A BOOK BY

PRAJASETU FOUNDATION

CYBER SAVVY

SPREADING AWARENESS ABOUT CYBER CRIME PREVENTION AGAINST WOMEN AND CHILDREN

Preface

As we navigate the ever-evolving landscape of the digital age, the importance of cyber safety has become paramount, especially for vulnerable groups like children and women. In our interconnected world, where technology permeates every aspect of our lives, understanding the risks and learning how to protect oneself online has become a necessity.

It is with great pleasure and a sense of responsibility that the Prajasetu Foundation contributes to the noble initiative named "Capital Connect," spearheaded by the Anti-corruption and Vigilance Council of India, in collaboration with the National Cybersecurity Research Council and Tamil Nadu Police. Through this initiative, we aim to raise awareness about cyber safety for women and children, equipping them with the knowledge and tools necessary to navigate the digital realm safely and confidently.

This book, titled "CyberSavvy," is a testament to our commitment to this cause. Written in lucid language and targeted towards children, women, and citizens alike, CyberSavvy serves as a comprehensive guide to understanding and mitigating cyber risks. Through practical tips, real-life examples, and engaging content, we strive to empower our readers to become vigilant and responsible digital citizens.

We believe that collaboration is key to addressing the challenges posed by cyber threats. By joining forces with esteemed organizations and stakeholders, we hope to create a safer online environment for all. We extend our heartfelt gratitude to the Anti-corruption and Vigilance Council of India, the National Cybersecurity Research Council, and the Tamil Nadu Police for their leadership and support in this endeavour.

Together, let us embark on this journey towards cyber safety, ensuring that our children, women, and citizens are equipped with the knowledge and resilience needed to thrive in the digital age.

Warm Regards,
Krithika Ramasethu.
Founder, Managing Director
Prajasetu Foundation

Title: CyberSavvy

Index

Introduction

Cyber safety means staying safe while using computers, smartphones, and the internet. Just like we learn to be careful in the real world to avoid dangers, we also need to be careful online.

Imagine the internet as a big city with lots of streets and places to visit. Some places are safe, like parks where you can play, and some places are risky, like dark streets where strangers might lurk.

Knowing how to navigate this online city safely is what cyber safety is all about.

Why Cyber Safety matters for Women and Children ?

Children and women sometimes face unique risks online. Bad people can use the internet to trick or hurt them. For children, this might mean encountering strangers who pretend to be friendly but have bad intentions.

For women, it could involve facing harassment or abuse through social media or online chats. Just like in the real world, we want everyone to feel safe and secure online.

That's why understanding cyber safety is essential for children and women. By learning how to protect ourselves and each other, we can make the internet a better place for everyone.

Now this is why cyber safety matters for women and children the most !!!

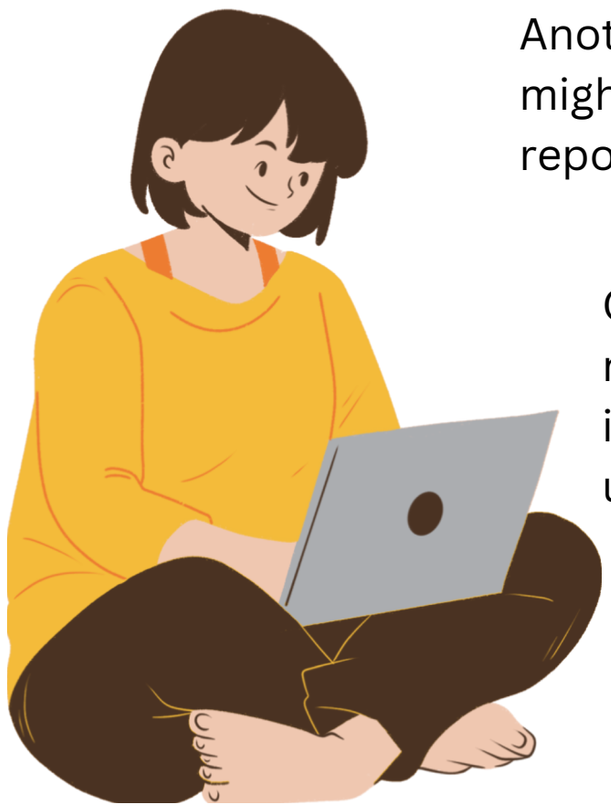
The Digital Landscape

The internet is like a giant library filled with information, games, videos, and more. You can use it to learn, play, and connect with friends. But just like in a big city, there are good and bad places to visit online. Some websites are safe, like educational sites or ones where you can watch funny videos.

But there are also places that might not be safe for kids or women. These could be websites with inappropriate content or places where people might try to trick you.

