Threats Encounters Online- For Adults

1. Fake Identities

In India, fake identities are a huge problem. In 2019, Facebook reportedly removed 5.4 billion fake accounts of Indian users.

1. A fake profile is the representation of a person or an organisation that does not exist on social media
2. They use names, photos and false information that make them look real but some extra research can make the fakeness of these profiles evident
3. Fake profiles are one of the most common ways of attack by a hacker
4. They're made to gain sensitive information such as account passwords, private pictures or videos, credit card or debit card details
5. The intent is to lure you into trusting these online users into giving them sensitive information.

How do you check for fake profiles?

Check the profile thoroughly for the following:

1. The profile has very few pictures or no new pictures
2. It was created recently
3. The information linked with their profile and how selective it is.
4. Little or no contacts in common, when the profile who is trying to add you has no common friends or interests, the reason can be malicious.
5. When a profile adds you but doesn't bother to actually engage is one of the major signs of a fake profile.

What is safe?

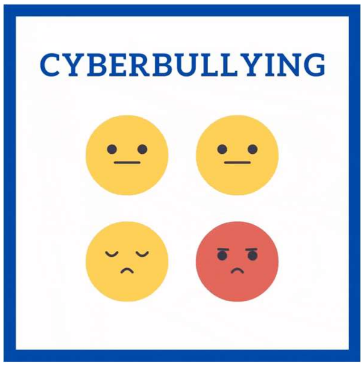
1. We have to understand that whatever we share on the internet stays on the internet. The best way to tackle is to understand that everything you share is susceptible to access and so we have to share information in a smart and responsible way only.

QUICK RESPONSE

- Use strong QWERTY passwords that include capital letters, letters or symbols
- Turn on two-factor authentication on all accounts
- Be wary of accepting friend requests from strangers
- Report these accounts on the social media platforms
- Never share any account information, ID card details, bank information or any other sensitive financial information on social media websites
- Familiarise yourself with the website functionality before you sign up

- Take out some time to read security policies and tools
- Be extra careful before clicking on links that are shared with you, even if they are sent by friends.

2. Cyber bullying



While people all over the world have been following the trend of face-to-face bullying, the internet and digital devices provided an outlet for bullies to do it anonymously. The first time India tackled with Cyber bullying was with the Vishaka vs. the State of Rajasthan, this led our country to become aware of online sexual harassment and cyber stalking.

What is Cyberbullying?

- Bullying that takes place over digital devices like cellphones, tablets, laptops or gaming devices
- It can occur in chat rooms, gaming rooms, social media platforms, texting, forums or wherever content can be shared
- Cyberbullying includes sending, posting or sharing negative, harmful, false or mean content about someone with the intention of hurting this person, humiliating them or excluding them from their online network
- Bullies online do not ask for permission and misuse their presence in your network to spread malicious rumours or stories about you
- Issuing online threats provoking self-harm or violence in real life.

QUICK RESPONSE

1. Please reach out and talk to someone. It can be a parent, a trustworthy friend, a teacher or an online civil society, but speak up because it's your right.
2. Ensure that you do not accept friend requests from strangers, especially if they keep messaging you even after you reject their requests
3. Be empowered by reading security settings and tools of all social media platforms you are a part of
4. Understand it's easier to be a bully online and if you encounter one, you must REPORT immediately
5. Report the profile under the Cyberbullying tag. If you encounter a cyberbully or someone you know is being bullied online, it's your responsibility as an online citizen to report this harmful personality to the platform
6. You can file a complaint on complaint-mwcd@gov.in
7. These are the Anti-Bullying Cyber Laws in India:
8. Sec.66A – Sending offensive messages through communication service, etc.
9. Sec.66C – Identity Theft
10. Sec.66D – Cheating by personation by using the computer resource

11. Sec.66E – Violation of privacy
12. Sec.67B – Punishment for publishing or transmitting of material depicting children in any sexually explicit act, etc. in electronic form
13. Sec.72 – Breach of confidentiality and privacy
14. Sec.503 Indian Penal Code (IPC) – Sending threatening messages through email
15. Sec.509 IPC – Word, gesture or act intended to insult the modesty of a woman
16. Sec.499 IPC – Sending defamatory messages through email
17. Sec .500 IPC – Email Abuse

3. Fake News

Fake news refers to false information or propaganda published under the guise of being authentic and spread through the medium of news and/or social media, leading to even Chinese whispers through word-of-mouth.

