Cybersecurity
साइबर सुरक्षा

- **Understanding Digital Threats** डिजिटल खतरों को समझना
- **Recognizing Cyber Threats** साइबर खतरों की पहचान करना
- **Incident Response & Recovery** ऑनलाइन मुश्किलों का सामना करना
- **Building Digital Resilience** डिजिटल सहनशीलता विकसित करना

UNNATI WELFARE SOCIETY

Understanding Digital Threats
Building Foundation Knowledge

मूलभूत ज्ञान का निर्माण करना
डिजिटल खतरों को समझना

UNNATI WELFARE SOCIETY

Why Cybersecurity Education Matters NOW?

Alarming Statistics for India's Education Sector

भारत के शिक्षा क्षेत्र से जुड़ी चौंकाने वाली सांख्यिकीय जानकारी

8,195

cyberattacks per week on educational institutions

प्रति सप्ताह शैक्षणिक संस्थानों पर 8,195 साइबर हमले।

2x

More than DOUBLE the global average (3,355)

वैश्विक औसत (3,355) से दो गुना से भी अधिक — यानी 2 गुना ज्यादा।

3x

Students aged 21329 are 3x more likely to fall for scams

आयु 21 से 29 वर्ष के छात्र स्कैम का शिकार होने की संभावना में 3 गुना अधिक होते हैं।

7,00,00,000

Average ransom demand: ($847,000)

औसतन फिरौती की मांग: $847,000 (लगभग ₹7 करोड़)

75%

of attacks start with phishing emails

75% साइबर हमले फिशिंग ईमेल से शुरू होते हैं।

37%

Educational attacks increased by 37% in 2024

शैक्षणिक संस्थानों पर साइबर हमलों में 2024 में 37% की बढ़ोतरी हुई।

Real Story:

Kabir, an 11-year-old who loved mobile games, saw a video titled:
"Download this secret app to unlock all levels for free!"
Excited, he clicked the link and downloaded the app from a random website—not the Play Store. Right after installing it, his phone started acting strange. Weird messages popped up, and his screen kept freezing. Later, his dad noticed that money was missing from his bank account, which was linked to the phone. The app Kabir downloaded had installed a dangerous virus that stole information from the phone.

What We Learn:

- ✓ **Never download apps from unknown websites.**
  कभी भी अनजानी वेबसाइटों से ऐप डाउनलोड न करें।
- ✓ **Use only trusted sources like the Play Store or App Store.**
  हमेशा केवल भरोसेमंद स्रोतों जैसे Play Store या App Store से ही ऐप डाउनलोड करें।
- ✓ **Always ask an adult before installing anything.**
  कुछ भी इंस्टॉल करने से पहले हमेशा किसी बड़े से पूछें।

A single wrong click can risk your data, your device—and even your family's money.
सिर्फ एक गलत क्लिक से आपका डेटा, आपका डिवाइस — और यहां तक कि आपके परिवार के पैसों तक को खतरा हो सकता है।

What is Cybersecurity?

Protecting our digital world from bad actors

हमारे डिजिटल दुनिया को बुरे तत्वों से सुरक्षित रखना

Think of it like home security, but for computers and internet

What We Protect:

- **Personal Information (photos, messages, passwords)**
  व्यक्तिगत जानकारी
- **Financial Data (bank accounts, payment cards)**
  आर्थिक जानकारी
- **Academic Records (grades, certificates)**
  शैक्षणिक रिकॉर्ड
- **Family Privacy (addresses, phone numbers)**
  परिवार की गोपनीयता

Your Digital Footprint

Everything you do online leaves a trace - like footprints in sand

आप जो कुछ भी ऑनलाइन करते हैं, वह एक निशान छोड़ता है — जैसे रेत में पैरों के निशान।

What Creates Your Digital Footprint:

- Social media posts and comments
  सोशल मीडिया पर की गई पोस्ट और टिप्पणियाँ
- Search history and websites visited
  सर्च हिस्ट्री और देखी गई वेबसाइटें
- Online purchases and downloads
  ऑनलाइन की गई खरीदारी और डाउनलोड भी निशान छोड़ते हैं।
- Emails and messages sent
  भेजे गए ईमेल और संदेश भी निशान छोड़ते हैं।