Common Platforms where Cyber Safety is Compremised

There are some places on the internet where you need to be extra careful. These include social media sites that are widely used, where people might say mean things or try to talk to you in a way that makes you uncomfortable.



Another risky place is online games. While they can be a lot of fun, some people might use them to bully or harass others. It's important to know how to block and report someone if they're being mean to you.

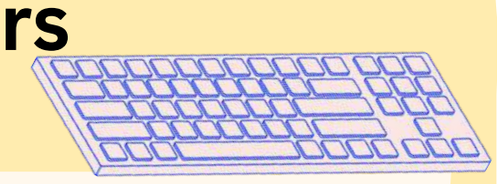
Chat rooms and messaging apps can also be tricky. Sometimes, strangers might try to talk to you and ask personal questions. Remember, it's okay to ignore them or tell a grownup if someone online makes you feel scared or uncomfortable.

By being aware of these places and knowing how to stay safe, you can enjoy all the good things the internet has to offer without worrying about the bad student.

Methods of Cyber Attack

Cyber attackers use various methods to target individuals and organizations, aiming to steal sensitive information, disrupt services, or cause harm. Here are some common methods of cyber attacks:

Keyloggers



Keyloggers are malicious software programs installed on a device to record keystrokes and other information entered by the user. This data is then sent to the attacker, allowing them to capture passwords, credit card numbers, and other con dential information.

SMS Spoofing

SMS spoofing involves sending text messages that appear to come from a different sender than the actual one. Attackers use this technique to trick recipients into revealing sensitive information or clicking on malicious links.

Vishing

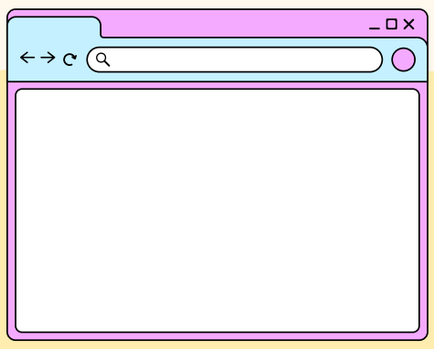
Vishing, or voice phishing, is a type of social engineering attack where the attacker calls the victim, pretending to be someone else, such as a bank representative or a trusted company employee. The goal is to deceive the victim into providing personal or financial information over the phone.

Phishing

Phishing attacks involve sending fake communications, such as emails or text messages, to trick recipients into revealing their personal information or downloading malware onto their devices. These messages often appear to be from legitimate sources, such as banks or government agencies.

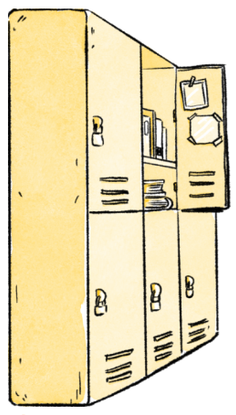
URL Poisoning

URL poisoning is a technique used to redirect users to malicious websites. Attackers create fake links that appear to lead to legitimate websites but actually direct users to harmful pages designed to steal their information or install malware on their devices.



Social Engineering

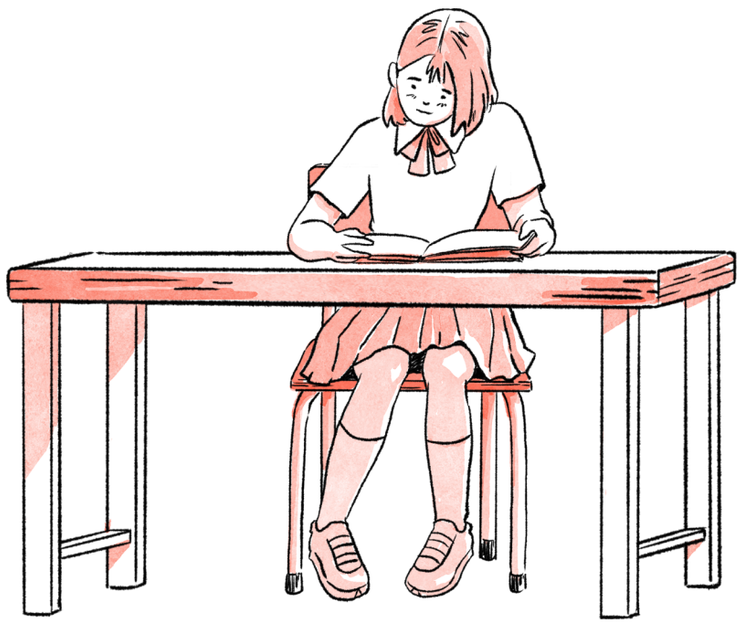
Social engineering attacks manipulate individuals into divulging sensitive information or performing certain actions through psychological manipulation. Attackers may impersonate trusted entities, exploit human emotions, or create false sense of urgency to deceive their targets.



