## 1. COURSE OBJECTIVE

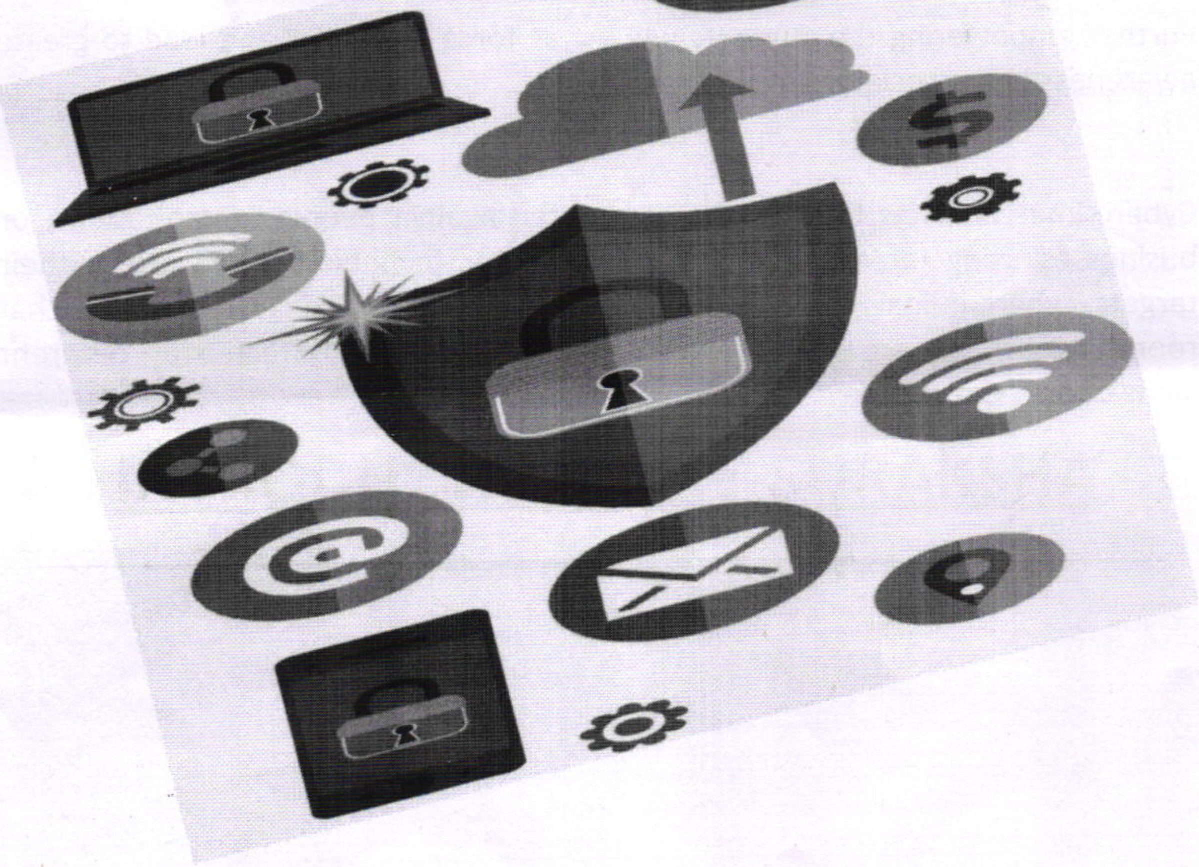
The introduction to E-Suraksha program is designed to provide students with a comprehensive understanding of the various types of E-Frauds and scams that happen online and the tactics used by cyber criminals to deceive individuals and gain unauthorized access to sensitive information. This course aims to educate and empower students to protect themselves against online threats by enhancing their digital literacy and promoting safe online practices.

Further empowering the students will act as force multiplier and lead to greater awareness in the society.

Cybercrimes are acts that can be committed against people, organizations, or businesses using internet, mobile, or computer technologies. To attack their targets, cybercriminals make use of tools like social networking sites, emails, chat rooms, websites, fake software, etc. Children especially affected by different kinds of online crime.