Once online, it can be there FOREVER

Password Power

Passwords are like keys to your digital house
पासवर्ड आपके डिजिटल घर की चाबी की तरह होते हैं।

WEAK Password Examples:
123456, password, your name, your birthday

STRONG Password Recipe:
- ✓ Mix uppercase and lowercase letters
- ✓ Add numbers (but not just at the end!)
- ✓ Include special characters (!@#$%)
- ✓ Make it at least 12 characters long

इस तरह का पासवर्ड तोड़ना बहुत मुश्किल होता है।
सुरक्षित रहें, स्मार्ट रहें

Two-Factor Authentication (2FA)

Double protection = Double security
2FA = एक और ताला आपकी डिजिटल दुनिया के लिए

What is 2FA?

Something you KNOW (password) +
Something you HAVE (phone)
कुछ जो आप जानते हैं – पासवर्ड
कुछ जो आपके पास है – मोबाइल फोन

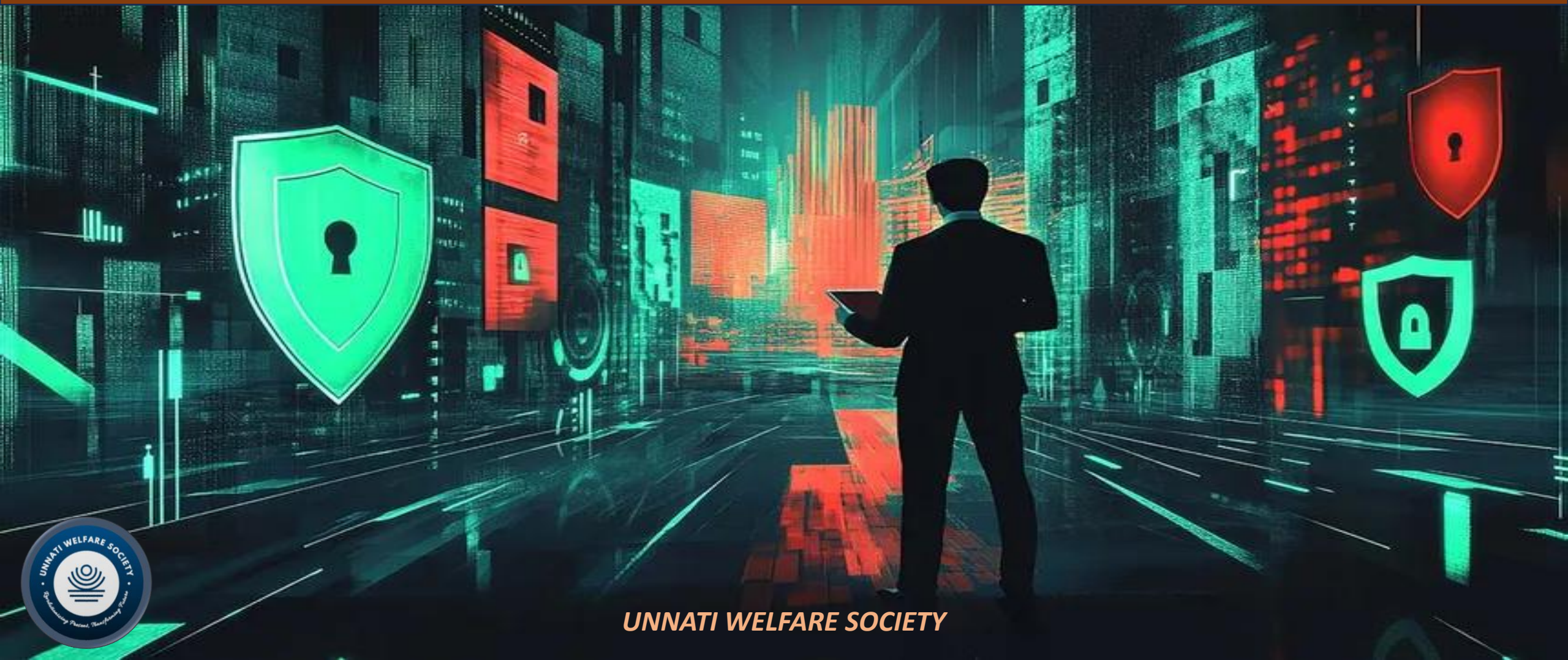
How it works:

1. Enter your password
   पासवर्ड दर्ज करें
2. Receive code on your phone
   अपने फोन पर एक कोड प्राप्त करें
3. Enter the code to login
   लॉगिन करने के लिए वह कोड दर्ज करें

Enable 2FA on: Email, social media, gaming accounts

Recognizing Cyber Threats
Know Your Enemy

साइबर खतरों को पहचानना
अपने दुश्मन को जानो



UNNATI WELFARE SOCIETY

Payment Frauds & Scams
भुगतान धोखाधड़ी और ठगी

Online Blackmail & Sextortion
ऑनलाइन ब्लैकमेल और सेक्सटॉर्शन

Ransomware Attacks
रैंसमवेयर हमले

Malicious Links & Phishing
हानिकारक लिंक और फिशिंग

Social Engineering Tactics
सोशल इंजीनियरिंग की चालें

Payment Frauds & Scams

भुगतान धोखाधड़ी और ठगी

How scammers target students' money:

Fake Scholarship Offers

फर्जी स्कॉलरशिप ऑफर

- Asking for 'processing fees' upfront

प्रोसेसिंग फीस" के नाम पर एडवांस में पैसे मांगते हैं

Fraudulent Textbook Sales

फर्जी टेक्स्टबुक सेल

- Too-good-to-be-true prices for expensive books

महंगी किताबों को बहुत ही सस्ते दाम पर देने का वादा

Fake University Communications

फर्जी यूनिवर्सिटी मैसेज या ईमेल

- Urgent fee payments through 'special' methods

फीस भुगतान के लिए खास लिंक या UPI आईडी भेजना

Protection: ***Always verify through official channels***

हमेशा ऑफिशियल वेबसाइट से ही जानकारी लें

True Story:
A Student Got Tricked

Ravi, a school student from a village, got a message on Facebook:
"You will win a mobile phone and scholarship. Just send ₹500 for registration."
Ravi asked his father for money and sent ₹500 by UPI.
Then they asked for ₹1,000 more to "confirm the prize."
Ravi sent it — but after that, the number was switched off.
No mobile. No scholarship. Just a loss of money.

What We Learn:

- ✓ Never send money to unknown people online.
- ✓ Real prizes or scholarships don't ask for payment.
- ✓ If you feel unsure, tell your parents or teachers immediately.
- ✓ If you are scammed, call 1930 or report at cybercrime.gov.in

Online Blackmail & Sextortion

किसी व्यक्ति को इंटरनेट के माध्यम से डराकर, धमकाकर या उसकी निजी जानकारी/तस्वीरों का दुरुपयोग करके पैसे या अन्य लाभ लेने की कोशिश करना।

WARNING: Predators target teenagers online

चेतावनी: ऑनलाइन शिकारी किशोरों को निशाना बनाते हैं

How it starts:

- Friendly stranger sends friend request
  कोई अनजान व्यक्ति दोस्ती का अनुरोध भेजता है
- Builds trust over time
  धीरे-धीरे विश्वास बनाता है
- Requests personal photos/videos
  निजी फ़ोटो/वीडियो की मांग करता है

NEVER comply with demands for:

Personal photos, money, or meeting in person

ध्यान रखें! कभी भी इन बातों के लिए हां न कहें: निजी तस्वीरें, पैसे, या आमने-सामने मिलना।

