CYBER SAFETY & SECURITY

Dr. Naveen Gupta

- **Winner of National ICT Award 2019**
- Youtuber, Author, Teacher Mentor
- Adobe Creative educator
- Cisco Certified
- Wakalet Ambassador
- Microsoft Certified Educator
- Microsoft Technology Associate - Python
- Microsoft Innovative Educator Expert(MIEE)
- Microsoft certified trainer

MENTION YOUR NAME AND STATE

What is Cyber?

Cyber refers to ….

- Virtual reality … the surfing of internet which we will perform on daily basis in our life.
-

WHAT IS DIGITAL LITERACY?

- Digital Literacy is one of the important 21st Century Literacy Skills. Digital literacy is the ability to use digital technology safely while staying within the bounds of social responsibility. It allows students, who are increasingly getting access to digital devices and the internet, to learn how to minimize risks and maximize benefits that come with using digital technologies. For instance: many students enjoy playing online games, however, they need to understand the potential risks associated with online gaming and accordingly take the necessary

EIGHT COMPONENTS OF DIGITAL LITERACY

- 1. Functional skills .
- 2. Creativity.
- 3. Critical thinking and evaluation.
- 4. Cultural and social understanding.
- 5. Collaboration.
- 6. Ability to find and select information .
- 7. Effective communication.
- 8. E-safety

E-SAFETY

- Put simply e-safety refers to staying safe online, and as internet-accessible devices are given to people of younger ages, it's important that we're able to protect them from harmful content and services. This includes: cyber-bullying, pornography, online exploitation, cyber crimes etc.

We are in the Digital World

Internet and smart gadgets are now integral part of our lives

More and more sensitive and valuable data artefacts beings stored or moved across digitally


How safe are we and our students in the cyber world?

Sequence of the Day

1. Cyber Security Threats
2. Cyber Safety Awareness
3. Cyber Safety and Security
4. Cyber Security – Initiatives in India

Objectives of the Session

- Increase awareness of cyber threats and vulnerabilities
- Empower individuals to protect themselves, their learners, and their information online
- Promote best practices for cyber security
- Collaborate to promote ethical mindset
- Empower our students to become Resources for increasing awareness on cyber threats
- Build a cyber security culture within the organization and communities

01 Cyber Security Threats

Cyber Security Threats

Cybercrime

Committed by one or more individuals who target systems for financial gain or to cause havoc

Cyberterrorism

Designed to break into systems and instil fear

Cyberattacks

Aimed at collecting and/or distributing sensitive data

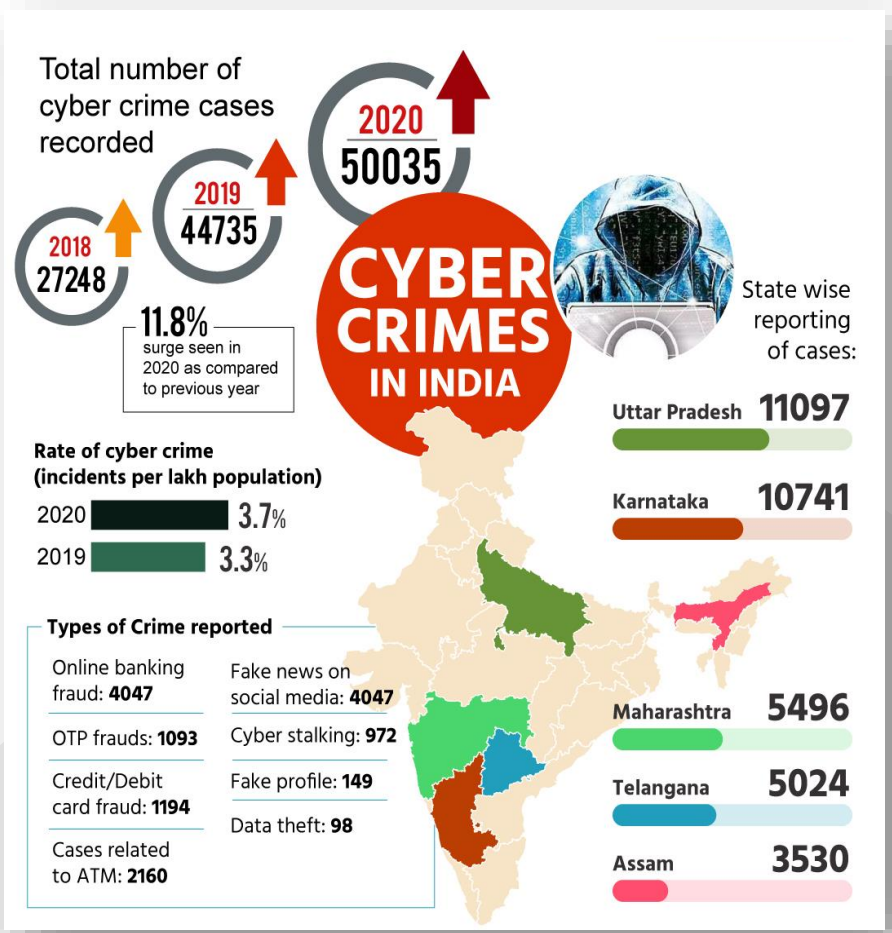
Short Answer

CYBERCRIME - A major issue

No different from any other crime happening in society

Affecting all the stakeholders from government, educational institutions, business to citizens alike

No geographical boundaries and the cybercriminals are unknown



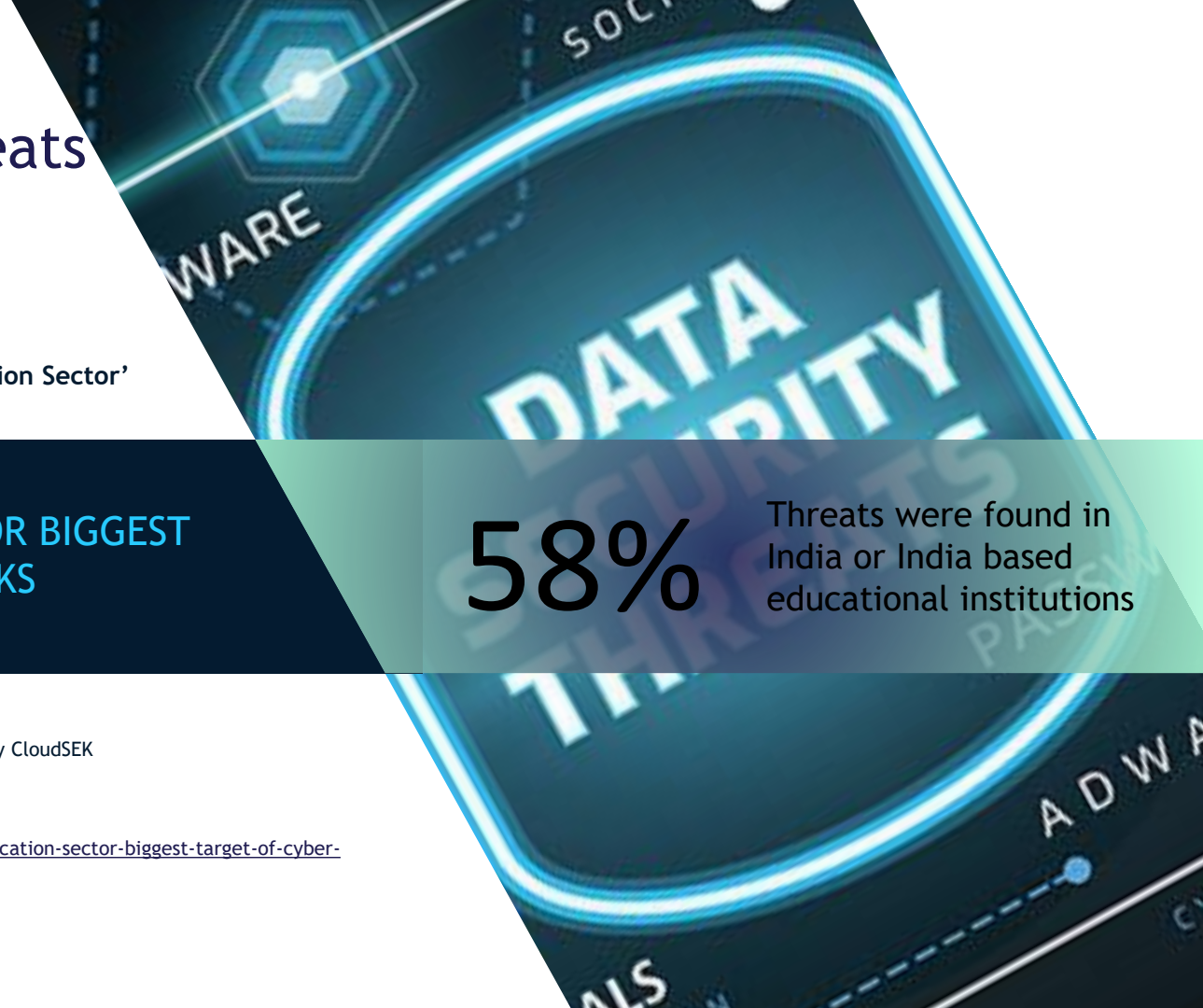
Source: https://iasscore.in/data-story/cyber-crimes-in-india