## Course Title

# INTRODUCTION TO E-SURAKSHA



## 2. METHODOLOGY (HOW THIS COURSE WORKS)

a. Primarily the state police should organize a ToT course for Student Police Cadet (SPC) trainers or invite experts to take the classes for students on E-Fraud.

b. The next step is to provide awareness classes and training to students about E-Fraud and equip them to act as amplifiers for further educating the society.

c. The students will be able to create awareness not only in their family, but friends, relatives, and neighborhood also.

d. This course can be translated in the local languages by the respective state Police so as to sensitize larger number of students and public about E-Fraud and the modus operandi of criminals.

## 3. ROLE OF STUDENTS

The role of SPC students in raising awareness about online frauds is essential in today's digital age. As technology continues to advance, so do the methods used by scammers and cybercriminals to deceive and exploit individuals online.

Students can play a crucial role in creating a safer online environment by fulfilling the following responsibilities:

- **Education and Awareness:**
  Students can educate themselves about various online frauds, scams, and phishing techniques. By understanding how these frauds work, they can educate their peers and even older generations about the risks and precautions to take while using the internet.

- **Sharing Information:**
  Students can act as messengers of information by sharing articles, videos, and other resources related to online frauds on social media, school

platforms, or community forums. The dissemination of such information can help others stay informed and vigilant.

- **Reporting Incidents:**
  If Students come across suspicious online activities or receive phishing emails, they should promptly report them to relevant authorities or their school's IT department. Reporting such incidents can prevent further damage and help identify and apprehend perpetrators. Also, they can report on the National Cyber Crime Reporting Portal (www.cybercrime.gov.in).

- **Organizing Awareness Campaigns:**
  Students can take the initiative to organize awareness campaigns and workshops within their schools or communities to address the risks of online frauds. This can include inviting experts or law enforcement officials to speak about cyber security and online safety.

- **Encouraging Strong Password Practices:**
  Students can advocate for using strong and unique passwords for different on!ine accounts and encourage others to do the same. Using password managers can also help enhance security.

- **Promoting Two-Factor Authentication (2FA):**
  Promoting the use of two-factor authentication for online accounts can add an extra layer of security and protect against unauthorized access.

- **Being Critical Online:**
  Students should be cautious while clicking on links, downloading files, or sharing personal information online. Encouraging a critical mindset can help prevent falling victim to phishing attempts.

- **Mentorship:**
  Students who are tech-savvy can mentor their peers, older adults, or younger children on safe internet usage, helping them understand potential risks and how to protect themselves from online scams.

- **Cyber Ethics:**
  Promote the importance of ethical behavior online and discourage engaging in cyber bullying or any form of online harassment, which can be harmful to individuals and society as a whole.

- **Continuous Learning:**
  Students should stay updated on the latest online fraud trends and cyber security best practices. Technology is constantly evolving, and staying informed is crucial to remain vigilant. Twitter and other social media handles of Cyber Dost, an initiative of I4C, may also be promoted.

## 4. LEARNING OBJECTIVES-

By the end of this course, students will be able to:

- Identify common online frauds and scams and understand their working mechanisms.
- Recognize warning signs and red flags associated with different types of cybercrimes and scams.
- Analyze phishing techniques and develop strategies to prevent falling victimto phishing attacks.
- Evaluate various types of identity theft and implement preventive measures.
- Understand the risks associated with online shopping, banking, and financial transactions.
- Develop strategies to safeguard personal and financial information online.
- Comprehend the techniques used in social engineering and devise strategies to avoid manipulation.
- Recognize the role of malware, ransom ware, and other malicious software in online frauds.
- Explore the legal and ethical aspects of cybercrimes.

- Develop critical thinking and decision-making skills to navigate online platforms securely.
- Equip students to make awareness in society.

## 5. SYLLABUS

Cyber security is like a digital shield that protects our online world from bad actors and digital threats. It's all about keeping our computers, smartphones, andthe vast network of interconnected devices safe from hackers and malicious software. Think of it as a virtual lock and key system for the internet.

Imagine you have a secret diary stored on your computer. Cyber security ensures that no one can break into your computer to read your diary without your permission. It does this by setting up barriers and defenses, like strong passwords, firewalls, and antivirus programs. These tools act as guards, monitoring your digital space and blocking any suspicious activity.

In a world where we rely heavily on the internet for communication, work, and entertainment, cyber security plays a crucial role in ensuring our online experiences are safe and secure. It's like having a digital superhero that works tirelessly to keep the virtual realm free from harm, allowing us to enjoy the benefits of the digital age without constantly worrying about threats lurking in the shadows.

