received, cross-reference the sender phone no. or email against the NCRP Suspect database, and present the findings.

The National Commission for Protection of Child Rights (NCPCR) emphasizes the principle of universality and inviolability of child rights and recognizes the tone of urgency in all the child related policies of the country. For the Commission, protection of all children in the 0 to 18 years age group is of equal importance. Thus, policies define priority actions for the most vulnerable children. This includes focus on regions that are backward or on communities or children under certain circumstances, and so on. The NCPCR believes that while in addressing only some children, there could be a fallacy of exclusion of many vulnerable children who may not fall under the defined or targeted categories. In its translation into practice, the task of reaching out to all children gets compromised and a societal tolerance of violation of child rights continues. This would in fact have an impact on the program for the targeted population as well. Therefore, it considers that it is only in building a larger atmosphere in favour of protection of children's rights, that children who are targeted become visible and gain confidence to access their entitlements.

1 Spam Phone number - 6364798018

Pishing messages on WhatsApp – pishing for jobs

Finding in the website –

Not Found

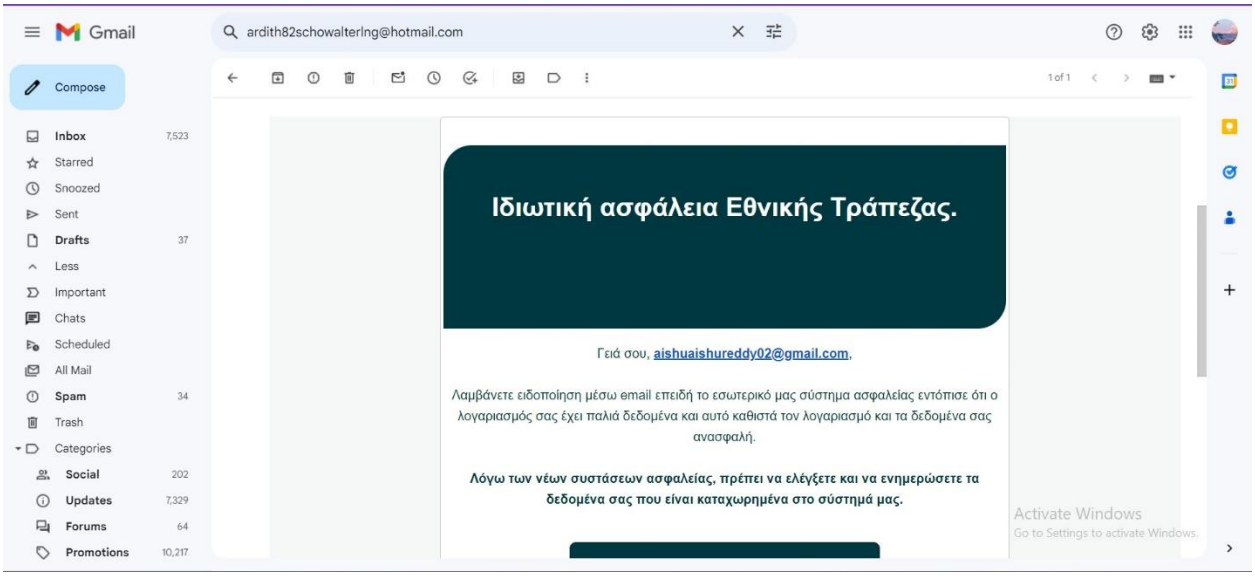
There are no records found with your search !!

2 Spam Email- ardith82schowalterlng@hotmail.com

Mail- in another language from an unknown source

Findings - Not Found

There are no records found with your search !!