If this happens: ***Tell a trusted adult IMMEDIATELY***

तुरंत किसी भरोसेमंद बड़े को सब कुछ बताएं।

UNNATI WELFARE SOCIETY

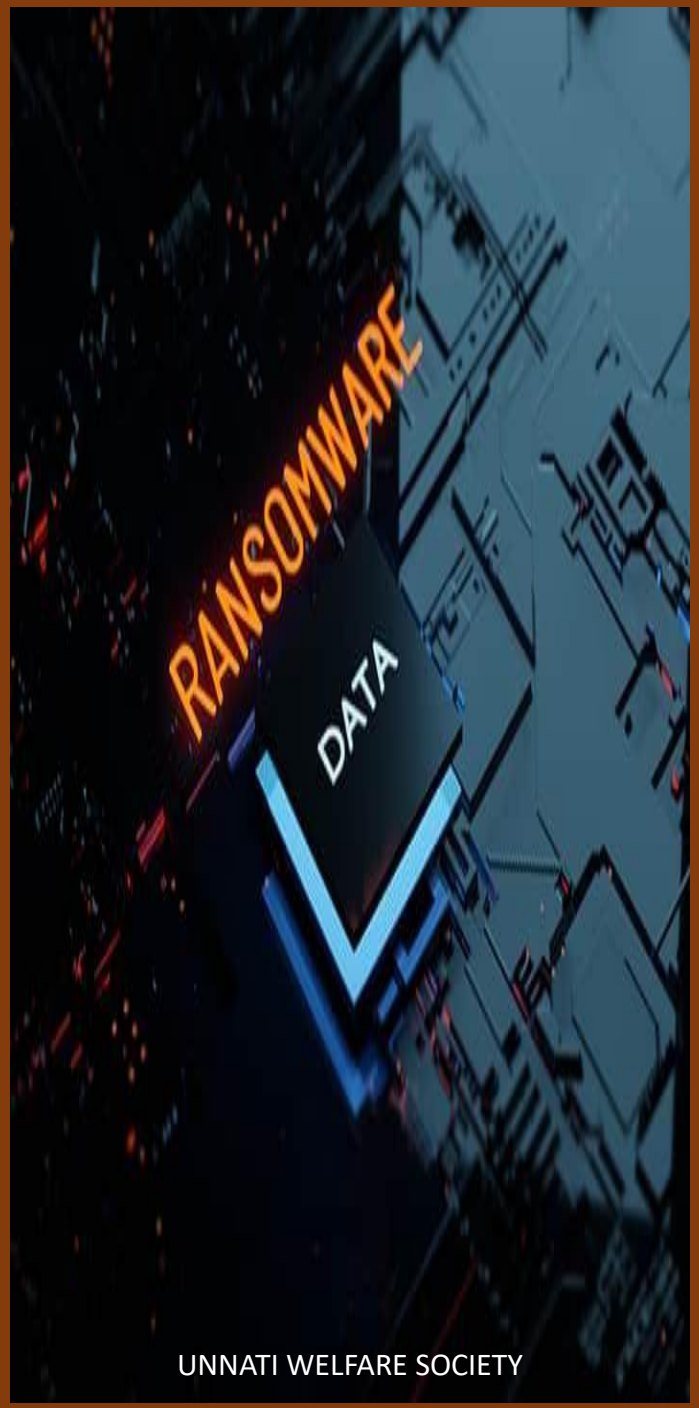
Real Story:
A Boy Got Tricked Online

Raju, a class 8 student, made a new friend on a mobile game.
The person said, "Let's be friends on WhatsApp too."
They started chatting every day. One day, the person said,
"Send me a funny photo of yourself without a shirt."
Raju trusted them and sent the photo. Next day, the same person said: "Now send more photos — or I will send this to your friends and teacher!"
Raju got scared and didn't know what to do.
Luckily, he told his older cousin, who called 1930 (Cyber Helpline), and reported it.

It can be even more serious.

What We Learn:

- ✓ Never share personal photos or videos online.
- ✓ Don't talk privately with strangers on games, WhatsApp, or Instagram.
- ✓ If someone makes you uncomfortable, tell your parents, teachers, or elder siblings.
- ✓ If you're in trouble, call 1930 or go to cybercrime.gov.in



UNNATI WELFARE SOCIETY

Ransomware Attacks

रैनसमवेयर एक प्रकार का खतरनाक सॉफ़्टवेयर (मालवेयर) होता है, जो आपके कंप्यूटर या मोबाइल की फ़ाइलों को लॉक कर देता है और उन्हें वापस पाने के लिए फिरौती (ransom) की मांग करता है।

Malicious software that locks your files for money

Real Impact on Schools:

- Classes Disrupted – No access to online lessons or study material.
  कक्षाएं बाधित या पढ़ाई में रुकावट
- Loss of Academic Records – Grades, assignments, and exam data may be lost.
  पढ़ाई से जुड़े दस्तावेज़ों का नष्ट होना
- Data Breach – Personal info (name, address, ID) can be stolen or leaked.
  डेटा चोरी

How ransomware gets in:

- Malicious email attachments वायरस युक्त ईमेल अटैचमेंट
- Infected websites and downloads वायरस से भरी वेबसाइटें और डाउनलोड फ़ाइलें

Prevention: ***Don't click suspicious links***
संदिग्ध लिंक पर क्लिक न करें

Real Story: Ransomware Attack in a School Computer Lab

In a school in Bangalore, students were learning computers. One day, a student downloaded a free game from a random website.
Next morning, the computer lab screens all showed this message:
"Your system is locked. Send $500 in Bitcoin to unlock your files."
The computers had been infected with ransomware.
Important files — like class notes, homework, and student data — were locked. Even teachers couldn't open anything.
The school had to call cyber experts and stop computer classes for a week.

What We Learn:

- ✓ Never download games or apps
- ✓ Don't click on strange links or open unknown email attachments
- ✓ Always ask your teacher or parents
- ✓ Use antivirus software and keep it updated

Malicious Links & Phishing

हानिकारक लिंक और नकली ईमेल, मैसेज या वेबसाइट के ज़रिए आपकी निजी जानकारी जैसे पासवर्ड, बैंक डिटेल आदि चुराने की कोशिश।

Phishing = Fishing for your personal information

Common Phishing Tactics:

- Urgent messages: 'Your account will be closed!'

  जल्दबाज़ी पैदा करना

- Too good to be true: 'You won $1000!'

  लालच देना

- Fear tactics: 'Your computer is infected!'

  डराना

Red Flags to Watch For:

- Spelling mistakes in emails
  ईमेल में वर्तनी की गलतियाँ
- Suspicious sender addresses
  संदिग्ध भेजने वाले का पता
- Urgent demands for personal info
  निजी जानकारी की जल्दी मांग

Real Story:

The Dangerous Link

Arjun, a class 10 student, received an email that looked like it was from his school principal. It said:
"Click the link to download your exam timetable."
The email had the school logo and even the principal's name — so Arjun clicked the link without thinking. But the link took him to a strange website that asked him to log in with his Google account password. He entered it.
Later that day, Arjun's email was hacked, and strange messages were sent to his friends from his account.
He immediately told his teacher. The school's IT team helped him secure his account and report the incident.

What We Learn:

- ✓ **Check the sender carefully** — not all emails are real, even if they look familiar.
- ✓ **Don't click on links** unless you're 100% sure they're safe.
- ✓ **Never enter your password** on unknown websites.
- ✓ **Tell an adult immediately** if something unusual happens with your account.

Social Engineering Tactics

सोशल इंजीनियरिंग एक साइबर हमला है जिसमें हैकर आपके दिमाग से खेलते हैं

मतलब, आपको धोखे से जानकारी देने या कुछ गलत करने के लिए मनाते हैं।

Manipulating people to reveal information

Common Techniques Targeting Students:

- Pretending to be from your school

  स्कूल का स्टाफ बनकर बात करना
- Claiming to be authorities (police, government)

  खुद को अधिकारी बताना (पुलिस/सरकार)
- Creating fake emergencies

  नकली आपात स्थिति बनाना
- Offering free gifts or money

  फ्री गिफ्ट या पैसा देने का झांसा

Defense Strategy: ***STOP - THINK - VERIFY – ACT***

रुको - सोचो - जांचो - फिर कदम उठाओ

Real Story:

The Fake Phone Call Trick

Rani, a class 8 student, got a call on her mother's phone one evening. The caller said: "I'm calling from your school's office. We lost your exam record. Please tell us your student ID, date of birth, and your father's name." Rani thought it was real because the person knew her name and school. She shared all the details.
Later, her father received a message that someone tried to log into their bank account using that information.
It was a social engineering trick — the caller pretended to be someone trustworthy to steal personal data.
Her parents reported the call to the cyber helpline 1930

What We Learn:

- ✓ **Social engineering means tricking people** by pretending to be someone you trust (like school staff or relatives).
- ✓ **Never share personal details** like birthdate, address, or account info over calls or messages.
- ✓ **Think before you trust** — even if the person knows your name or school.
- ✓ **Always tell parents or teachers** if someone asks you for information online or on the phone.