Malware

Malware, short for malicious software, encompasses various types of harmful software, including viruses, spyware, and ransomware. Malware can infect devices through infected email attachments, malicious websites, or software vulnerabilities, allowing attackers to steal data, spy on users, or extort money.

Understanding these methods of cyber attacks is essential for protecting oneself against potential threats. By staying informed and adopting cybersecurity best practices, individuals can reduce their vulnerability to cyber threats and safeguard their digital assets.



Cyber Risk for Children

In today's digital age, children are increasingly exposed to various online risks that can jeopardise their safety and wellbeing Understanding these risks and taking appropriate precautions is essential for ensuring a positive and secure online experience for children. Here are two signi cant cyber risks for children and how to address them:

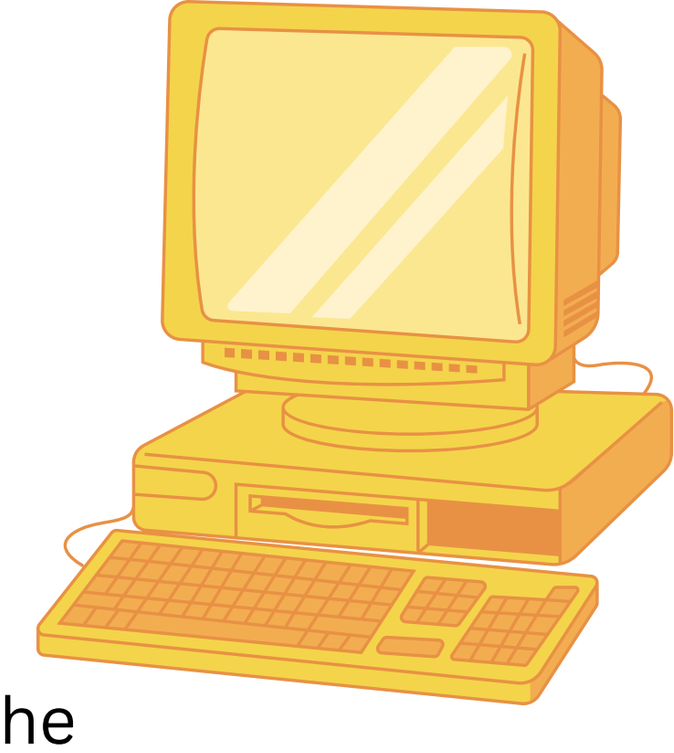
Online Predators: Who They Are? and How to Spot Them?

Online predators are individuals who use the internet to groom, manipulate, and exploit children for their own evil purposes. These predators often disguise themself as friendly and trustworthy individuals to gain the trust of children. They may engage in online chats, social media interactions, or gaming environments to establish relationships with their victims.

To protect children from online predators, it's crucial to educate them about the signs of potential danger and establish clear guidelines for online interactions. Parents and caregivers should encourage open communication with children and promote an environment where they feel comfortable discussing their online activities.

To protect children from online predators, it's crucial to educate them about the signs of potential danger and establish clear guidelines for online interactions. Parents and caregivers should encourage open communication with children and promote an environment where they feel comfortable discussing their online activities.

Protecting Personal Information Online



Children must understand the importance of safeguarding their personal information when using the internet. Revealing too much personal information online can make children vulnerable to various risks, including identity theft, cyberbullying, and harassment.

Some key signs that may indicate the presence of an online predator include:

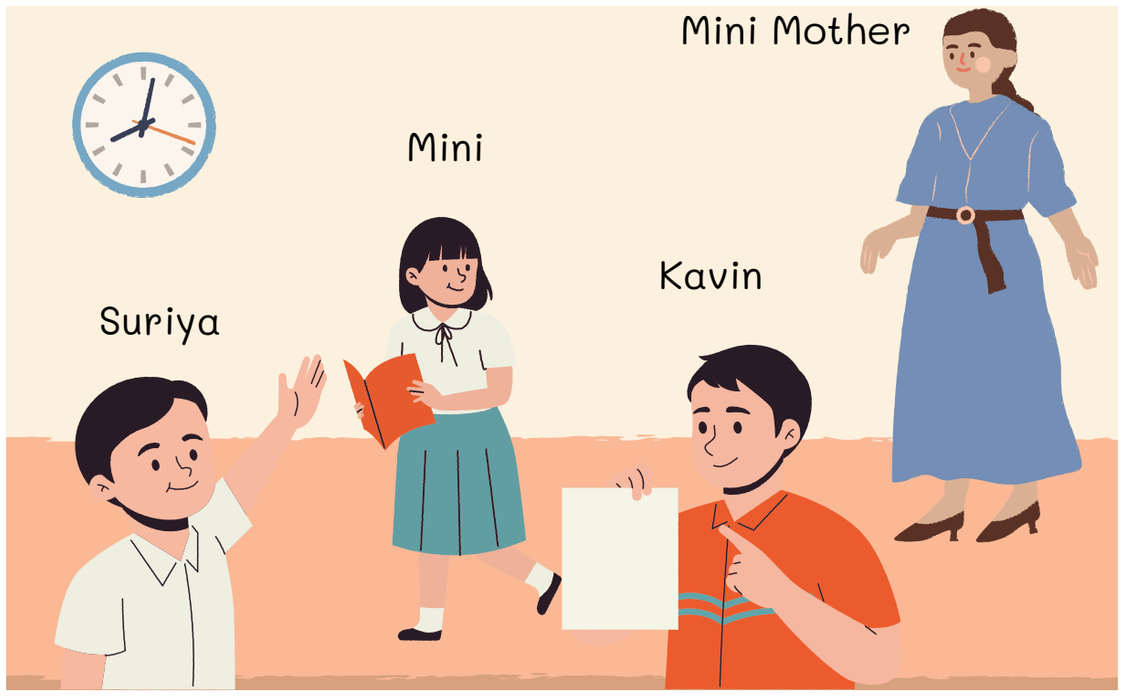
- **Adults posing as children or teenagers**
- **Requests for personal information, such as name, address, school, or phone number**
- **Offers of gifts, money, or other incentives in exchange for personal information or meetings**
- **Attempts to isolate the child from their family and friends**
- **Pressure or manipulation tactics to engage in inappropriate or sexual conversations**

Some Essential Rules Children need to follow

- Avoid revealing too much personal information, such as full name, address, school name, or phone number, in online transactions
- Never share passwords with anyone except parents or guardians.
- Communicate only with people they know and trust in real life.
- Exercise caution when opening links or attachments from unknown sources, as they may contain malware or phishing attempts
- Always log out of accounts after using them, especially on shared devices.
- Never reply to emails or messages from unknown or suspicious sources.
- Avoid entering websites through email links; instead, use authorized pages from the source website directly.

By adhering to these internet safety rules and being vigilant about their online interactions, children can minimize their exposure to cyber risks and enjoy a safer and more secure online experience.

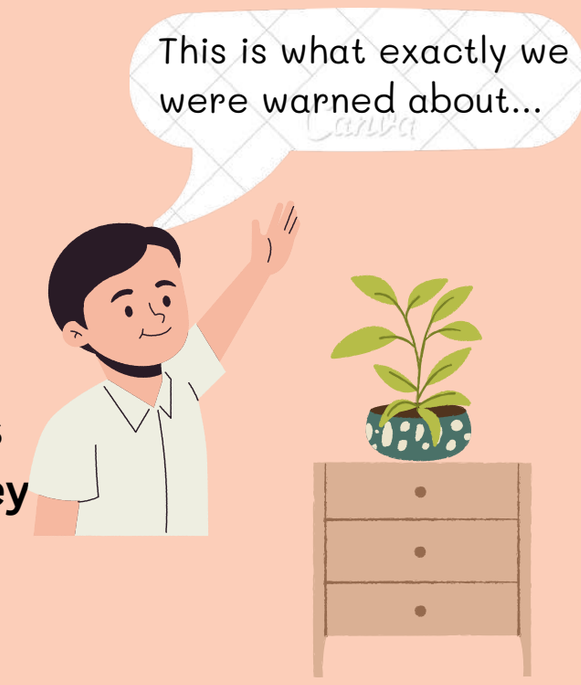
The Adventure on the Internet



There were three best friends named Surya, Kavin, and Mini who lived in Coimbatore in the same apartments. They studied in the same school. Whether they were playing in the park or fnding interesting movies on the internet, they enjoyed trying new things together.

They came across a website that promised entertaining films and thrilling activities one day while browsing the internet. They eagerly clicked on a link, which took them to a page with eye-catching graphics and upbeat music. However, as they scrolled down, they saw something odd. Some of the images and videos made them uneasy because of their peculiar appearance.

Recalling their parental guidance on online safety, Surya, Kavin and Mini immediately shut down the page and discussed with their parents what they had observed. They came to understand that certain content on the internet was unsuitable or harmful and was not intended for children. They choose to inquire with their parents out of curiosity.



According to Mini's mother, there are guidelines to keep everyone safe on the internet, just like in the real world. She informed them that it was illegal to transmit or publish content online that was inappropriate for children under Section 67B of the IT Act.