Fake news can be categorized as –

1. **Disinformation**: False information deliberately and covertly spread to mislead and influence public opinion or obscure the truth. The information is intentionally presented by the manipulation of facts to tweak the narrative, i.e., used as a tool of propaganda. Example: the messages we have received about Covid-19 prevention and cure, are meant to be misleading in nature
2. **Misinformation**: False information that is inadvertently spread and published regardless of the intent to fabricate facts and/or mislead. Example: the messages saying Covid-19 cannot survive in tropical countries are misinformed.
3. **Mal-information**: When genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere. Example: saying drinking bleach, using blow dryers on the face, or drinking turmeric milk can cure Covid-19 have led people into panic and harm themselves physically by drinking bleach

QUICK RESPONSE

- Be a critical thinker and understand what news you're consuming, sharing or spreading
- Always check the source to be from relatable news media stations, organisations or government platforms
- Be critical of too positive or too negative headlines because they can be exaggerated for clickbait
- Check the author for credible source

- Check the date of the publication
- Understand if the piece of information is news or being shared as a joke
- Do a quick google search and see if there are other articles supporting this news
- Always check the images to understand if the article is using false images to spread a particular agenda
- Check the URLs. Fake news is often manufactured to look real and that's why checking URLs(.com, .org, .edu) is very important
- Break the cycle of fake news spread and be the empowered online user who challenges fake news

4. Doxing

What is Doxing?

- Doxing refers to researching and broadcasting private or identifying information about someone online, usually having malicious intent.
- This information is gathered via social media websites or hacking user accounts.
- Doxing is an intentional online attack with the intent to shame, humiliate or harass a human being
- In India, doxing is a popular form of taking revenge or threatening someone
- Doxing can also turn malicious and manifest itself into stalking or threat of violence

QUICK RESPONSE

1. Use strong QWERTY passwords that include capital letters, letters or symbols
2. Turn on two-factor authentication on all accounts
3. Do not over share your private information on social media platforms
4. Review your privacy settings and ensure that you make them private so the consumers are people you select
5. Do not provide personal information such as ID card numbers, bank account information if asked
6. Be wary of friend requests from strangers
7. Take some time and review the profiles that you accept to ensure they're not fake
8. Be alert of phishing emails
9. Report the doxing attack to the platform in which your personal information has been shared

5. Phishing

What is Phishing?

- It is designed to convince the victim to divulge in their financial information like that of – bank accounts, credit cards, ATM Pin, etc
- These are individuals posing as a bank official, telephone operator, official institution member to trick you into identity theft or financial loss
- Phishing emails often have too good to be true lottery offers
- Phone calls from unusual numbers can also be triggers to identify phishing threat
- Supposed calls from banks demanding your OTP or card details
- When you get messages with hyperlinks professing miracle deals or unusual bank activity
- Paytm reportedly filed a FIR with Noida police 's cyber wing against 3,500 such phone numbers
- The problem of phishing is so rampant in India that Netflix got inspired to make a show on it

QUICK RESPONSE

- To protect against spam mail, spam filters can be placed
- Do not give out your email ID on unnecessary platforms
- Check your chrome settings or other browser settings to place ad blockers and prevent fraudulent websites from opening
- Change your passwords on a regular basis and always use QWERTY passwords with uppercase characters, numbers and symbols
- Do not ever share your bank details on the phone or online
- Do not click on random links that profess too good to be true deals

6. Scamming

As we all know, internet scams are widespread and really dangerous because they can range from identity theft, financial threat and leak of private information.

What is Scamming?

- Online fraud that is facilitated by cybercriminals on the internet

- This can take place via SMS, email, social media, fake bank or tech support phone calls, or even pop up links for ads
- Internet thieves trick you into sharing your private bank details or signing up for a trusted website
- The scamming links are hidden in pop up ads of jackpot wins, earning large amounts through simple activities or pornographic photos
- When you receive a call from alleged bank support staff that ask you for your ATM pins or OTP numbers

1. Do not share your private bank details on any social media platforms
2. Do not share your OTP on the phone with anyone
3. Be wary of getting official calls from unusual numbers
4. Stay updated on security reforms and read up on actions being taken against scammers
5. Set up multilayered security features
6. Buy from authentic and legitimate websites or sources only
7. Don't respond to spam messages and consider changing browser security to filter spam
8. Don't trust unsolicited phone calls or emails. Instead, ask for proof of identity and research the company

References

- Robinson, L., Segal J., (November 2019), "Bullying and Cyberbullying
- Bisson, David (November, 2019), "5 Social Engineering Attacks to Watch Out For"
- Fruhlinger, Josh,What is phishing? How this cyber attack works and how to prevent it"
- Coble, Sarah, (January 2020), "Over Half of the Organizations Were Successfully phished in 2019"
- "Doxxing: What Is It and How to Avoid Being a Victim [Infographic]"HTML Resource, (October 2019)
- Yonder Resource, (March 2019), "Misinformation vs. Disinformation: What's the Difference?"
- Wardle, C., Derakhshan, H, (2017, September 27), "Information Disorder: Toward an interdisciplinary framework for research and policy making."
- Lilleker, Darren, (January 2020), "You're probably more susceptible to misinformation than you think"
- Morris, K., Yeoman, F, (January 2020), "Why media education in schools needs to be about much more than 'fake news"