Incident Response & Recovery When Things Go Wrong

साइबर हमले के बाद की प्रतिक्रिया और समाधान

UNNATI WELFARE SOCIETY

Emergency Response Framework

आपात स्थिति में अपनाने की प्रक्रिया

The STOP-THINK-CONNECT Method

STOP

Don't panic or make quick decisions
(घबराएं नहीं और जल्दीबाज़ी में निर्णय न लें)

Disconnect from internet if needed
(ज़रूरत पड़ने पर इंटरनेट से डिस्कनेक्ट करें)

THINK

What exactly happened?
(वास्तव में क्या हुआ है?)

What information might be at risk?
(कौन सी जानकारी खतरे में हो सकती है?)

CONNECT

Tell a trusted adult immediately
(तुरंत किसी भरोसेमंद बड़े को बताएं)

Report to appropriate authorities
(संबंधित अधिकारियों को रिपोर्ट करें)

Who to Contact & When

Emergency Contacts for Different Situations:
विभिन्न परिस्थितियों के लिए आपातकालीन संपर्क

Financial Fraud:

वित्तीय धोखाधड़ी

जब कोई व्यक्ति धोखे से आपके पैसे या बैंक की जानकारी लेकर आपको आर्थिक नुकसान पहुंचाए, उसे वित्तीय धोखाधड़ी कहा जाता है।

- ✓ Bank/Card Company: Call number on back of card
  बैंक/कार्ड कंपनी: कार्ड के पीछे दिए गए नंबर पर कॉल करें
- ✓ Cyber Crime Helpline: 1930 (India)
  साइबर क्राइम हेल्पलाइन (भारत):
  1930 पर तुरंत कॉल करें

धोखाधड़ी होने पर घबराएं नहीं — तुरंत 1930 पर कॉल करें और बैंक को सूचित करें।

School-Related Issues:

स्कूल से जुड़ी समस्याएं

- ✓ School IT Department
  स्कूल की IT टीम से संपर्क करें
- ✓ Trusted teacher or counsellor
  किसी भरोसेमंद शिक्षक या काउंसलर को बताएं

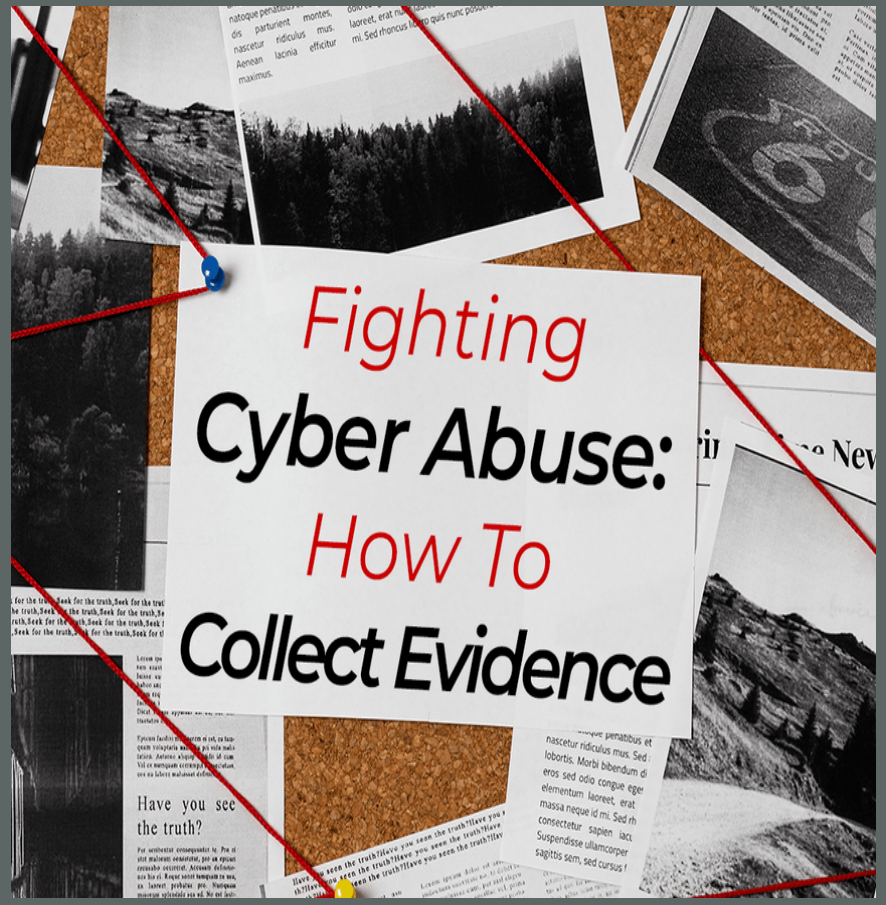
Personal Safety Threats:

व्यक्तिगत सुरक्षा से जुड़ी धमकियाँ

- ✓ Local Police: 100
  100 पर पुलिस को कॉल करें
- ✓ Child Helpline: 1098
  1098 पर बच्चों की हेल्पलाइन से मदद लें

Evidence Collecting

सबूत जमा करना



How to document incidents properly:

Screenshots:

- Capture suspicious messages/emails
  जो भी संदिग्ध लगे – उसका स्क्रीनशॉट लो
- Include sender information and timestamps
  कौन भेजा, कब भेजा – सब दिखना चाहिए

Written Records:

- Date and time of incident
  घटना की तारीख और समय लिखें
- What you were doing when it happened
  घटना के समय आप क्या कर रहे थे, साफ़-साफ़ बताओ
- What actions you took
  तुरंत तुमने क्या किया – सब लिखकर रखो

DO NOT delete anything - it might be evidence

कुछ भी न मिटाएं, हो सकता है वही सबूत हो

Recovery Strategies

साइबर हमले के बाद सुधार के उपाय

Steps to get back on track:
फिर से पटरी पर लौटने के **कदम**

Immediate Actions :

तुरंत किए जाने वाले कार्य

- ✓ Change all passwords
  सभी पासवर्ड तुरंत बदलें
- ✓ Enable 2FA on all accounts
  सभी अकाउंट्स पर 2FA चालू करें
- ✓ Update security software
  सुरक्षा सॉफ़्टवेयर (एंटीवायरस आदि) अपडेट करें

Data Recovery :

डेटा पुनर्प्राप्ति

- ✓ Restore from backups (if available)
  बैकअप से डेटा वापस लाएं (यदि उपलब्ध हो)
- ✓ Professional help for serious damage
  गंभीर नुकसान होने पर प्रोफेशनल की मदद लें

Emotional Recovery :

भावनात्मक पुनर्प्राप्ति

- ✓ Talk to counsellors if feeling stressed
  अगर मन भारी लगे, तो किसी भरोसेमंद काउंसलर या टीचर से बात करें

Building Digital Resilience
Staying Strong Online

डिजिटल दुनिया में सतर्क,
सुरक्षित और मज़बूत बने रहें।

UNNATI WELFARE SOCIETY

Advanced Security Practices

एडवांस्ड साइबर सुरक्षा की आदतें

Level up your digital protection:
ऑनलाइन सेफ्टी को और बेहतर बनाएं

1.

Privacy Settings Review:
प्राइवेसी सेटिंग्स की जांच

- ✓ Social media accounts (monthly check)
  सोशल मीडिया अकाउंट्स की हर महीने जांच करें
- ✓ Gaming platforms and apps
  गेमिंग प्लेटफॉर्म और ऐप्स की प्राइवेसी सेटिंग्स भी जांचे

Real Story

I. Rahul didn't check his privacy settings.
His photos, phone number, and profile were visible to everyone.
A stranger:
- Stole his photo
- Created a fake account
- Messaged Rahul's friends and family asking for money

This is called Identity Theft and online fraud.

II. Anya didn't change her chat privacy in a game.
Her chat was public, and strangers started messaging her.

One person:
- Became fake friend
- Took personal information
- Tried to blackmail her for money

Advanced Security Practices

एडवांस्ड साइबर सुरक्षा की आदतें

2.

