E-COMMERCE & DIGITAL SECURITY
Assignment-14
N Ravinder Reddy
Roll No: 2406CYS106

Assignment Questions:

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

Ans:

1. Profile Picture:
   - The profile picture might be too perfect or appear to be a stock photo.
   - Reverse image search could reveal if the picture is stolen from elsewhere.
2. Limited Information:
   - The profile might have very little information about the person, such as missing personal details, work or education history, or interests.
   - Lack of recent posts or activity on the platform.
3. Inconsistent Details:
   - Information provided might not match up. For example, the location mentioned in the profile might not align with the language used in posts or comments.
   - Employment or education history might seem implausible or inconsistent.
4. Unusual Friend Requests or Interactions:
   - Sending friend requests to people who have no mutual connections or who seem to have no common interests.
   - Unusual or overly friendly messages to strangers, often with links or requests for personal information.
5. Grammar and Language:
   - Poor grammar, spelling mistakes, or the use of unusual phrases could indicate that the profile is operated by someone not fluent in the language they claim to speak.
6. Too Good to Be True Offers:
   - Promises of easy money, fantastic job opportunities, or offers that seem too good to be true.
   - Requests for money or financial information.
7. Lack of Engagement:
   - Little to no interaction with other users' posts or comments, especially if the profile has been active for a while.
   - A disproportionate number of followers compared to the level of engagement on posts.
8. Multiple Profiles with Similar Content:

    - If you come across several profiles with similar content, especially if they're using the same photos or posting identical messages, it could indicate a network of fake profiles.

9. Privacy Settings:
    - Profiles with extremely restrictive privacy settings might be trying to hide something or avoid being reported.
10. Check for Verification:
    - If the platform offers verification badges for public figures or businesses, the absence of such a badge on a profile claiming to be a public figure or business could be a red flag.

Q. 2. Outline the objectives and demographics of Interpol's International Child Sexual Exploitation Database.

Ans:

Victim identification involves the detailed analysis of images and videos to locate and rescue child sexual abuse victims.

Online child sexual abuse is one of the rare crime areas where police officers start with the evidence and work their way back to the crime scene.

The images can either be discovered through:

- Child exploitation investigations;
- Proactive monitoring of online platforms;
- Forensic analysis of seized mobiles, laptops, digital storage units, etc.

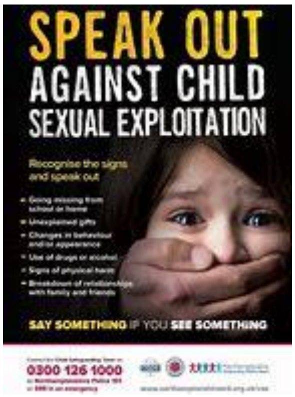
Once images are found, victim identification specialists take over. They go through the images with a fine-toothed comb with the objective of removing the child from harm and arresting the abuser.

Evidence of a serious crime

Contrary to common beliefs about sexual abuse, the abuser is most often a person known to the child, such as a family member, neighbour or childcare professional. The vast majority of child sexual abuse cases are not documented, mostly taking place behind closed doors in private settings.

When the abuse is recorded or photographed, however, what is really being documented is evidence of a serious crime. Abusers often use the images for future sexual gratification, or to be traded and shared with other abusers.

Photos and videos of child sexual abuse found on the web are not virtual; they are evidence of a real crime involving real children and real suffering.


SPEAK OUT
AGAINST CHILD
SEXUAL EXPLOITATION
Recognise the signs and speak out
Going missing from school or home
Unexplained gifts
Changes in behaviour and/or appearance
Use of drugs or alcohol
Signs of physical harm
Breakdown of relationships with family and friends
SAY SOMETHING IF YOU SEE SOMETHING
0300 126 1000

Preventing users from accessing websites that show child sexual abuse material is an important part of the fight against this crime. By blocking access, it stops re-victimization of the children abused, and has a pedagogic effect on users who may be about to commit a serious offence by viewing or downloading illegal material.

To block access to Internet domains that disseminate child sexual abuse material, police can give Internet Service Providers a list of domains, or web addresses, to block in their networks. When users attempt to view the page, they may be redirected to a 'stop page' containing information on the reason for the redirection, links to legislation, where to complain, etc.
Preventing access to child sexual abuse material is used as a complement to investigations, arrests and undercover operations.

It is important to note that no criminal cases are generated as a result of anyone being redirected from a domain containing child sexual abuse material.

Access blocking should be used as part of a holistic approach to combating child sexual exploitation.

The INTERPOL 'Worst Of' List

We maintain and provide a list of domains that disseminate the most severe child abuse material worldwide. It is available to national police through our National Central Bureaus.