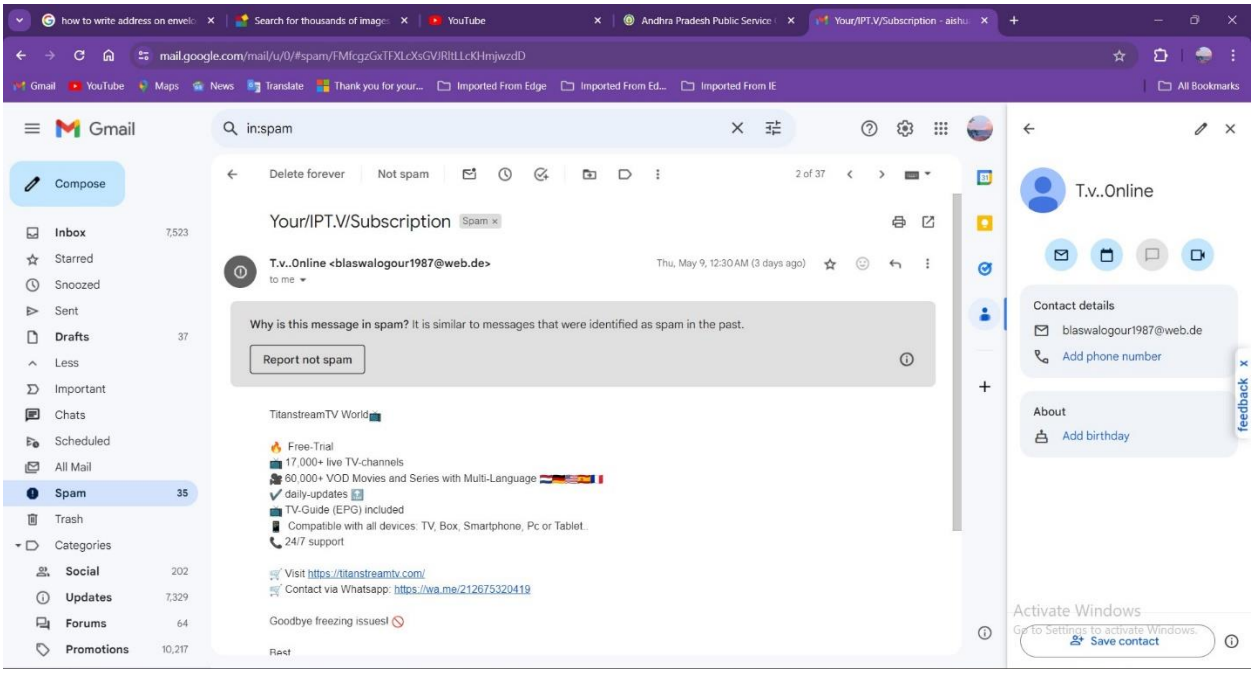
3 Spam Email-

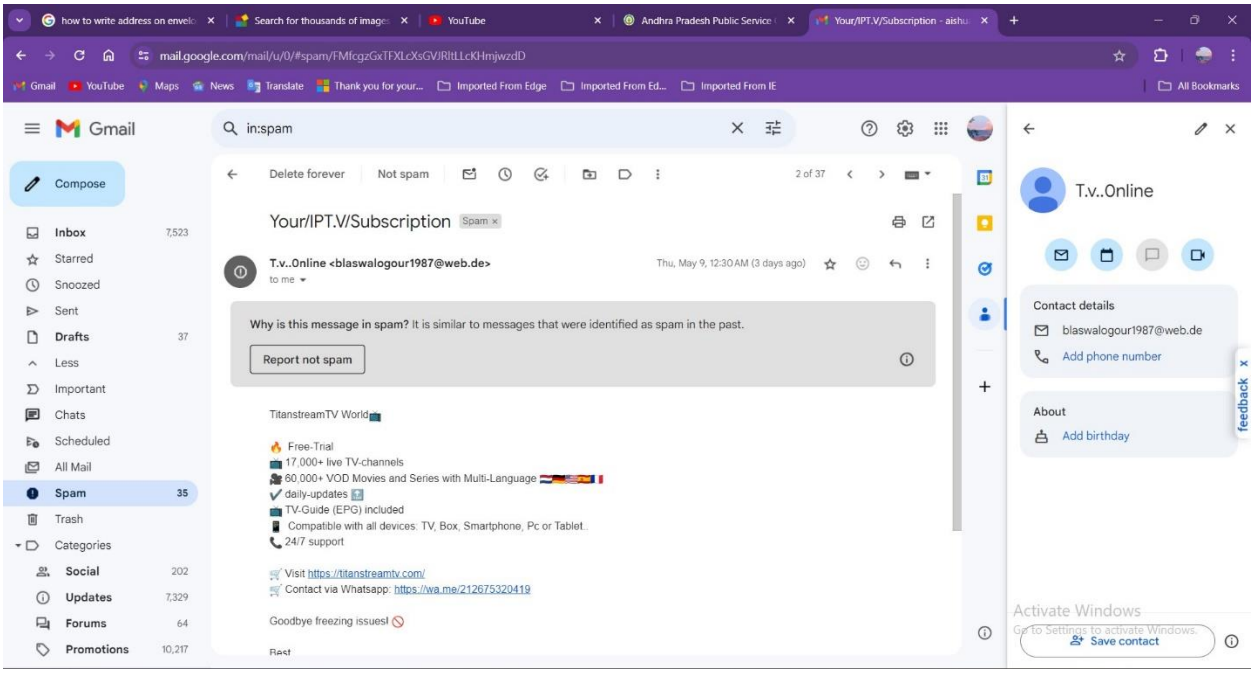
T.v..0nline <blaswalogour1987@web.de>

Mail- spam mail promising some kind of offer to a fake site.

Findings - Not Found

There are no records found with your search !!



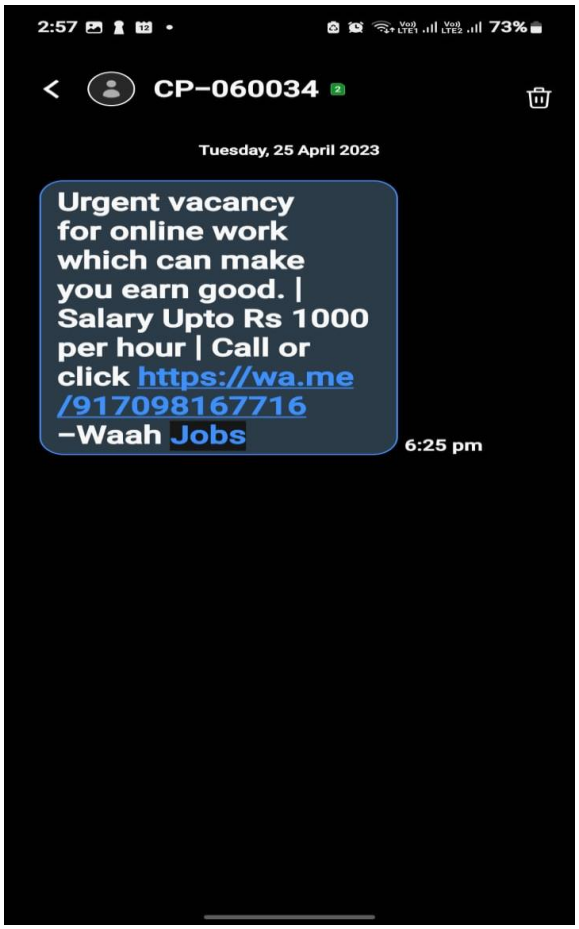


4 SMS – CP-060034

Mail- spam sms promising some kind of job offer link to a fake site.

Findings - Not Found

There are no records found in your search!!



5 Spam mobile Number- 4116906005

Phone calls – repeated phone calls

Findings - Not Found

There are no records found in your search!

Spam mobile Number- 82277607487

Phone calls – FINANCIAL FRAUD

Findings - Not Found

There are no records found in your search!

QUESTION 4

4. What are the guidelines to be followed by children while accessing public systems, as per ISEA portal (www.infosecawareness.in)?

Here are some cybersecurity recommendations for children using public computers, as the ISEA portal (infosecawareness.in) does not provide specific guidelines targeting children:

1. Exercise caution when sharing personal information: Refrain from sharing details like names, addresses, phone numbers, or school names with strangers online.

2. Avoid downloading files from untrusted sources: Public computers may lack robust security measures, so it's best to steer clear of downloading files or programs from websites with questionable reputations.

3. Stay vigilant against phishing attempts: Be wary of emails or messages that request personal information or prompt you to click on suspicious links.