Device Security:
डिवाइस की सुरक्षा

- ✓ Lock screens on all devices
  हर डिवाइस का लॉक स्क्रीन ऑन रखो
- ✓ Regular software updates
  सॉफ्टवेयर समय-समय पर अपडेट करते रहो

Real Story

I. Aman wanted to buy shoes online. He saw a website with a big discount and quickly entered his card details.
But the website was fake.
What happened?
- His money was stolen
- His card was used for other purchases

This is called phishing and online shopping fraud

II. Nisha downloaded a game from a random website, not the Play Store.
The app looked normal, but it had a virus inside.
What happened?
- Her phone started hanging
- Her photos and data were stolen
- She started receiving scam messages

This is called malware attack

Advanced Security Practices

एडवांस्ड साइबर सुरक्षा की आदतें

Safe Browsing Habits:
सुरक्षित ब्राउज़िंग की आदतें

- ✓ Verify website URLs before entering data
  वेबसाइट पर कोई भी जानकारी डालने से पहले URL ध्यान से देखो
- ✓ Use reputable app stores only
  सिर्फ भरोसेमंद ऐप स्टोर से ही ऐप डाउनलोड करो

Real Story

I. Ravi searched for his bank's login page on Google.
He clicked the first link, which looked like his bank's website but had a slightly different URL.
He entered his username, password, and OTP.
What went wrong:
The website was fake, created by scammers. They used his details to steal ₹75,000 from his account within minutes.

This is called phishing through a fake URL.

II. A college student downloaded a "free movie app" from a random website (not Play Store).
It asked for permissions to access photos, messages, and contacts.
Later, her phone was:
Locked by ransomware
A message appeared: "Pay ₹5,000 to unlock your phone"
Her contacts received scam messages

This is a malware/ransomware attack through untrusted apps.

Digital Citizenship

डिजिटल नागरिकता का मतलब है इंटरनेट और डिजिटल दुनिया का सही, सुरक्षित, जिम्मेदारी से और सम्मानपूर्वक इस्तेमाल करना।

Being a responsible digital citizen:

Respect Others Online:
ऑनलाइन दूसरों का सम्मान करें

- No cyberbullying or hurtful comments
  किसी की भावनाओं को चोट मत पहुँचाओ
- Think before you post or share
  कुछ भी पोस्ट या शेयर करने से पहले सोचें

Digital Ethics:
डिजिटल नैतिकता

- Don't pirate software or content
  चोरी किया हुआ कंटेंट देखना या शेयर करना भी **गलत** है
- Respect others' privacy and intellectual property
  किसी की फोटो, वीडियो या आइडिया को बिना पूछे इस्तेमाल करना **अनैतिक** है

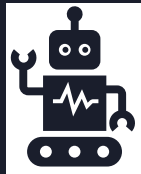
Be a Positive Influence:
एक सकारात्मक प्रभाव बनें

- Share helpful and accurate information
  सही और काम की जानकारी शेयर करें
- Help friends stay safe online
  दोस्तों को ऑनलाइन सुरक्षित रहने में मदद करें

Future-Proofing Your Security

आज से ही ऐसे सुरक्षा उपाय अपनाओ जो भविष्य में भी काम आएं।

Staying ahead of evolving threats:
बदलते साइबर खतरों से एक कदम आगे रहें



Emerging Technologies:
नई उभरती तकनीकें

- AI-generated deepfakes (fake videos/images)
  AI द्वारा बनाए गए नकली वीडियो और तस्वीरें
- Voice cloning scams
  आवाज़ की नकल करके ठगी
- Smart device vulnerabilities
  स्मार्ट डिवाइस में सुरक्षा की कमजोरियाँ

Future-Ready Mindset:
भविष्य के लिए तैयार सोच

- Stay curious about new security tools नई सुरक्षा तकनीकों के बारे में जानने की जिज्ञासा रखें
- Follow trusted cybersecurity sources भरोसेमंद साइबर सुरक्षा स्रोतों को फॉलो करें
- Practice healthy skepticism online ऑनलाइन किसी भी जानकारी पर तुरंत विश्वास न करें – सोच-समझकर भरोसा करें

जिज्ञासु बनो, अपडेट रहो, और सोच-समझकर क्लिक करो – यही है स्मार्ट डिजिटल नागरिक की पहचान।

Resources & Support

संसाधन और सहायता

Where to get help and learn more:

Emergency Helplines (India) :
आपातकालीन हेल्पलाइन

Cyber Crime:
1930
Child Helpline:
1098
Police Emergency:
100

Trusted Websites :
विश्वसनीय वेबसाइटें

- StaySafeOnline.org
- CyberSecurity.gov.in
- ConnectSafely.org

Stay Strong, Stay Safe, Stay Smart

UNNATI WELFARE SOCIETY