## i. INTRODUCTION TO ONLINE FRAUDS AND SCAMS

The landscape of online frauds and scams is constantly evolving, but here's an overview of some common types:

- **Phishing:** Fraudsters send deceptive emails or messages that appear to be from trusted sources to trick individuals into revealing personal information, such as passwords or credit card numbers.

- **Identity Theft:** Criminals steal personal information to impersonate victims, open fraudulent accounts, or make unauthorized transactions.

- **Online Shopping Scams:** Fake online stores or sellers lure customers with attractive offers, but then fail to deliver the promised goods or provide substandard products.

- **Tech Support Scams:** Scammers pretend to be tech support agents and convince victims to grant remote access to their computers, often charging for unnecessary services.

- **Investment Scams:** Fraudulent investment opportunities promise high returns but result in losses or the disappearance of funds.

- **Romance Scams:** Con artists create fake online personas to develop emotional relationships with victims and then request money for various reasons.

- **Data Breaches:** Cyberattacks on organizations lead to the theft of customerdata, which can be sold or used for identity theft.

- **Lottery and Prize Scams:** Victims are informed they've won a lottery or prize but must pay fees or taxes upfront to claim their winnings.

- **Job and Employment Scams:** Fake job postings or work-from-home offerstrick job seekers into providing personal information or paying for trainingor equipment

- **Charity Scams:** Fraudsters pose as charitable organizations during disasters or crises to solicit donations that never reach the intended cause.

- **Loan Scams:** Bogus lenders offer loans with low interest rates but charge upfront fees or disappear after receiving payments.

**Understanding the Motivation of cyber criminals**

- **Money:** Many cybercriminals are motivated by the prospect of making money through activities such as hacking bank accounts, credit card fraud.

- **Thrill and Challenge:** Hacking for the fun of it.

- **Data Theft:** Stealing personal information (like passwords).

- **Revenge:** Targeting someone they're angry with.

- **Political or Ideological Beliefs:** Promoting their views through cyberattacks.

- **Espionage:** Spying on companies or governments and gathering sensitive information.

- **Identity Theft:** Pretending to be someone else online or misusing stolen identities for fraud.

- **Cyber bullying:** Harassing or tormenting others online causing emotional harm through the internet.

**The impact of online frauds on students and society**

Online frauds can have a significant impact on both students and society:

- **Financial Loss:** Students may fall victim to scams, phishing, or fraudulent websites, leading to financial losses that can be especially burdensome for them. In society, the cumulative financial impact can be substantial.

- **Psychological Distress:** Victims of online fraud may experience stress, anxiety, and a loss of trust in online platforms. This can affect their mental well-being and their ability to engage in online activities.

- **Educational Disruption:** Online fraud can disrupt a student's education, as falling victim to scams can lead to distraction, loss of funds for tuition, or even identity theft, affecting academic progress.

- **Trust issue:** Widespread online fraud destroy trust in online systems, making it harder for society to embrace the benefits of the digital age, from e-commerce to online education.

- **Cyber security Costs:** Society and educational institutions may need to invest more in cyber security measures to protect against online fraud, increasing overall costs.

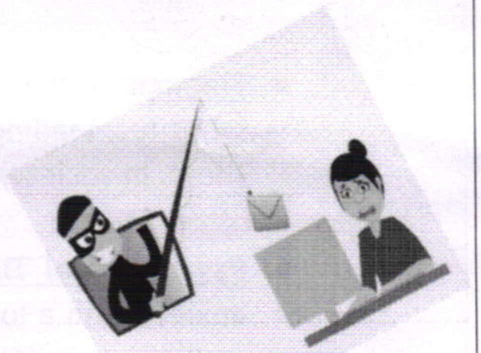
- **Digital Literacy:** To combat fraud, students and society need to develop better digital literacy skills to recognize and avoid online scams, which requires time and effort.