Data Security Threats

THE REPORT titled
‘Çyber Threats Targeting the Global Education Sector’

INDIAN EDUCATION SECTOR BIGGEST TARGET OF CYBER ATTACKS

58% Threats were found in India or India based educational institutions



Study conducted by Singapore-based company CloudSEK

Source: https://www.deccanherald.com/national/indian-education-sector-biggest-target-of-cyber-threats-report-1105555.html

CYBERCRIME

Criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic wracking (destruction) to denial of service attacks

Phishing	Credit Card Fraud	Stalking
Illegal Downloading	Denial of Service attacks	Child Pornography
Ransomware	Bank Robbery	Trafficking
Creation or distribution of Viruses		Hacking

Short Answer

Source: https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html

The three biggest current cyber threats that schools should be aware of are phishing, denial of service (DoS) attacks, and ransomware.

Why Are Schools So Vulnerable to Cybersecurity Threats?

Vast amounts of private data – students, staff, parents and even alumni

Outdated Technology

Limited Resources

Lack of training and awareness

Quick Poll submissions

Quick Poll submissions

“There are cyber threats out there, this is a dangerous world, and we have to be safe, we have to be secure no matter the cost.”

— Edward Snowden

Quick Poll submissions

02 Cyber Safety and Security

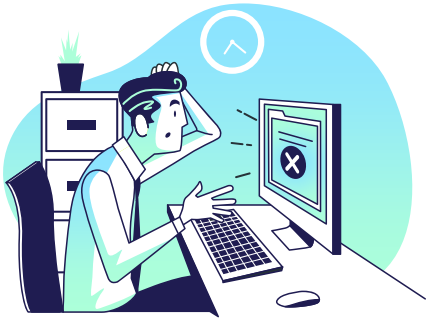
Cyber Safety and Security

Body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage or unauthorized access

Means through which people can defend themselves against dangers that lurk online

Combination of cyber ethics and tools to protect individuals from inappropriate content and behavior or Cyber fraud

Why Cyber Security?



For protecting our sensitive data (of students, parents, teachers, and other stakeholders), personally identifiable information (PII), protected health information (PHI), personal information, intellectual property and other important information from theft and damage attempted and keeping our students safe and secure online

Cyber Security Framework

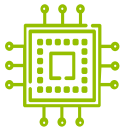
Cybersecurity is a framework that requires the marshaling (arranging) of the following resources in a coordinated manner

People

Almost always the weakest link in an organization's cyber resiliency; must be trained to recognize cyber threats and social engineering.

Processes

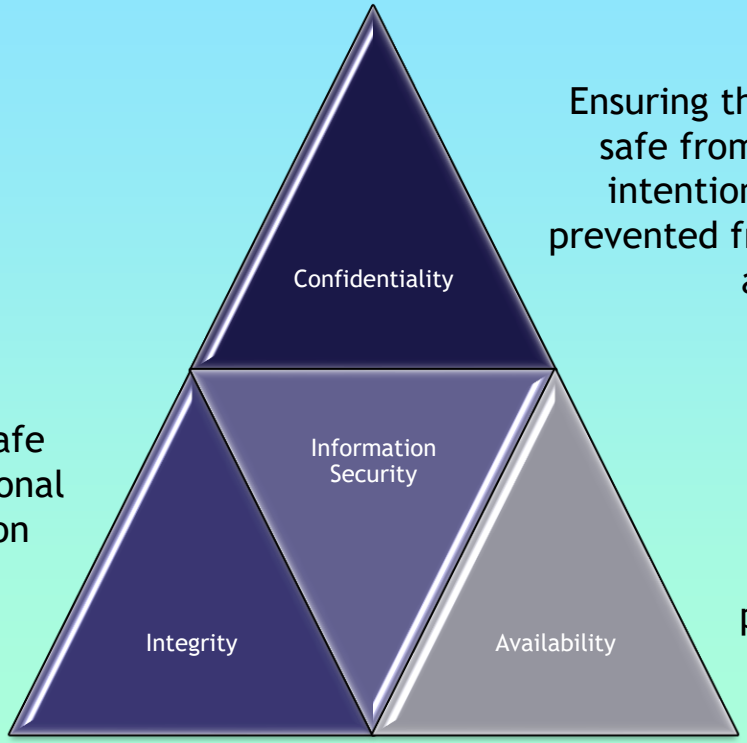
Provide the frameworks for cybersecurity governance; range from preventative strategies to avoid cyberattacks to real-time interventions in the event of cybercrime



Technology

IT infrastructure (hardware and software) organizations use to achieve cybersecurity; example include antivirus software and defensive AI that scans computer networks for anomalous behaviors and learns from prior cyberattacks

Goals or Objectives of Cyber Security Framework



Ensuring the information is safe from accidental or intentional disclosure, prevented from unauthorized access

Ensuring information is safe from accidental or intentional modification or alteration