Additionally, according to Surya's mother, there are rules like the POCSO Act that shield kids from things that could harm or confuse them. She clarified that in the event that they came across something on the internet that seemed off . The parents gave a revisit about the lessons on good touch, bad touch and virtual touch to the children.

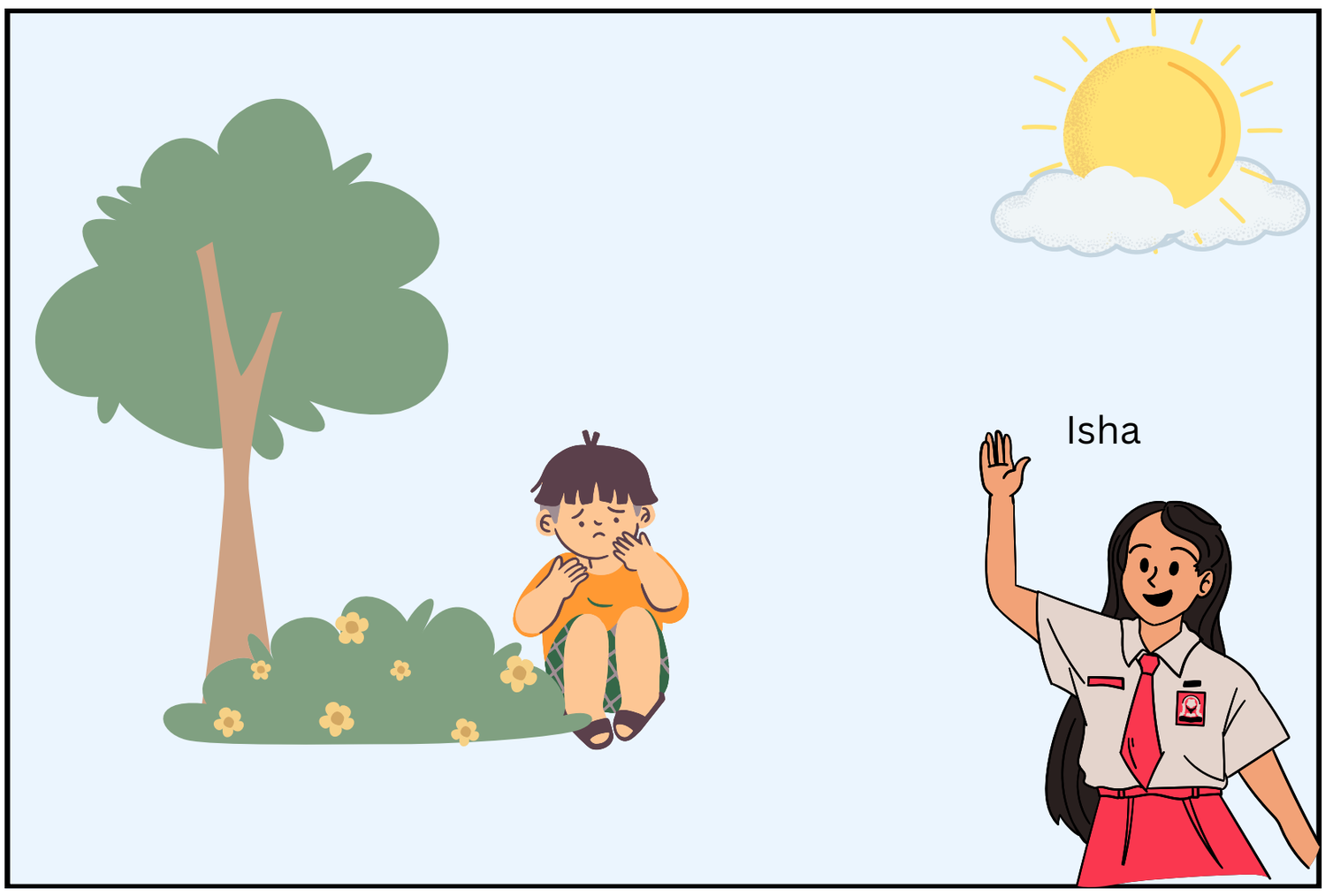
The three best friends resumed their online explorations, but this time they were more vigilant and mindful of the laws as they felt more knowledgeable and in control. With their newly acquired expertise, they carefully navigated the digital world while keeping a close eye on one another. And as they did, their friendship deepened, adding to the joy and excitement of each online journey.

As a parent it is our duty to teach our kids about cyber safety and I'm proud how they handled a situation...

Since we know about cyber safety we are able to do what is right...

We should spread this safety awareness as much as possible !!!