**Some video links are provided for better understanding:**

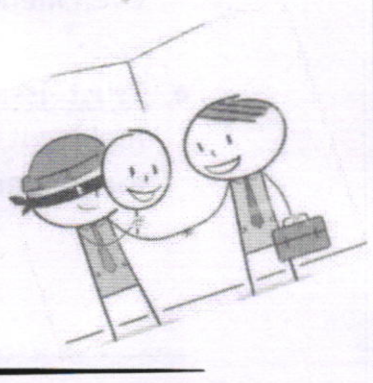
- Online scams: https://youtu.be/ICz89A0x0tc?si=LR3mfi9_uUuLPX6P
- Internet safety and security: https://youtu.be/yiKeLOKc1tw?feature=shared

## ii. PHISHING ATTACKS AND IDENTITY THEFT

**"Phishing is scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illegally."**



**"Identity theft is the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making unauthorized transactions or purchases."**



## How To Recognize Phishing

Scammers use email or text messages to try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could get access to your email, bank, or other accounts. Or they could sell your information to other scammers.

You might get an unexpected email or text message that looks like it's from a company you know or trust, like a bank or a credit card or utility company. Or maybe it's from an online payment website or app. The message could be from a scammer, who might

- Say they've noticed some suspicious activity or log-in attempts — they haven't
- Claim there's a problem with your account or your payment information — there isn't
- Say you need to confirm some personal or financial information — you don't
- Include an invoice you don't recognize — it's fake
- Want you to click on a link to make a payment — but the link has malware
- Say you're eligible to register for a government refund — it's a scam
- Offer a coupon for free stuff — it's not real

## Preventive measures to avoid falling victim to phishing attacks

- Never provide your personal information in response to an unsolicited request.
- Never provide your password over the phone or in response to an unsolicited Internet request.
- Review account statements regularly to ensure all charges are correct.

- **Morphing Pictures and Misusing**

Morphing images of children is a serious issue that can have a devastating impact on the child's life. It can be used to create child sexual abuse content, or to humiliate or embarrass the child. The misuse of morphed images of children is a serious problem that can have a lasting impact on the child's life. It is important to be aware of the risks and to take steps to protect children from this type of abuse.

If you are concerned that your child may be a victim of the misuse of morphed images, there are a number of resources available to help you. You can contactthe National Centre for Missing and Exploited Children (NCMEC) at 1-800-THE- LOST (843-5678) or visit their website at https://www.missingkids.org/.

- **Fake Phone Call**

Fake phone calls are a common type of cybercrime that can target children.

Here are some specific examples of fake phone calls ,

- ➢ A caller claiming to be from a bank or credit card company says that the child's account has been compromised and that they need to verify their personal information to protect it.
- ➢ A caller claiming to be from a government agency says that the child has committed a crime and that they need to pay a fine or face arrest.
- ➢ A caller claiming to be from a tech support company says that the child's computer has been infected with a virus and that they need to pay for a service to fix it.
- ➢ A caller claiming that your ATM card has been blocked. Provide your ATM card's 16 digit number/validity date/CVV number (Card Verification Value)

on the back of the ATM card. If you tell the ATM card number, validity date, CVV number and OTP password written on the back of the card, you will immediately become a victim of fraud.

Be alert and careful; do not tell information related to bank account and ATM to anyone. If you receive a call like this, you should immediately contact your bank branch. For fake phone calls- do not answer phone calls from unknown numbers, hang up on calls that make them feel uncomfortable, never give out personal information over the phone, we should monitor our child's phone activities and talk to them about any suspicious calls they receive.

**Some video links are provided for better understanding:**

- What is phishing: https://youtu.be/sS3mZVCARZg?si=ylWxxc9oAJTmZgLQ

## iii. SAFE ONLINE SHOPPING, BANKING, AND FINANCIAL TRANSACTIONS

There are several risks associated with online shopping, banking, and financial transactions, including security breaches, identity theft, unsecured Wi-Fi, payment fraud, account takeovers, downloading malicious software or clicking on infected links, fake online retailers, transaction errors, etc.

**Securing personal and financial information**

Securing personal and financial information is crucial to protecting yourself from identity theft and financial fraud. Use strong, unique passwords, enable two-factor authentication (2FA), Keep software updated, be cautious with emails, secure your devices, use secure Wi-Fi networks, install security software, and regularly backup data.

**Preventive measures**

Preventive Measures for Online Shopping, Banking, and Financial Transactions:

- Use Strong Passwords Enable Two-Factor Authentication (2FA).
- Update Software.
- Beware of Phishing.
- Use Secure Wi-Fi.
- Monitor Your Accounts.
- Shop from Reputable Websites.
- Use a Secure Connection.
- Be Cautious with Personal Information.
- Keep Financial Information Secure.