Ensuring accessibility of information to authorized personnel at the right time

03 Cyber Security Awareness

From the perspective of an Individual, School and Students

TECHNOLOGY ALONE CANNOT PROTECT YOU FROM EVERYTHING

Attackers go where security is weakest -
Vulnerabilities within Technology

ESSENTIAL TO REDUCING CYBERSECURITY RISK
AND CREATING CYBERSECURITY AWARENESS

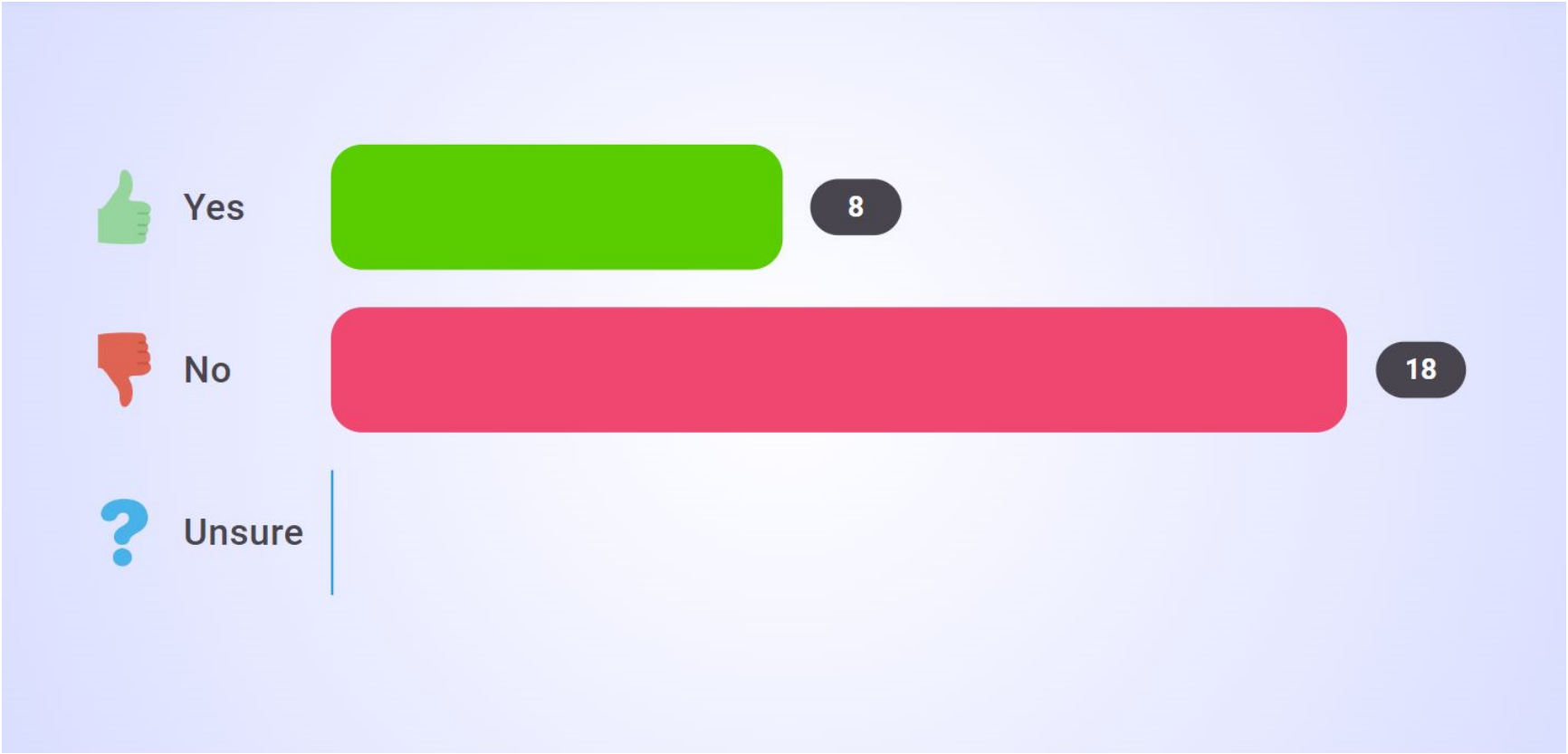
Cyber Security Awareness

An ongoing process of educating and training about the threats that lurk in cyberspace, preventing such threats and what is to be done in the event of a security incident

Helps inculcate a sense of proactive responsibility for keeping oneself and organisation and its assets safe and secure

Enhances the security posture, thereby paving the way to building more resilient systems/individuals

Quick Poll submissions



Understanding different types of Cyber Attacks

What are the digital assets we need to protect against theft / hacking or unauthorized disclosure?

Phishing

An attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as credit card numbers, bank information, or passwords -- on websites that pretend to be legitimate; can affect anyone of any age, whether in their personal life or in the workplace

Features of a Phishing Email

- Need to verify account information
- Sense of urgency
- Too good to be true
- Spelling errors
- Link email or attachment
- Alert that your account is in trouble
- Generic greetings

Safeguarding against Phishing

Employ common sense before handing over sensitive information	Never trust alarming messages
Do not open suspicious or strange emails/ SMS/ WhatsAPP — esp. Word, Excel, PowerPoint or PDF attachments	Avoid clicking any embedded links in emails/SMS/WhatsApp
Keep your Browser, Software and Operating System up to date	Never respond to any spam

Social Engineering (Psychological Manipulation)

A tactic to manipulate people into giving up confidential information, including bank information, passwords, or access to their computer to covertly install malicious software that can steal such information from the system. **For instance**, an intruder could pose as IT helpdesk staff and ask users to give information such as their usernames and passwords.

Types of Social Engineering attacks

- Baiting
- Pretexting
- Manned Phishing
- Vishing/Smishing (Voice/SMS)

Avoiding Social Engineering Attacks

Check the source	What do they know?
Break the loop (ignore the sense of urgency)	Ask for ID
Apply common sense - Is this realistic?	Secure your devices

Source: https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks

Cyber Stalking

Technologically-based ‘attack’ on a person who has been targeted specifically for that attack for reasons of anger, revenge or control; can take many forms, including: harassment, embarrassment and humiliation of the victim

Protection from Cyberstalking

Be selective about accepting friend request of strangers on social media	Learn how to block someone who is making you uncomfortable
Learn how to remove someone from our friends list	Remember to logout from social media websites after use
Secure your phone with password	Refrain from sharing your personal information
Disable location services for social media sites, mobile devices etc.	Consult your relatives and friends, if you think you are a victim of Cyber stalking

ATM Fraud

Fraudulent activity of gaining illegal access to someone's ATM card and PIN to withdraw money from their account

Card Theft Pin Compromise Card Skimming

Cash Reversal Cash Trapping

ATM Fraud Prevention

Cover your hand when you enter ATM PIN	Ensure that no one is peeking while you are entering PIN
Always prefer ATM machine near Bank Branch	Disable your card immediately if it is lost
ATM owner should use high quality security level, branded and top quality machines, latest technology software etc.	Ensure that there is no hidden camera

ATM Fraud

Debit Card or Credit Card Fraud takes place when a fraudster uses a device to tamper an Automated Bank/Teller Machine (ABM/ATM) or Point of Sale payment terminal ('debit machine') to capture data from a payment card and/or Personal Identification Number (PIN); then uses the information to make purchases

Debit and Credit Card Fraud Prevention

Avoid use of debit card to buy things	Check your bank activity regularly
Be careful with store value Apps	Never give your credit card number to anyone
Place a sticker over the security on your card	Avoid free trail offer
Do not forget to sign out from mobile banking	Report fraud immediately

Cyber Safety on the Move

Most vulnerability to cyber attacks when traveling

Safeguarding against Cyber Attack while traveling

Avoid using public WiFi networks	Do not have your device charged from unknown stranger
Do not charge your device from public USB charging stations	Disable Bluetooth connectivity when not in use
Never pick up / attempt to see what's in a USB stick you find lying around	Update your devise OS, Browser, and Antivirus software before travel
Do not share your current location with the world – on Social Media	Use privacy screen on your mobile / laptop

Cyber Safety and Schools

💬 Short Answer submissions (1/3)

Name	Response
Puneeta singh	Yes
Shivani	Yes
Priyanka agarwal	Yes sure
Sita	Yes
Manjusha	Yes

💬 Short Answer submissions (2/3)

Name	Response
Vrushali Gandhi	Yes
Rumki Sengupta	Yes Sir.Very important.
Poonam jha	Yes
NEHA RAJPUT	YES, SIR
Neha bhardwaj	Yes

Short Answer submissions (3/3)

Name	Response
suman singh	yes, as they have sesitive data about students, parents, management
Lucky	Yes
Upasana	Yes.....as school have data of students, parents and teachers.
ESTHER	Students data, parents mail
Anitha kothapalli	It's very important to keep in schools

School Threat Landscape

Cyber threats from outside the school

Criminals

Cyber Threats from inside the school

Students and Staff

Accidental cyber incidents

Like loss of USBs, hard disks

..and many more like Hacktivists seeking to further their agenda / goals by grabbing attention

What are some other sources you'd like to add to this landscape?