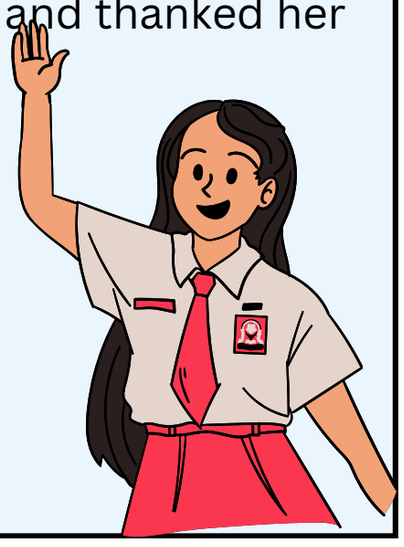
The Helping Hand

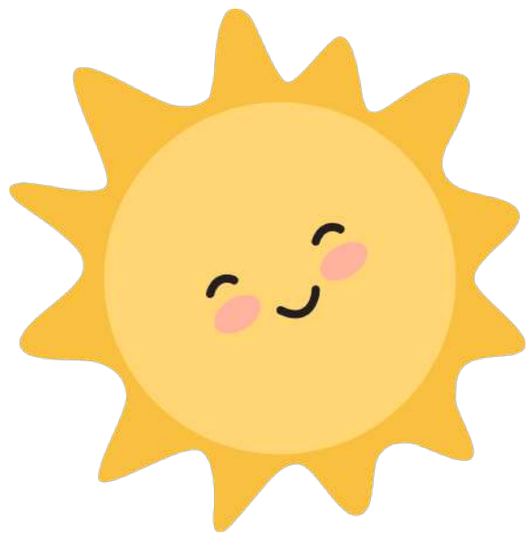


In a bustling city lived a young girl named Isha. She was bright and curious, always eager to explore the world around her. But one day, while playing in the park, She noticed a little boy sitting alone on a bench, looking sad and scared. Approaching him with concern, Isha asked the boy what was wrong. Through tearful eyes, he revealed that he had run away from home because he was afraid of his parents. Isha knew she needed to help him but wasn't sure what to do.

Suddenly, she remembered something her teacher had told her about a special number called 1098, the Child Helpline. With determination, Isha dialed the number and explained the situation to the kind voice on the other end. Within minutes, a team of caring adults arrived at the park, comforting the frightened boy and ensuring his safety. They reassured Isha that she had done the right thing by calling for help and thanked her for being brave and compassionate.

Remember kids 10,9,8 easy to remember right 1098

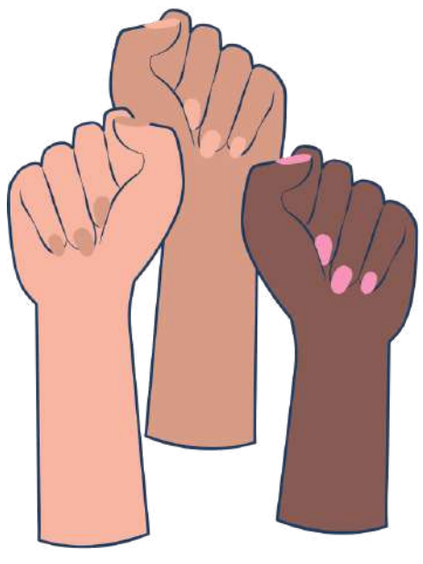




From that day on, She understood the importance of the Child Helpline number 1098. It was a lifeline for children like her new friend, providing support, protection, and hope in times of need. And as she watched the boy being reunited with his family, Isha knew that she had made a difference by reaching out and lending a helping hand.

Cyber Risks for Women

Women face specific cyber risks that can compromise their safety and wellbeing in the digital world. Understanding these risks and taking proactive measures is crucial for women to protect themselves online. Here are some key cyber risks for women and ways to mitigate them:



Online Harassment and Abuse

Online harassment and abuse are prevalent issues that many women encounter in cyberspace. This can include receiving threatening messages, being stalked on social media, or experiencing cyberbullying. Perpetrators may use various platforms to target women, causing emotional distress and psychological harm.

To combat online harassment and abuse, women should:

- **Keep personal information private and limit sharing details about their daily activities or whereabouts online.**
- **Block and report individuals who engage in harassing behaviour on social media platforms or other online forums.**
- **Seek support from trusted friends, family members, or online support groups if they experience harassment or abuse online.**
- **Avoid sharing details like your address, places you visit often, or your daily routines, as this information can give stalkers insight into your life both online and offline.**
- **Limit your online sharing to trusted friends and family members, and be cautious about who you add to your social media networks.**
- **Consider involving law enforcement authorities if the harassment escalates or poses a serious threat to their safety.**

Cyber Stalking

Cyber stalking is a serious crime that can have severe consequences for victims. It involves someone using the internet or other electronic means to harass, intimidate, or threaten another person. To protect yourself from cyber stalking, it's essential to keep your personal information private online.