**What to Do When There's an Issue:**

- Report Unauthorized Transactions.
- Change Passwords.
- Contact Customer Support.
- File a Complaint.
- Check for Fraud Alerts.
- Install Security Software.

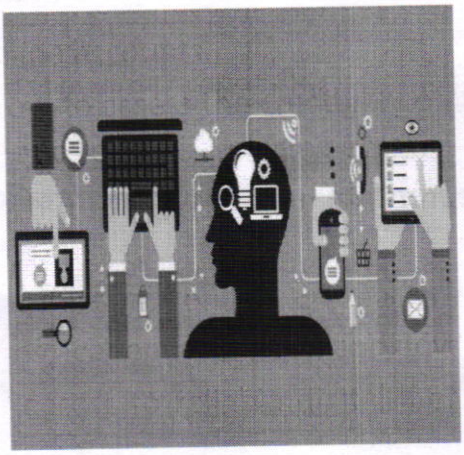
**Some video links are provided for better understanding:**

- Safe shopping and banking online: https://youtu.be/6At2rCPJWPo?si=mVUNvHeS99gFTz-5
- How do online payments work: https://youtube.com/watch?v=li-eClybZKA&feature=shared

## iv. Malware, Ransomware, and Other Threats:

- **Introduction to malware, ransomware, and other malicious software**
- **Preventive measures to avoid malware infections**
- **Recognizing and responding to ransomware attack Safeguarding devices and data against online threats**

## v. TEACH DIGITAL LITERACY SKILLS



a. Teach how to connect to the internet and navigate web browsers.

b. Explain the concept of URLs, hyperlinks, and how to use search engines effectively.

c. Emphasize the importance of not sharing personal information online.

d. Explain how to adjust privacy settings on social media platforms and otheronline accounts.

e. Teach how to assess the credibility of websites, spot fake news, verify sources and recognize phising emails.

f. Discuss the dangers of misinformation and how to fact-check information.

g. Teach effective online research techniques, including using databases,academic sources, and advanced search operators.

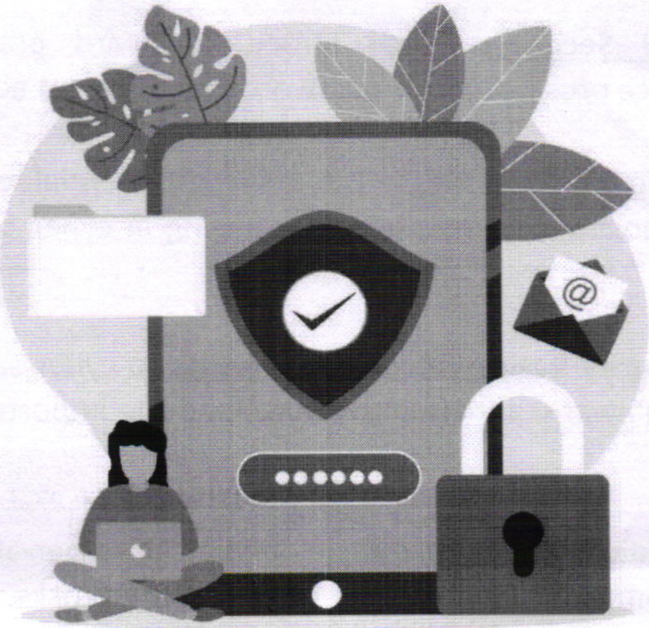
h. Provide access to reliable digital literacy resources and websites for further learning.

**Some video links are provided for better understanding:**

➢ Importance of Digital Literacy : https://youtu.be/A6k82xAK5ns?si=lnP0MYYys3yVKYhg

## vi. **ENCOURAGE SKEPTICISM**

Encouraging skepticism in students about cyber safety is essential in today'sdigital age. Here are some ways to promote this mindset:



- **Critical Thinking:** Teach students to question information online. Encourage them to ask who created the content, why it was created, and whether it's reliable.

    a. **Source Evaluation:** Show them how to assess the credibility of sources, including websites, news articles, and social media accounts. Emphasize the importance of cross-referencing information.

b. **Privacy Awareness:** Discuss the importance of protecting personal information online. Teach them about privacy settings and the potentialrisks of oversharing.

c. **Digital Literacy:** Promote digital literacy skills, including the ability to spotmanipulated images, deep fakes, and misinformation.

d. **Password Security:** Teach strong password practices and the importance ofusing unique passwords for different accounts.

e. **Social Media Awareness:** Discuss the potential consequences of sharing sensitive information or engaging in cyber bullying on social media.

f. **Cybersecurity Basics:** Introduce students to cyber security concepts, such as malware, antivirus software, and the importance of software updates.