Major Areas of Concern

1

Protection of Students

Online threats like cyberbullying, harassment, inappropriate content, identity theft, and online predators

2

Privacy and Data Protection

Schools handle a significant amount of sensitive student data, including personal information and academic records

3

Protection of School Resources

School's digital infrastructure needs to be protected from cyber threats such as malware, viruses and hacking attempts

4

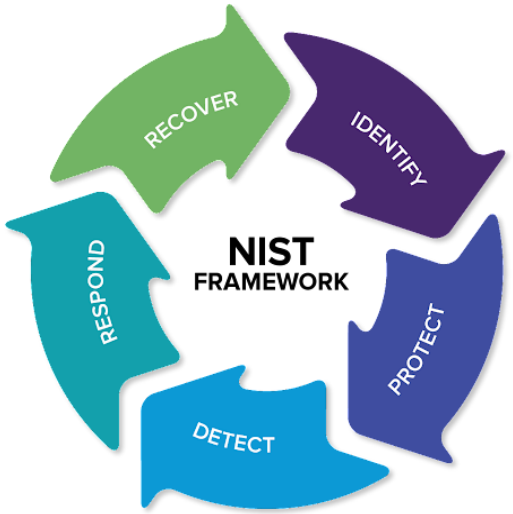
Legal and Regulatory Compliance

By prioritizing cyber safety, schools can meet legal requirements and uphold ethical standards

What Schools need to do?

Schools:

- need to have a Holistic Cyber Resilience Strategy
- can adopt any Cyber Security Framework which provides a systematic approach to cybersecurity like NIST Cyber Security Framework.



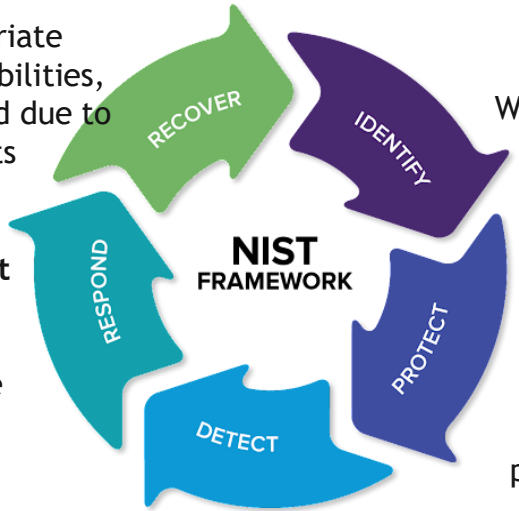
The NIST Cybersecurity Framework identifies five steps which can be taken to avoid cyberattacks

What Schools need to do?

As per the NSIT Cyber Security Framework schools need to

5. Recover – Resuming operations after the attack
Implement the appropriate processes to restore capabilities, services and data impaired due to cybersecurity events

1. Identify – Assessing Risks
What processes and assets need protection?



4. Respond – Mitigating the threat and understanding the adversaries
Develop techniques to contain the impacts of Cybersecurity events, and manage the impact of the cyber incident situation

2. Protect – Reducing the Attack Surface
Implement appropriate safeguards to ensure protection of key information assets

3. Detect – Identifying suspicious and unknown threats
Implement appropriate mechanism to identify the occurrence of cybersecurity incidents

Approach to Teaching Students- Digital Citizenship & being Safe online

Embedding Digital citizenship into the whole school curriculum in an ongoing and authentic way

Adopting effective teaching strategies like story telling, discussion wherein students can be presented with real life scenarios to learn from

By involving parents and community in the awareness programme

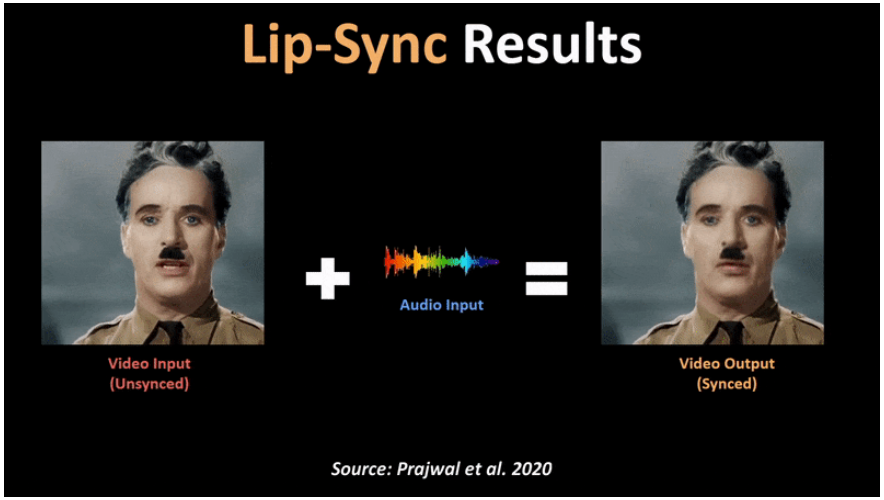
Practical Tips to minimise vulnerability to cyber attacks

- Take ownership at a senior level
- Understand your own culture and bigger risks in the school (is it pupils, staff or an external threat?)
- Establish access control policies
- Ensure that third party providers have a strong cyber security culture
- Use secure configurations
- Encourage reporting and discussion of near misses
- Engage and educate staff, students, parents and community at large
- Follow trusted sites and people to keep up to date

Source: https://www.9ine.com/newsblog/cyber-crime-in-schools#:~:text=The%20three%20biggest%20current%20cyberthreats%20that%20schools%20should%20be%20aware,crime%20and%20cyber%2Ddependent%20crime%3F

What is deepfake AI?

Deepfake AI is a type of artificial intelligence used to create convincing images, audio and video hoaxes. The term describes both the technology and the resulting bogus content, and is a portmanteau of deep learning and fake



https://deepfakesweb.com/

https://www.youtube.com/watch?v=gLoI9hAX9dw

Deepfake videos are still at a stage where you can spot the signs yourself. Look for the following characteristics of a Deepfake video:

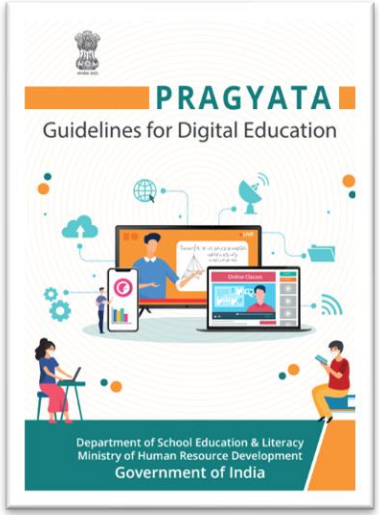
Jerky movement	Shifts in lighting from one frame to the next	Shifts in skin tone
Strange blinking or no blinking at all	Lips poorly synched with speech	Digital artifacts in the image

If your organisation lost access to key infrastructure and systems, could you and your school cope? Do you have a tried-and-true plan in place?