4. Seek help from a trusted adult: If you encounter anything inappropriate or unsettling online, don't hesitate to inform a parent, teacher, or another trusted adult.

5. Use the computer for approved purposes only: Ideally, children should use public computers under adult supervision and limit their browsing activities to approved purposes like school work or educational websites.

6. Always log out properly: Make sure to log out of accounts completely before leaving a public computer to prevent unauthorized access.

7. Consider using incognito or privacy mode: Utilize the incognito or privacy mode feature in your browser to minimize the risk of personal information being stored on the computer. However, note that incognito mode does not guarantee complete anonymity.

QUESTION 5

5. Go through CIS Google Android Benchmark document and provide a brief overview of the privacy and browser configuration settings suggested.

CIS Google Android Benchmark document:

Privacy Settings:

- **App Permissions:** Be cautious when granting permissions to apps. The benchmark recommends reviewing permissions for each app and only allowing access to features absolutely necessary for the app's functionality. For instance, a flashlight app doesn't need access to your location. Consider using tools that allow you to audit and manage app permissions more easily.
- **Lock Screen:** A strong lock screen is your first line of defense. The CIS Benchmark recommends using a PIN with at least six digits, a complex pattern, or fingerprint unlock. Avoid using easily guessable codes like birthdays or simple patterns. Fingerprint unlock can be convenient, but be aware of potential vulnerabilities (e.g., someone using your sleeping finger to unlock).
- **Find My Device:** This built-in Google feature is crucial if your device is lost or stolen. Enabling it allows you to locate your device on a map, lock it remotely to prevent unauthorized access, or even erase all data on the device as a last resort.
- **Location Services:** Many apps request location data. The benchmark recommends disabling location services when not in use. This reduces the amount of data collected and helps preserve battery life. You can manage location permissions on an app-by-app basis.
- **Advertising ID:** This unique identifier allows advertisers to track your activity across different apps and websites. The CIS Benchmark suggests opting out of personalized

advertising based on this ID. This will limit the ability of advertisers to target you with specific ads, but may not entirely prevent them from tracking your activity.

- **Data Sharing:** Many apps and services collect data about your activity. The benchmark recommends reviewing data sharing settings for each app and service you use. Disable data collection that you find unnecessary. Be wary of pre-checked boxes that consent to data sharing during app installation.

Browser Configuration Settings (Chrome is assumed):

- **JavaScript:** JavaScript is a programming language that enables websites to offer interactive features and dynamic content. While disabling JavaScript entirely can enhance security, it may also break some websites or prevent them from functioning properly. The CIS Benchmark recommends keeping JavaScript enabled with caution. Be wary of visiting untrusted websites or clicking on suspicious links, as these could contain malicious JavaScript code.
- **Pop-ups and redirects:** These can be disruptive and even lead to malicious websites. The benchmark recommends enabling the blocker for pop-ups and redirects in your browser settings. This helps protect you from intrusive advertising and potentially harmful content.
- **Cookies:** Cookies are small files stored on your device by websites. They can be used to personalize your browsing experience or track your activity across different websites. The CIS Benchmark suggests considering options like blocking third-party cookies or clearing cookies regularly. Third-party cookies are placed by domains other than the one you're visiting, and they can be used for tracking purposes. Clearing cookies regularly helps protect your privacy by removing any tracking data stored on your device.
- **Safe Browsing:** This Google security feature helps protect against malware and phishing attacks. The CIS Benchmark recommends enabling Safe Browsing in your browser settings. When enabled, Safe Browsing warns you before visiting websites suspected of containing malware or phishing scams.
- **Incognito Mode:** Incognito mode allows you to browse the web privately without your browsing history being saved on the device. The CIS Benchmark acknowledges that Incognito mode offers some privacy benefits, but it's important to understand it doesn't guarantee complete anonymity. Your browsing activity might still be tracked by your internet service provider (ISP) or the websites you visit. Incognito mode also doesn't prevent websites from tracking you using cookies placed during previous browsing sessions.

It covers a wide range of security recommendations for Android devices, including device security, network security, application security, and more. Consulting the latest version of the CIS Benchmark is recommended for the most up-to-date security best practices for your Android device.