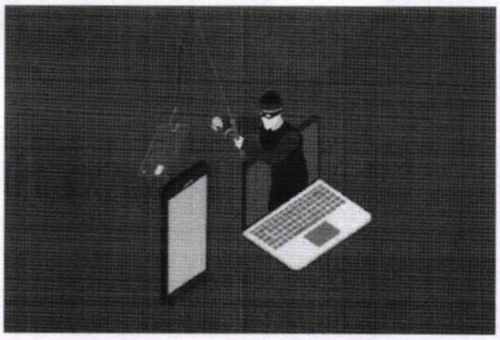
g. **Case Studies:** Share real-life examples of cyber-attacks and their impact tomake students aware of the potential risks.

h. **Encourage Questions:** Create an open environment where students feelcomfortable asking questions about cyber safety and seeking help whenneeded.

**Some video links are provided for better understanding:**

- Encourage skepticism: https://youtu.be/HxySrSbSY7o?si=eZNtjZcmZ26V6dyX
- Internet safety tips: https://youtube.com/watch?v=X9Htg8V3eik&feature=shared
- Staying safe online: https://youtube.com/watch?v=PtfEnh0gbbU&feature=shared

## vii. EXPLORE REAL LIFE EXAMPLE

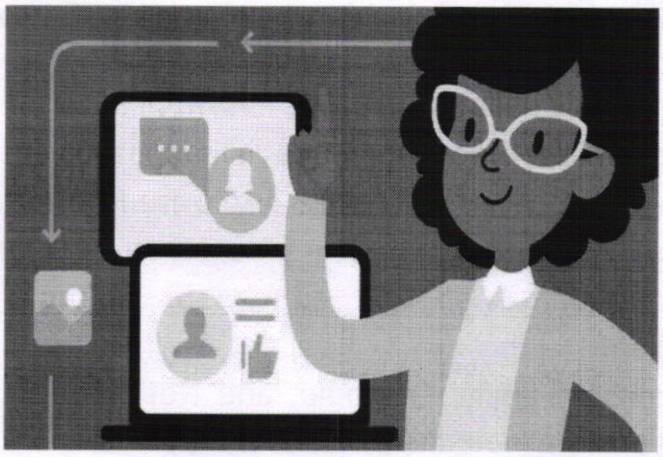


Share real-life stories of individuals who have fallen victim to online frauds and scams. Discuss the consequences and impact of these incidents to help students understand the seriousness of the issue.

**Some video links are provided for better understanding:**

- Cyber crime: https://youtu.be/g4B_HFL8z4Y?si=tINqXeVJ6juFDj_8
- Phishing example: https://youtu.be/3-zuLMdZo9M?si=TkVjLK2X94GVX_To
- Types of cyber crimes: https://youtu.be/bAO_ur8CJvY?si=dZnGxaYBwSS85Pq

## viii. PROVIDE RESOURCES AND TOOLS



Educating students about cyber safety is essential in today's digital age. Here are some resources and tools you can use:

➢ **Websites and Online Resources:**

- Common Sense Education: They offer free lesson plans, videos, and interactive activities on digital citizenship and online safety.
- Stay Safe Online: The National Cyber Security Alliance provides tips and resources for staying safe online.

➢ **Videos and Tutorials:**

- YouTube has numerous educational channels that cover cyber safety topics. Look for channels like "NetSmartz" and "CyberWise."

➢ **Interactive Games and Simulations:**

- Games like "Interland" by Google teach kids about internet safety through fun gameplay.
- The "CyberPatriot" competition is a great tool for high school students interested in cybersecurity.

➢ **Books and E-books:**

- "The Teen's Guide to Social Media... and Mobile Devices" by Ana Homayoun is a valuable resource for teens and parents.
- "Cyber Smart: Five Habits to Protect Your Family, Money, and Identity from Cyber Criminals" by Bart McDonough is a helpful book for a morein-depth understanding.

➢ **Online Courses:**

- Platforms like Coursera, edX, and Udemy offer courses on cybersecurity and online safety. These are suitable for older students and adults.