Available Resources

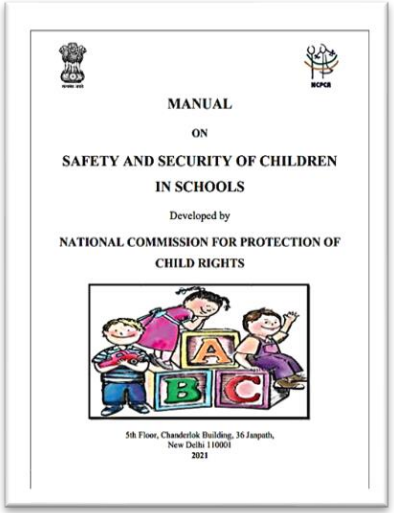
CBSE Resource Material to ensure safe and healthy digital habits among students

Available at https://cbseacademic.nic.in/web_material/Manuals/Cyber_Safety_Manual.pdf



Guidelines by MoE for school heads and teachers describe the need assessment, planning and steps to implement digital education while ensuring cyber safety and privacy measures

Available at: https://www.education.gov.in/sites/upload_files/mhrd/files/pragyata-guidelines_0.pdf



National Commission for Protection of Child Rights (NCPCR) issued guidelines to ensure safety of students including cyber safety

Available at https://ncpcr.gov.in/public/uploads/165650439662bc404c9314e_Manual%20on%20Safety%20and%20Security%20of%20Children%20in%20Schools%20(Sep%202021).pdf

Available Resources

Cyber Safety & Security - CIET-NCERT Resources (in English and Hindi)

https://ciet.nic.in/pages.php?id=booklet-on-cyber-safetysecurity&ln=en

Schools need to take all NECESSARY STEPS and use all these RESOURCES to build AWARE RESPONSIBLE AND EMPOWERED stakeholders

A Few Best Practices

Summary

Your checklist

Review

Review the privacy settings for your social media, professional networking sites and app accounts.

Know

Know who to report any unusual activity to. If you're not sure, ask your line manager or IT team.

Check

Check your device is set to receive updates automatically.

Set

Set a strong password and switch on two-factor authentication, if available, for your most important accounts.

Remove

Remove any apps that have not been downloaded from official stores.

Check

Check that the password for your work account is unique.

Flag it

If it's not possible to follow security advice, process or policy - flag it to your IT team.

Source: https://www.ncsc.gov.uk/information/cyber-security-training-schools

Stay alert and watch out for data thieves getting their hands on your data

5 easy ways to stay protected:

1. Use strong and unique passwords
2. Don't postpone updates
3. Store data in the right folders and drivers
4. Beware off phishing and social engineering attempts
5. Immediately report lost or stolen devices

If you suspect anything is wrong immediately report it to the person responsible for IT

CyberPilot

A long password is a strong password.

password2

x77iLyE#0

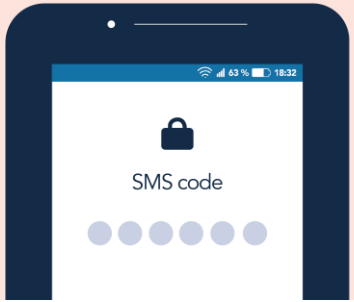
SheLovesITC#You

Number 3 is a good example of a strong password that is also easy to remember. If you want to make it even stronger you can add numbers and punctuation marks, rather than only using words.

CyberPilot

4 tips to better protect your SoMe accounts

1. Protect your devices with a password, pin, and fingerprint.
2. Avoid logging into devices other than your own (e.g., a library computer)
3. Use long and unique passwords for all your accounts
4. Activate multi-factor authentication for all your accounts



CyberPilot

Source: https://www.cyberpilot.io/free-gdpr-and-cyber-security-posters

What is the website mentioned as the source for free GDPR and cyber security posters?

A. cyberpilot.io

B. GDPRposter.com

C. securityposters.net

D. cybersecuritysource.com

 Answer

Correct answer: A

Multiple Choice

4 steps to better and safer video conferences

Be aware of which services are approved for video conferences in your workplace

Close unecessary files, windows, and applications that you don't want to share on your screen

If another participant is sharing too much, kindly bring it to their attention

Only share what is necessary on your screen. E.g., a specific window instead of the entire desktop

CyberPilot

3 tips for if you suspect a phone scam

1. Consider whether the information you are providing can be abused in any way.
2. Always be polite, but remember to set clear boundaries on how far you are willing to go.
3. If you are being pressured in any way, cut the conversation short by taking a time-out.

CyberPilot

Avoid being hacked on social media

Do not 100% trust anyone on social media. Even the people you know may have had their account taken over by a hacker.

If you suspect that someone in your network has been hacked, remember that you cannot confirm the person's identity by writing back. Instead, contact the person through other channels, e.g., by calling them on the phone.

Mult-factor authentication is the best defence against having your accounts hacked into by cybercriminals.

CyberPilot

Source: https://www.cyberpilot.io/free-gdpr-and-cyber-security-posters

04 Cyber Security

Initiaives in India

Counter Cyber Security Initiatives in India

Computer Emergency Response Team-India(CERT-In)	National Critical Information Infrastructure Protection Centre (NCIIPC) of India	Cyber Swachhta Kendra
National Cyber Coordination Centre (NCCC)	Cyber Surakshit Bharat	National Cyber Security Policy
Personal Data Protection Bill	National Crime Records Bureau (NCRB)	Data Security Council of India (DSCI)

Lodging a Complaint

In case your compromised email account has been used to send mails

01

- Take a print-out of the alleged mail along with full headers
- Take full header only from the first receiver's email account (not from the forwarded ones)

02

- Collect documentary evidence (e.g. screenshots, bank transaction statements, etc.) of the misuse of the hacked account

03

- Lodge a complaint at your nearest Police Station detailing the complete incident along with the above documents

04

- Save a copy of all the above mentioned documents in soft form and provide them to the Police Station investigating Officer on a CD-R.