Picture Morphing and Deep Fakes

Picture morphing and deep fakes are techniques used to manipulate images or videos to create fake content that appears genuine. With the advancement of hightech software and artificial intelligence (AI), creating convincing deep fakes has become easier than ever.

These manipulated images or videos can be used for various malicious purposes, including spreading false information, defaming individuals, or creating fake identities.

It's important to be vigilant and skeptical of media content online, especially if it seems too good to be true or if it portrays someone in a negative light.

Always verify the authenticity of images and videos before sharing them, and report any suspicious or harmful content to the appropriate authorities or platforms.

Safety Tips for Online Dating and Social Networking

Online dating platforms and social networking sites can expose women to various risks, including romance scams and emotional manipulation. Predators may use these platforms to exploit women's emotions and deceive them for financial gain or other ulterior motives

To stay safe when using online dating and social networking sites, women should

- **Exercise caution when interacting with strangers online and avoid sharing personal or sensitive information too quickly.**
- **Trust their instincts and be wary of individuals who seem too good to be true or pressure them into making hasty decisions.**
- **Arrange to meet in public places and inform friends or family members about their plans when meeting someone from an online dating site.**
- **Report any suspicious or abusive behaviour to the dating platform's administrators and cease communication with individuals who exhibit red flags.**

By following these safety tips and remaining vigilant online, women can reduce their vulnerability to cyber risks and enjoy a safer and more secure digital experience

Relevant IT Acts and IPC Sections

IT Act and IPC

There are several laws under IPC and IT Act, some are listed below

Cyber Stalking

IPC Section 354 D - Stalking

Picture Morphing

IPC Section 469 - Making false electronic document for causing defamation.

IT Act Section 67 - Punishment for publishing or transmitting obscene material in electronic form

Profile Hacking

IT Act Section 66 - Computer related offence

Deep Fakes

IT Act Section 67 - Punishment for publishing or transmitting obscene material in electronic form

IT Act Section 67 - Punishment for publishing or transmitting material containing sexually explicit in electronic form

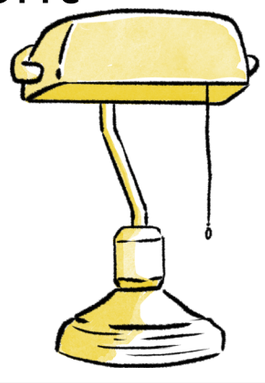
Social Trolling

IPC Section 509 - Word, gesture or act intented to insult modesty of women

Building Digital Resilience

In today's digital age, building digital resilience is crucial for both children and women to navigate the online world safely and confidently. By empowering children to stay safe online, strengthening women's cybersecurity awareness, and implementing practical strategies for cyber safety, we can build digital resilience and create a safer and more secure online environment for everyone.

Here are some ways to empower children to stay safe online, strengthen women's cybersecurity awareness, and implement practical strategies for cyber safety:



Practical Strategies for Cyber Safety:

- **Use strong, unique passwords for online accounts and enable two factor authentication whenever possible to add an extra layer of security.**
- **Keep software and antivirus programs up to date to protect against vulnerabilities and malware infections.**
- **Be cautious when clicking on links or downloading attachments from unknown or suspicious sources, as they may contain malware or phishing attempts.**
- **Regularly backup important data and files to a secure location to prevent data loss in the event of a cyber attack or system failure.**
- **Stay informed about the latest cybersecurity threats and trends, and be proactive in implementing security measures to mitigate risks effectively.**

Empowering Children to Stay Safe Online:

- **Teach children about the importance of internet safety from a young age. Discuss concepts like privacy, online behaviour, and the potential risks of sharing personal information online.**
- **Encourage open communication with children and create a safe space for them to ask questions or express concerns about their online experiences.**
- **Set clear guidelines and boundaries for internet use, including rules about which websites they can visit, who they can communicate with online, and how much time they can spend online each day.**
- **Teach children how to recognize and respond to online threats, such as cyberbullying, grooming, or inappropriate content. Encourage them to trust their instincts and seek help from a trusted adult if they ever feel uncomfortable or unsafe online.**

Strengthening Women's Cybersecurity Awareness:

- **Educate women about common cyber threats and vulnerabilities they may encounter online, such as phishing scams, identity theft, or online harassment.**
- **Provide resources and training programs to help women improve their cybersecurity skills, including how to create strong passwords, identify suspicious emails, and secure their online accounts.**
- **Promote awareness of online privacy rights and best practices for protecting personal information online, such as using privacy settings on social media platforms and avoiding oversharing personal details.**
- **Encourage women to stay informed about cybersecurity news and trends, and to stay vigilant against emerging threats in the digital landscape.**

Support System

In India, support systems play a crucial role in assisting individuals who have experienced cyber incidents or become victims of cyber crimes. By accessing support systems, seeking help, and reporting cyber incidents promptly, victims of cyber crimes in India can receive the assistance they need to address the situation effectively, protect their rights, and pursue justice. It's essential to raise awareness about available resources and encourage victims to seek support without hesitation.