The "Worst of" list contains domains that distribute child sexual abuse material and which have been verified by at least two different countries/agencies. The domains entered into in the "Worst of" list contain images and movies which fit the following criteria:

- The children are "real";
- The ages of the children depicted are (or appear to be) younger than 13 years;
- The abuse is considered severe.

Baseline

The Baseline system allows partners in the public and private sectors to recognize, report and remove known child sexual abuse material from their networks.

They can do this by checking images and videos against INTERPOL's Baseline list, which contains the 'digital signatures' of some of the worst child abuse images and videos.

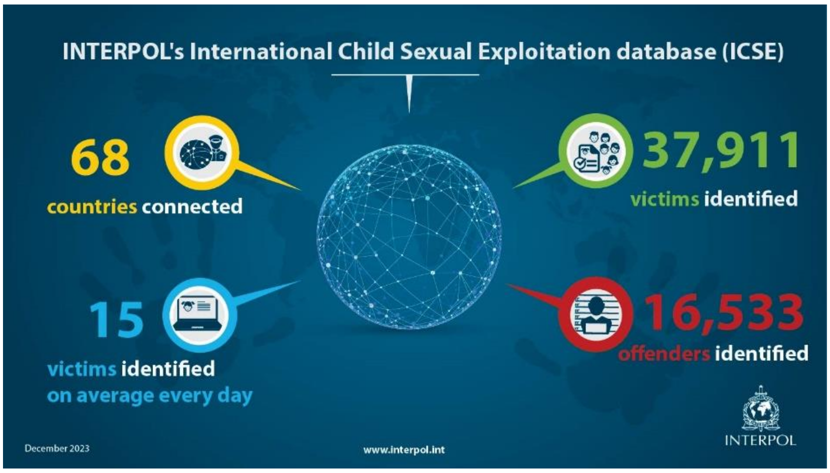
If a signature matches, network operators alert the police and remove the material, thereby limiting its circulation.

A user-friendly booklet on the manifestations, legal frameworks and technical terms and tools related to online child sexual exploitation

Baseline criteria

To be included in the Baseline list, child abuse images and videos must be recognized as such by our specialist network of investigators, and meet specific criteria in terms of the severity of the image content, for example those believed to feature children aged 13 and under.

The strict criteria ensure that the Baseline list refers only to images and videos which would be considered as illegal in any country.



Q. 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.

Ans:

The National Cybercrime Reporting Portal (NCRP) under I4C was launched on 30.08.2019. The older version of the Cybercrime reporting portal under CCPWC scheme enabled the filing of Cybercrime complaints pertaining to Child Pornography (CP)/ Rape or Gang Rape (RGR) – Sexually Abusive Content only. The revamped version of the portal allows reporting of all types of Cybercrime. The National Cybercrime Reporting Portal (NCRP) was dedicated to the nation by the Hon'ble Home Minister of India on 20th January 2020.

Recognizing phishing email scams

What are some general clues that an email isn't legitimate but is instead a phishing email?

Grammatical errors

Many phishing emails are filled with grammatical errors, odd capitalization, and misspellings. The emails might also contain odd phrases or sentences that sound a bit off. Read your email aloud. If something doesn't sound right, or professional, be suspicious. It could be a phishing attack.

Low-resolution logo

Phishers will often cut and paste the logos of government agencies, banks and credit card providers in their phishing emails. If the logo is of low quality — it's fuzzy, indistinct, or tiny — this is a sign that the person contacting you doesn't really work for that company.

Odd URL

One of the easiest ways to tell if an email is a scam? Hover over whatever link the message is asking you to click. This will show the link's URL. Often, you'll see that the URL doesn't belong to whatever company is supposedly sending you the message.

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

Ans:

Do you use the Internet?

If Yes, then read this entire content carefully. The Internet is considered as the greatest platform and technology in this century and has become an integral part of our daily lives. It helps us as a learning and communication tool and offers us a wide range of opportunities. It is an invaluable source of knowledge and encourages creativity and imagination.

Do you follow ethics?

Internet ethics implies our behaviour while using it. We should be aware that we should always be honest, and respect the rights and property of others on the internet.

Step 1: Do you share about internet access with your family?

Sharing about internet activity with your family members is the first step to being safe on the internet. Your parents always love you and look after your safety so that they will be with you in all difficult periods.

So share each and everything that you do and face on the internet.

Step 2: Do you use a family computer?

If Yes, then follow some family rules and guidelines as the family members use internet for different purposes like banking, shopping, sometimes even doing office work, etc.

Most online games or videos may require credit/debit card details to play, watch videos etc. So, when using the family computer you may share such sensitive data to known/unknown people without the knowledge of your family members which can create financial losses to the family.