A complaint can be lodged on
https://cybercrime.gov.in/

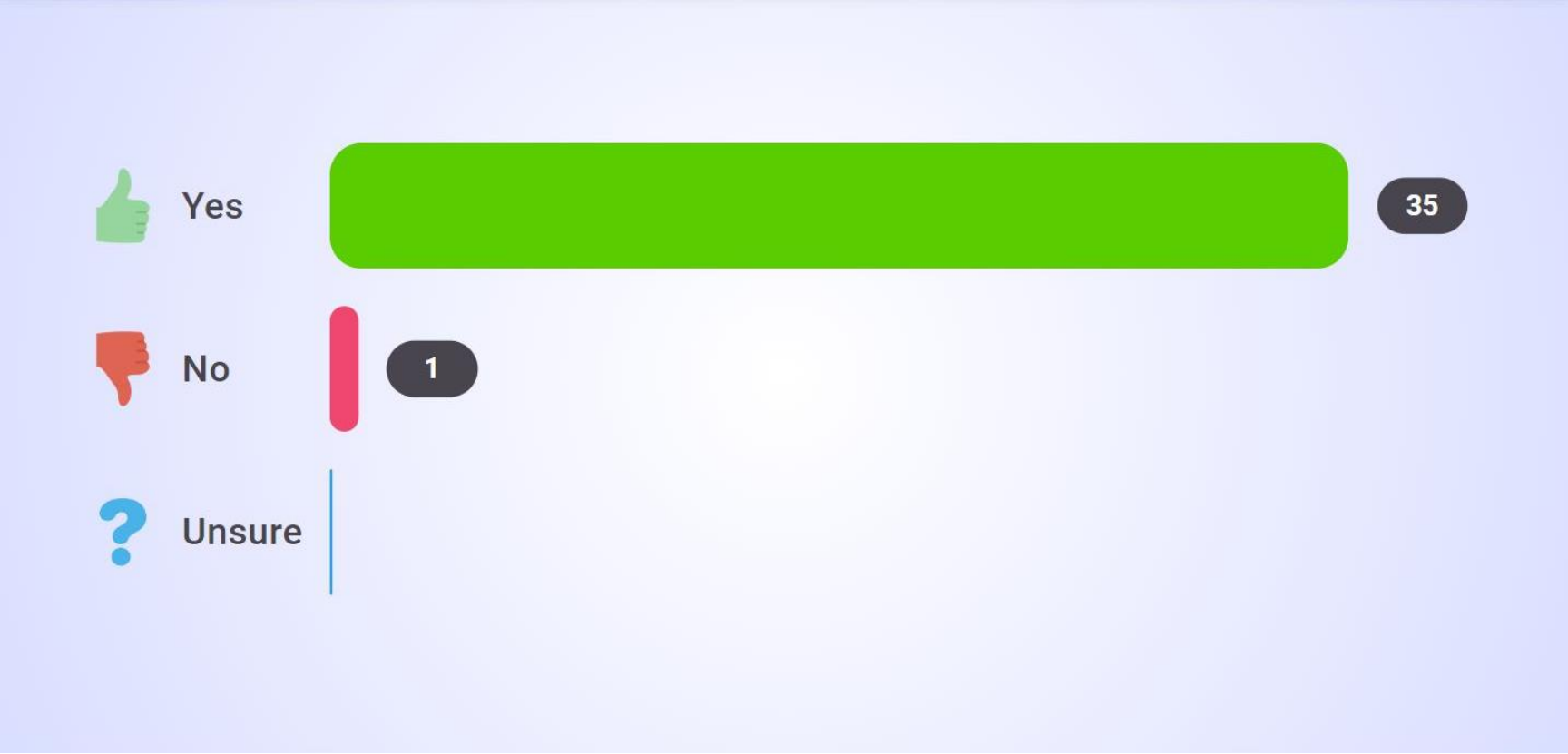
https://staysafeonline.in/

Stay Safe Online Campaign

To raise awareness to among citizens to stay safe in the online world

Dissemination of multilingual awareness content in the form of infographics, cartoon stories, puzzles, short videos, etc.

Quick Poll submissions



Follow Ethical Online Behaviour

Cyber Ethics

Acceptable behavior standards to be followed while using the internet; helps stay safe online by setting up a set of moral principles that govern the usage of Computers and Internet

https://staysafeonline.in/

Quick Poll submissions

Acceptance

Action of consenting to receive or undertake what Internet offers as it belongs to everyone and there is no barrier of national and local cultures

Sensitivity to National and Local cultures

Be aware, sensitive, thoughtful and understanding about the differences in the national and local cultures of the netizens you meet in an online world

Ethics while using Email & Chatting for Communication

Do not use internet chatting for communicating with strangers and do not forward the emails from strangers

Do not pretend to be someone else on digital space

Adopt trustful and truthful means of interaction & communication to promote a healthy, vibrant, positive cyber space

Avoid using bad language on public platforms

Do not to be rude or use bad language while using email communication, chatting, blogging and social networking

Source: https://staysafeonline.in/

Which of the following platforms should you avoid using bad language on?

A. Email communication

B. Social networking

C. Shopping online

D. Reading books

 Answer

Correct answer: B

 Multiple Choice

Protection of Personal Information

Ensure protecting your sensitive personal information and restrict sharing information to anyone on public platforms

Be careful while accessing online content & app downloads

Be aware of copyright policy and be careful to follow it downloading applications, music, software etc.

Supervision of the Internet usage

Supervise internet usage & take appropriate guidance from aware members, regarding acceptable, ethical & secure ways of accessing the internet

Encouraging safe usage of internet

Safe usage of internet should be encouraged among people for optimum utilization of its benefits for progress and growth

Accessing Internet

Be cautious while accessing the internet

Source: https://staysafeonline.in/

CYBER-SAFETY ACTIONS

1. Install OS/Software Updates

2. Run Anti-virus Software

3. Prevent Identity Theft

4. Turn on Personal Firewalls

5. Avoid Spyware/Adware

6. Protect Passwords

7. Back up Important Files

Short Answer from garima

What is a logic bomb?
A logic bomb is a string of malicious code inserted intentionally into a program to harm a network when certain conditions are met.
Unlike many other types of cyber attacks, a logic bomb attack is subtle yet often sophisticated and capable of causing explosive damage that's difficult to trace or mitigate. A malicious piece of code is secretly inserted into a computer's or network's existing software. It may also be inserted into other forms of malware such as viruses, worms or Trojan horses.
A logic bomb is sneaky because its code lies dormant until the trigger occurs.
If the trigger is related to a date or time, the logic bomb will go off on a certain date -- e.g., Y2K -- and is known as a time bomb.
In order to maximize damage before being noticed, logic bombs are mainly used with trojan horses, worms, and viruses. The primary objective of logic bombs is to reformat a hard drive, modify or corrupt data, and remove important files from the system. The devastation caused by a logic bomb can be a huge level.
Characteristics of a logic bomb virus
There are multiple characteristics of a logic bomb, which are as follows:
1. It is dormant for a set period of time: Logic bombs can go undetected for a long time of period and are subtle.
2. Its payload is unknown until it triggers:
3. It's triggered by a certain condition:
EXAMPLE -In late 2001, a systems administrator quit his job at UBS and only hours later bought numerous "put" options that would allow him