➢ **Cyber Safety Software:**

- Tools like Norton Family, Qustodio, and Net Nanny can help parents monitor and protect their children's online activities.

- **Educational Organizations and Workshops:**
  - Reach out to local cyber security organizations or your school district to inquire about workshops or presentations on cyber safety.

- **Discussion and Open Communication:**
  - Encourage open conversations about online experiences and potential risks with students. Create a safe space for them to ask questions.

- **Social Media Safety Guidelines:**
  - Share guidelines on safe social media use, like not sharing personal information and being cautious about online friends.

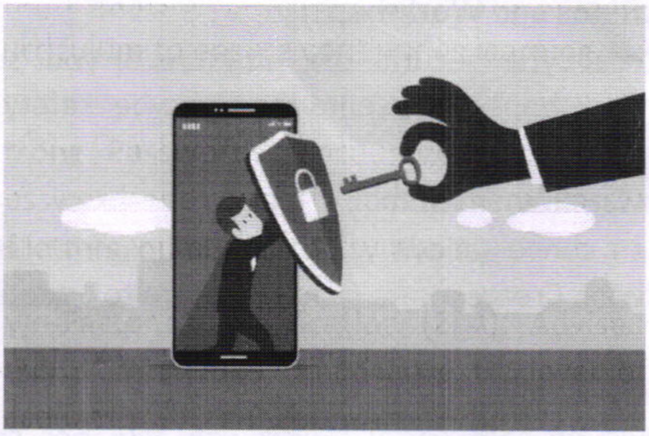
- **Password Managers:**
  - Teach students about the importance of strong, unique passwords and introduce them to password managers like LastPass or 1Password.

- **Privacy Settings:**
  - Show students how to adjust privacy settings on social media accounts and apps to control what information is shared.

**Some video links are provided for better understanding:**

- Resources and tools:
  https://youtube.com/watch?v=yrln8nyVBLU&feature=shared

## ix. DISCUSS PREVENTIVE MEASURES



Preventing cyber threats among students requires a combination of education, awareness, and proactive measures. Here are some preventive measures for ensuring cyber safety among students

a. **Digital Literacy Education:** Teach students about online risks, privacy, and responsible internet use. This should be integrated into the curriculum to ensure continuous learning.

b. **Strong Passwords:** Encourage students to create strong, unique passwordsand regularly update them. Passwords should include a mix of letters, numbers, and symbols.

c. **Two-Factor Authentication (2FA):** Advise students to enable 2FA wherever possible to add an extra layer of security to their online accounts.

d. **Safe Browsing Habits:** Emphasize the importance of only visiting trustedwebsites and not clicking on suspicious links or downloading files from unknown sources.

e. **Social Media Awareness:** Teach students about the potential risks of sharing personal information on social media platforms and the importanceof privacy settings.

f. **Secure Wi-Fi and Networks:** Encourage students to use secure Wi-Fi networks and avoid public, unsecured networks when possible.

g. **Regular Updates:** Stress the importance of keeping software, apps, anddevices up to date to patch vulnerabilities.

h. **Online Etiquette:** Promote respectful online behavior, including not engaging in cyber bullying, harassment, or sharing inappropriate content.

i. **Data Privacy:** Teach students about data privacy and the importance of safeguarding their personal information. Explain how their data may beused by online services.

j. **Reporting Mechanisms**: Ensure students know how to report cyber bullying, harassment, or any suspicious online activity to appropriate authorities or school personnel.

k. **Parental Involvement:** Encourage parents to be involved in their child's online activities, including setting age-appropriate guidelines and monitoring online behavior. For that Parents can,

   i. Establish house rules and guidelines.
   ii. Encourage and maintain an open and on-going dialogue with yourchildren.
   iii. Encourage kids to think before they click.
   iv. Look out for harmful content.
   v. Discuss the risks of posting and sharing private information.
   vi. Be a good role model.
   vii. If there are any crimes against the child, parents make sure that theyeither consult or report the matter to the appropriate authority.

l. **Secure Devices:** Teach students to secure their devices with passcodes orbiometrics to prevent unauthorized access.

m. **Regular Backups:** Emphasize the importance of backing up important filesand data to prevent data loss in case of cyber-attacks.