Seeking Help and Reporting Cyber Incidents:

- If you've experienced a cyber incident or believe you've been a victim of cyber crime, seeking help promptly is essential. One avenue for assistance is contacting the Cyber Crime Helpline at 1930 or 155260 or 18002096789. This helpline provides guidance and support to individuals facing cyber threats or crimes.
- Additionally, victims can reach out to their local police station or cyber crime cell to report incidents and seek assistance. Most major cities in India have dedicated cyber crime cells staffed with experts who investigate cyber crimes and provide support to victims.
- It's crucial to document all relevant information about the incident, including any communication with the perpetrator, screenshots of suspicious activities, and details of financial transactions if applicable. This information can be helpful during the reporting process and subsequent investigations.

Resources for Victims of Cyber Crimes:

- Victims of cyber crimes in India have access to various resources and support services to help them navigate the aftermath of an incident. Organizations such as the Cyber Crime Helpline, Cyber Crime Cells, and the National Cyber Crime Reporting Portal (www.cybercrime.gov.in) offer guidance, support, and assistance to victims.
- Legal assistance is also available to victims through organizations such as legal aid clinics, NGOs, and cyber law firms specialising in cyber crime cases. These resources can provide victims with legal advice, representation, and assistance in filing complaints or seeking redress through the legal system.
- Counseling and support services are available to help victims cope with the emotional and psychological impact of cyber crimes. Many NGOs and mental health organizations offer counselling services specifically tailored to individuals who have experienced cyber harassment, cyber bullying, or other forms of online abuse.

Government Initiatives

Indian Government has taken numerous initiatives to prevent cyber attacks. Some of the initiatives listed below

The Indian government has taken several initiatives to combat cyber crimes, particularly those involving child sexual abuse material. Section 67B of the Information Technology (IT) Act, 2000, imposes strict penalties for publishing, transmitting, or viewing such material online. Additionally, the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs has been established to facilitate comprehensive and coordinated responses by law enforcement agencies to cyber crimes.

Through the Nirbhaya Fund, the government implements the 'Cyber Crime Prevention against Women and Children (CCPWC)' project, which focuses on raising awareness about cyber crimes, issuing alerts and advisories, and enhancing the capacity of law enforcement personnel and judicial officers. Furthermore, the government has mandated internet service providers to block access to websites containing child sexual abuse material, utilizing lists provided by organizations like the Internet Watch Foundation (IWF) and Project Arachnid.

A memorandum of understanding (MoU) has been signed between the National Crime Records Bureau (NCRB) of India and the National Center for Missing and Exploited Children (NCMEC) of the USA. This MoU facilitates the sharing of reports on online child pornography and sexual exploitation, received by NCMEC's Tip Line, with Indian authorities for further action through the National Cybercrime Reporting Portal.

This book would not have been possible without the vision, passion and efforts of entire

Prajasetu Team

Author : Krithika Ramasethu

Sincere Thanks!

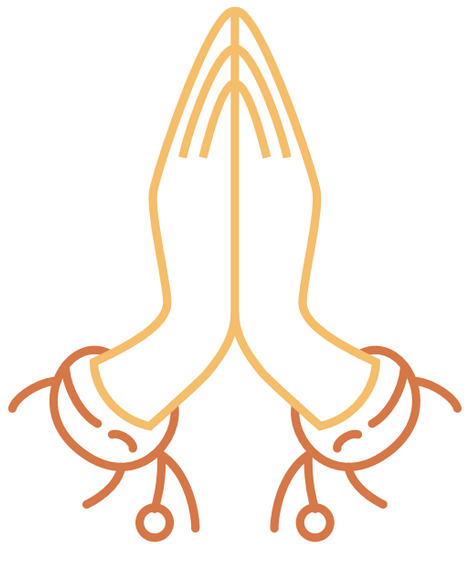
Mr. Sam Prakash (ACVCI)
&
Anti Corruption and Vigilance Council of India

Website:

www.prajasetu.in
www.acvcindia.com

Special Thanks to!

Mr.Gunasekaran
Coimbatore
Advisor - Prajasetu



Jai Hind !!!