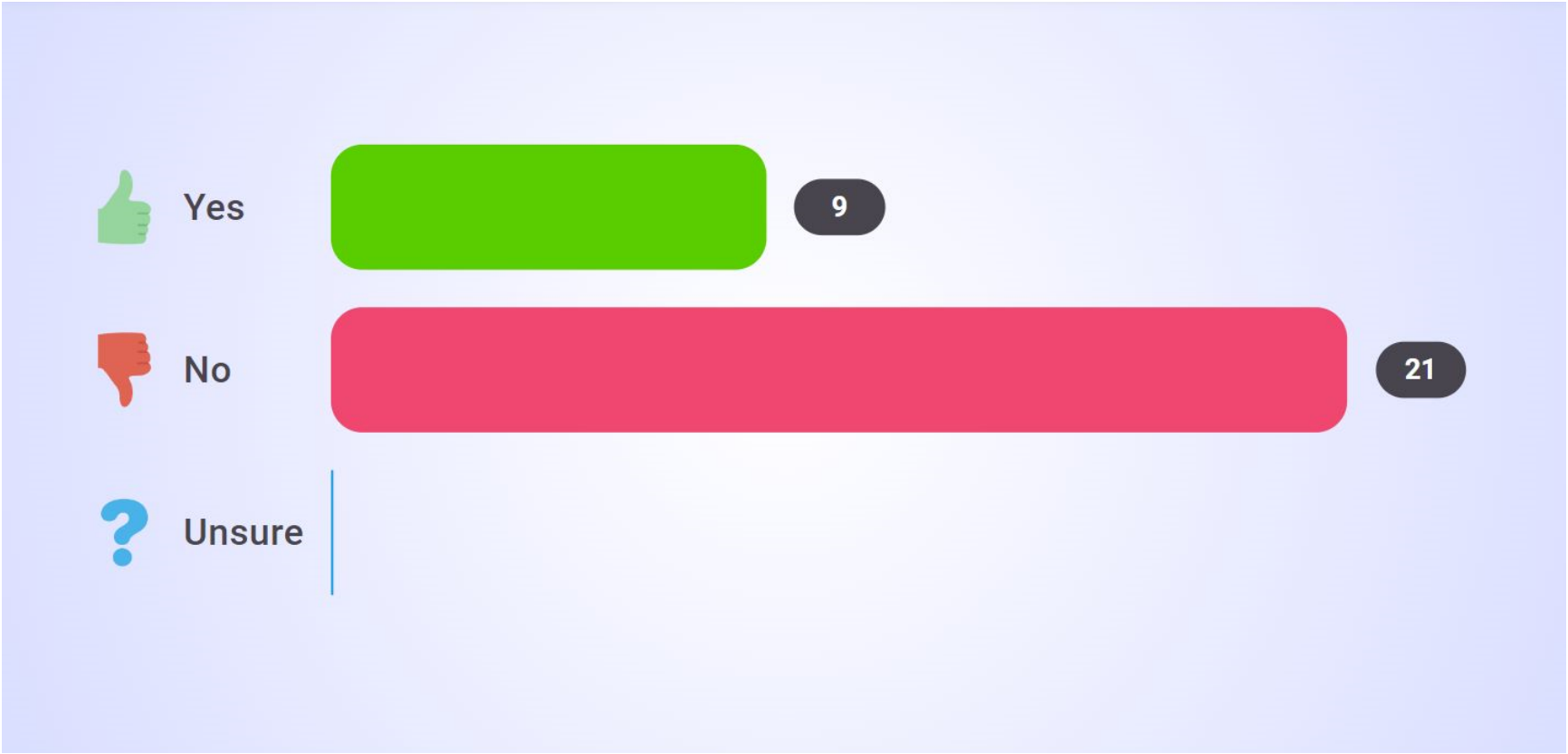
Tools and Web resources

- https://infosecawareness.in/teacher
- https://isea.gov.in/
- https://ciet.nic.in/upload/Cyber_safety_for_schools_new.pdf
- https://www.csk.gov.in/
- https://www.ibm.com/topics/nist
- www.Whatismyip.com
- https://haveibeenpwned.com/

Some Practical tips

- Pad Lock
- Mailtrack
- Check whether my Email is compromised or not
- To see google chrome passwords
- Password Generator

Quick Poll submissions



Feedback

💬 Short Answer submissions (1/14)

Name	Response
Archana Misra	Good workshop
Anita Thomas	The session was very informative and helpful.
Loyla Leo Joseph	Very informative, interactive & engaging.
Govind Singh	Session is really helpful. Thanks a lot for this session.
Prajakta	It was wonderful and eye opener too

💬 Short Answer submissions (2/14)

Name	Response
T Suanlian Tonsing	rhnk you sir... haveibeenpawned was enlighting
Anshu Singh	Interesting session
Rekha Inda	Very useful information thankyou so much sir🙏 😊
Yash Domadiya	Thank You for Guidance Sir,Very Informaative...Session.
Neha Pal	Informative session

💬 Short Answer submissions (3/14)

Name	Response
Prabhleen Chauhan	Excellent session!!
Dipal	It was very amazing session.
Sheetal phogat	NYC rules and security
Shyamli	Awesome
Ritika Joseph	Very informative and innovative session. Thank you sir.

💬 Short Answer submissions (4/14)

Name	Response
Tanvangi	Amazing session A wide variety of information was shared Thank you so much
Pinki	Very informative session. Very new things I have learnt today about cyber security
Anusha	Very very informative and useful to teachers personally as well as to educate the children who spending most of the time in gadgets
Vidhi	Session was very informative
Priya sukhija	It was a wonderful session and brief and summarize

💬 Short Answer submissions (5/14)

Name	Response
Manmeet Katyal	Very informative and we will try definitely to teach the students about the same.
Sneha Roy, Jharkhand	Excellent,understandable and full of knowledge
Divya Sharma	It is a great session, I learnt so many things from this session.Thank you for making a part for of this
Madhuri kachhiya	CYber safety attack' is very informative nd useful
Shefali, Jodhpur	Absolutely amazing sir.got to know many new things

💬 Short Answer submissions (6/14)

Name	Response
Shahi gulshanar ahmed	Very good Sir, needy information ,thank you so much Sir for your meaningful time with us
Radha Sharma	Session was very helpful.Thank you sir
Nitin Goyal	The Session is so much imformative & You also sir.
Monika Shekhawat	Session was very informative & relevant in today's context.
Shahi gulshanar ahmed	Very good Sir, needy information ,thank you so much Sir for your meaningful time with us

💬 Short Answer submissions (7/14)

Name	Response
Sunil agrahari	It's amazing information, I'm surprised to know so many things about this. Thx
SUMIT	Session is very interactive, knowledge and helps to avoid cyber frauds and crime which are quite common in digital era
Mitakshra	Very informative
Garima	It was very helpful and knowledful for us sir .By this we can save ourselves from getting cheated online . Thank u sir
Nikhil Agarwal Jaipur raj	It was an understanding session for us to get aware of cyber safety and security.

Short Answer submissions (8/14)

Name	Response
Manju Sharma	It was very nice and educative session.
Chitra Sehgal	Very informative and knowledgeable session sir Thank you so much sir
DIVYA ARORA	It was informative and very uesful.Thank you sir
Roshani Yadav	wonderful session
Farah Jharkhand	I really liked the session and got very much useful information

💬 Short Answer submissions (9/14)

Name	Response
Pooja Kumari	This session is very good and informative I want more session like this
Tejal Trivedi	Happy i learnt so many things from u r concept
Priya pahuja	Meaning ful session
Darshana patil	It is so much informative.
Hitesh Gujarat	It was a great experience which enhanced my knowledge in cyber security.

💬 Short Answer submissions (10/14)

Name	Response
PRAVEENA	GOOD SESSION ,INFORMATIVE
Shamla shajahan	Session was amazing and very very informative.it helped me to have good knowledge which is very useful nowadays.
BHARAT KATARIYA	Excellent
Monica Tiwari	Sir , Your hard for preparing the workshop is really commendable. I loved and enjoyed this workshop. Thakyou
Muskan Mishra	The best part was that we got chances to interact . Other sessions are just slide show with lengthy theoretical slides. You shared real life examples that was amazing . I learned a lot . Just a question how to set privacy screen?.. as you mentioned while travelling we should use that.

💬 Short Answer submissions (11/14)

Name	Response
Kartika Nair	Very informative section
Harjinder kaur	It really was a good session, i have learnt many more things about cyber security and how to avoid cyber crime.
Debajit Paul	It was really nice session. Learned a lot of new things and improved my views on lot topic on keylogging and the ways I can be attacked only. The website mentioned at the end where really good and I will try to implement in my life and school and try to make our environment free from cyber attacks.
Anshu Mathur	Very helpful
Mayuri Joshii	The session was meaningful. I learned so many new things about cyber security today.

💬 Short Answer submissions (12/14)

Name	Response
Manila Sankhla	Very supported
Priyanka Rai	Good evening sir.... It was really very good informative session and most of all for me as I am not so much digital savvy .... Thank you. And the stars which I have received that was so encouraging
Mukul	Session was really good.
Bindiya Rana, Rajasthan	Very informative session. I learned a lot from you as I was so worried about these threats, whenever I heard this. Thanks a lot Sir.
Reshma Hasim	It was a very useful class..Thank you so much for giving us tips for being safe in this cyber world...