Also there are chances that when using a family computer you may even share important office files or documents to your online friends which can create a career threat to your family members. Therefore always follow some rules and guidelines of family for accessing the internet.

Step 3: Do you love to see videos?

Watching videos on the internet is always fun and pleasure, but at the same time there are risks like malicious links could take you to inappropriate or illegal content. If you encounter any such activity, intimate it to your family members.

Remind family members that people meet online may be strangers.

Step 4: Do you follow any celebrity over the internet?

Like any other child, you may follow and chat online about your favourite celebrities in all kinds of fields. There are lots of celebrity sites, but only the ones operated by the celebrities themselves or entertainment news publishers are appropriate to follow.

You need to be extra careful of fan sites that turn up in search results but aren't run by celebrities and the people who cover them. It's not always easy to tell, but at least they'll lower down in the search results.

Step 5: Do you believe everything on the internet is true?

It's common for you to think everything on the internet is true. But, the content on the internet is a collection of lot of people's views as they can write and post without any guidance and control. The Internet contains a wealth of valuable information, but at the same time, it is a great medium for disseminating falsehoods and inaccuracies.

Though the information on the internet is very valuable, but you should realize that there are still biased views and information to market their products and agenda. So, you need to be careful and confirm the same by going into various sources of internet.

Step 6: Do you love to play games?

Yes, Children love to play games. We always love to play online games and extend our arms further with unknown members on the internet.

To play games on internet, some websites ask credit/debit card details though they tell it is free. Be careful while playing free online games as sometimes automated charges can apply which can be burden to the family members.

Also, the details and identification passed on the website can be accessed by others and identification theft can occur.

Step 7 : Do you love to be social?

Yes, Children love to be social and make new friends. The Internet helps you to keep in touch with old friends and extend your arms to new members. Though it is a great opportunity to extend friend circles, never share passwords even with the closest buddies because bullying is common as some kids or hackers try to post embarrassing messages by using shared passwords or post links to malicious sites.

At the same time, you should also know that there are social reasons why kids are hacked. So always log out of accounts when you are finished using computers shared with other people especially those used in public, such as at school or public libraries.

Step 8: Do you keep your identification?

For hackers or attackers, Children's identification is more valuable. Criminals get most of the information about children such as name, address, class, and school name to target them. The collected information may be useful for guessing the passwords of children and their parents as in general passwords of family members are related to family names.

Further, they may use the same information to make friendship with you online and try to get to know about your family and consequently, they may apply for credit cards in your family members' name.

It is suggested that children should not share any information related to sensitive and financial aspects in social networks and maintain privacy with known and unknown members.

Protecting Oneself/Child from becoming a victim of cyber grooming:

1. One must be educated as to not accept friend request from unknown people on social media platforms. Cyber groomer can even create a fake account to befriend victims.

2. One must be educated as to not share their personal information like date of birth, address, phone number and school name on social media or other online platforms. One can go to the privacy settings on their social media platforms as to select who can access their posts online. One must try to restrict access of their profile to their friends only.

3. One must always be cautious when the person one is chatting to give too many compliments regarding their appearance in just a short span of your acquaintance.

4. One must Avoid talking to people who ask questions related to one’s physical or sexual experiences . One can either ask the person to stop asking such questions when it makes one feel uncomfortable. If they continue to do the same, one must immediately inform parents/elders/teachers etc.

5. One must Educate people to not talk to people who asks to share their sexually explicit photographs or videos.

6. Educate children to never turn on webcam for any unknown person.

7. Educate a child to talk to their elders or parents, if their chat partner suggests to keep their conversation with them secret.

8. Educate a child as to not go and meet any person whom they met online alone. One must always take a friend or any elder person while going to meet someone whom one met online.

9. One must be educated/made aware to never install unwanted software and apps like dating app, online games etc from unknown sources. One should be very careful while chatting in the chat rooms. One should never share personal details in the chat room and limit their identity.

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

Ans:

This document, Security Configuration Benchmark for Google Android, provides prescriptive guidance for establishing a secure configuration posture for the Google Android OS. This guide was tested against the Android Version 9.0.0. This benchmark covers Android 9.0.x and all hardware devices on which this OS is supported. In determining recommendations, the current guidance treats all Android mobile device platforms as having the same use cases and risk/threat scenarios. In all but a very few cases, configuration steps, default settings, and benchmark recommended settings are identical regardless of hardware platform. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

This document is intended for system and application administrators, security specialists, auditors, help desk, end users, and platform deployment personnel who plan to use, develop, deploy, assess, or secure solutions that use Android 9.0.x

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal. Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.