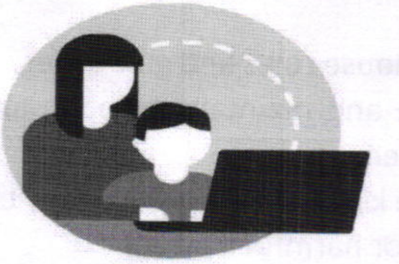
n. **Cyber security Resources:** Provide access to cyber security resources andorganizations that offer guidance on safe online practices.

o. **Simulation Exercises:** Conduct cyber security awareness drills or simulations to help students practice responding to online threats in acontrolled environment.

**Some video links are provided for better understanding:**

p. Preventive measures: https://youtu.be/Kz2es3-XJvw?si=oJ3RN4BkSKkGEZrQ

## x. PROMOTE OPEN COMMUNICATION



To promote open communication in students about cyber safety, consider the following strategies:

a. **Create a Safe Environment:** Encourage an environment where studentsfeel safe discussing their online experiences without fear of judgment or punishment. Ensure that they understand the importance of reporting anycyber bullying or unsafe situations.

b. **Education and Awareness:** Provide age-appropriate cyber safety education, including the risks and consequences of online activities. Regularly update students about emerging online threats and trends.

c. **Interactive Workshops:** Conduct interactive workshops or guest lectures byexperts in the field of cyber safety to engage students and answer their questions.

d. **Encourage Questions:** Encourage students to ask questions about cyber safety and address their concerns openly. Make it clear that there are no"stupid" questions when it comes to online safety.

e. **Use Real-Life Examples:** Share real-life stories and examples of cyber bullying or online dangers to make students aware of the potential risksand consequences.

f. **Involve Parents:** Engage parents by organizing parent-teacher meetings orworkshops on cyber safety, emphasizing the importance of collaboration between parents and educators.

g. **Peer-to-Peer Support:** Encourage students to look out for their peers andreport any concerning online behavior to school authorities.

h. **Anonymous Reporting:** Provide a way for students to report cyber bullying or online threats anonymously if they feel uncomfortable revealing their identity.

i. **Stay Updated:** Continuously update your own knowledge about cyber safety to be better equipped to guide and educate students effectively.

## xi. REINFORCE THE MESSAGE

Promoting cyber safety among students is crucial. Consider these points to reinforce the message:

a. Education
b. Strong Passwords
c. Privacy Settings
d. Cyber bullying Awareness
e. Respectful Online Behavior
f. Critical Thinking
g. Two-Factor Authentication
h. Regular Updates
i. Safe Downloads
j. Open Communication
k. Positive Role Models
l. Real-Life Impact
m. Empowerment
n. Regular Reminders

By consistently emphasizing these points, students can develop the knowledge and skills needed to stay safe in the digital world.

## 6. CONCLUSION

In conclusion, this course on E-Suraksha serves as a comprehensive guide for raising awareness about the online cyber space. By providing students with essential knowledge andskills to navigate this digital realm safely and responsibly, the aim is to empower them to make informed decisions, protect their personal information, and contribute positively to the digital world. Through the topics covered in this course/ module, we hope to foster a generation of responsible digital citizens who can confidently and securely engage in the online cyber space. Hence, awareness is to be created amongst the SPC students by imparting classes by incorporating this course in their training.

# REFERENCE

1) https://www.cisa.gov/news-events/news/keeping-children-safe-online
2) https://www.unicef.org/rosa/stories/5-ways-protect-your-young-child-online
3) https://www.justice.gov/coronavirus/keeping-children-safe-online
4) https://consumer.ftc.gov/identity-theft-and-online-security/protecting-kids-online
5) https://www.un.org/en/global-issues/child-and-youth-safety-online
6) https://www.childlineindia.org/a/issues/online-safety
7) https://www.esafety.gov.au/parents/issues-and-advice/parental-controls
8) https://www.childrens.health.qld.gov.au/blog-10-things-keep-kids-safe-online/
9) https://aifs.gov.au/resources/resource-sheets/online-safety
10) https://www.childwelfare.gov/topics/management/workforce/socialmedia/safety/
11) https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/COP.aspx
12) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10453252/
13) https://www.michigan.gov/msp/services/safetytips/internet-safety/internet-safety-for-parents
14) https://www.unicef.org/globalinsight/reports/protecting-children-cyberconflicts
15) https://unesdoc.unesco.org/ark:/48223/pf0000374365