💬 Short Answer submissions (13/14)

Name	Response
Shyam Lal Agrawal	It is very important session for present conditions. Understanding and helpful.
Farheen Bangalore	Awesome session, very informative.
Shumaila Mazhar	It was awonderful session we learnt a lot.
SOHINI SARKAR	Nice session. Thank you sir.
Babita Kanwar	Content was very helpful in creating awareness about cyber security.

💬 Short Answer submissions (14/14)

Name	Response
Sangeeta pal	Very good session and nice session.i have learnt so many things.
Priyanka Masih	Wonderful session

Short Answer submissions (1/6)

Name	Response
Disha mule	sir let me clear my point I literally like your session but in between my baby was Interrupting me that's why it marked as no...
Manju Joshi	Very informative session
Moorthy	Very informative..
subhash	very nice sir
BRATATI ROY CHOUDHURY	Excellent .became aware

💬 Short Answer submissions (2/6)

Name	Response
Gayathri Jiju	session was really informative
Pramila	A very informative session indeed
Pooja Sethi	Nice session thank you sir 🙏 🙂
Krunali Prajapati	Learnt a lot sir, very informative enjoyed this. Very interactive
Iqra noor	very informative . Superb session

💬 Short Answer submissions (3/6)

Name	Response
Kavita Yadav	Nice session.
DAAN SINGH BISHT	The session was really interesting.
Apoorwa Bhatnagar	It was a nice session very much informative thanks for the great session
Shwetimasingh	Very informative...
JAYEETA CHAKRABORTY	liked the session a lot. thanks for providing such valuation information .

💬 Short Answer submissions (4/6)

Name	Response
Zainab Firdouse	Need more sessions of this type...very informative
ANURAG KUMAR	Very nice session sir.
SUSHMITA SUMAN	Awesome Session sir....Thank you sir
Rachna Sharma	Excellent session
Soumya Soman	Very informative . Sir it is a new awareness that don't use public wifi 😁

💬 Short Answer submissions (5/6)

Name	Response
Arushi Agarwal	Thank you sir, for the knowledgeable and wonderful session.
Lily Acharya	Very nice session sir thank you
Sayani Mazumdar	Really an informative and interactive session. Loved your session Sir. Came to know a lot about Cyber Security and how to overcome the cyber threats effectively
Namita	Thank you Naveen Sir, for a very informative, interesting and interactive session.
Nirman kaur	This session was really knowledgeable . I enjoyed and learned many things thank u so much sir

Short Answer submissions (6/6)

Name	Response
RANBIJAY KUMAR RATNESH	Really it was a very good and informative session. I hope it will definitely help us to make our students aware about cyber security and threats. Thanks

Key Messages

Be a good Digital Role Model	Be aware and educate your students of dangers and threats in digital space	Be aware of guidelines and policies
Educate yourself regularly / stay informed	Always log out / off your account	Upload appropriate documents and videos with due permissions
Practice open communication - have open talks, share & discuss	Never store, share and distribute your password and files	Think before you share. What you share can take life of its own
Be Ready to Learn, Unlearn and Relearn	Do not look at on others' information without permission	Check your account settings regularly
Hold open & effective discussion on proper use of digital resources	Use your own device to copy and to publish	Create Awareness for cyber security

Did you know?

The I.T. Act contains **13 chapters** and **90 sections**.

Offences included in the I.T. Act 2000

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Salient Features of I.T Act

- Digital signature has been replaced with electronic signature to make it a more technology neutral act.
- It elaborates on offenses, penalties, and breaches.
- It outlines the Justice Dispensation Systems for cyber-crimes.
- It defines in a new section that *cyber café is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public*.
- It provides for the constitution of the Cyber Regulations Advisory Committee.
- It is based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.
- It adds a provision to Section 81, which states that the provisions of the Act shall have overridden effect. The provision states that *nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957*.

Section	Offence	Punishment	Bailability and Congizability
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs	Offence is Bailable, Cognizable and triable by Court of JMFC.
66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs	Offence is Bailable, Cognizable and
66-A	Sending offensive messages through Communication service, etc...	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable and triable by Court of JMFC

66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-D	Cheating by Personation by using computer resource	Imprisonment of either description up to 3 years and /or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC

66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life	Offence is Non-Bailable, Cognizable and triable by Court of Sessions
67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC

67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form	On first Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC
67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first Conviction imprisonment of either description up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment of either description up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non Bailable, Cognizable and triable by Court of JMFC
67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.

Source: https://www.tutorialspoint.com/information_security_cyber_law/offences_and_penalties.htm

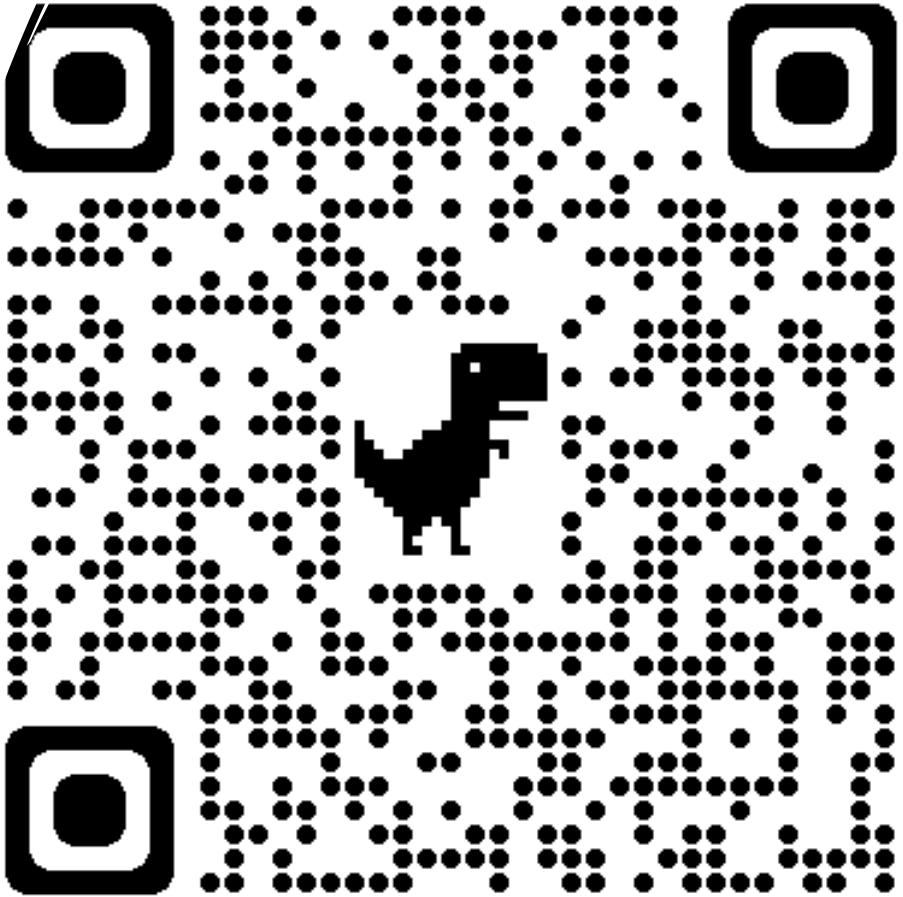
Q & A

Follow me:

- https://www.youtube.com/channel/UCCewPojFWnn5pzQ_KOTKxVQ
- https://www.facebook.com/naveen.gupta1/
- https://www.linkedin.com/in/naveenguptacomputer/
- https://twitter.com/naveengupta1
- https://wakelet.com/@NaveenGupta429

- https://linktr.ee/naveen.gupta

WHATSAPP CHANNEL LINK



Thank You