St. Xavier's College Jaipur

Affiliated to University of Rajasthan, Jaipur
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Department of Computer Science
in collaboration with the
Student Cyber Safety Committee
is organizing

Cyber Security Awareness Month
Cyber Jaagrookta Diwas

1 – 30 October 2025

As part of this initiative, the following activities will be organized during the month:

Daily Awareness Posters –
Based on the topics covered in the Value Added Course (VAC) – Cyber Law and Ethics

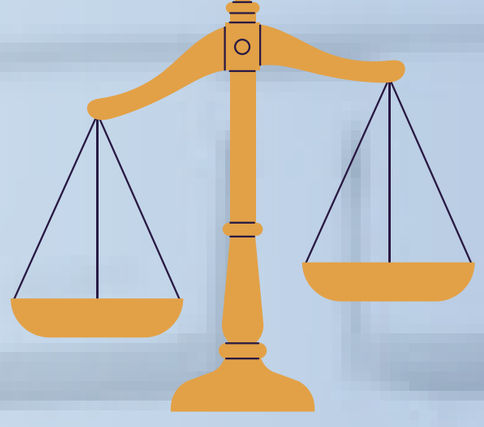
Cyber Law & Ethics Newsletter 2025 –
A comprehensive newsletter highlighting the learnings, awareness drives, and student contribution

STUDENT COORDINATORS		PROGRAM COORDINATORS	ORGANISER
Darshik Khandelwal Hardik Natani Kripa Sunil Mukund Sewani Mohd Munis	Neha Sharma Tushar Benedick Yuvraj Singh Divyansh Choudhary Robin Shinu	Ms. Pushpanjali Saini Dr. Vaishali Singh Dr. Arpita Banerjee Coordinator, SCSC & HEAD, CS	Dr.(Fr.) Arokya Swamy SJ (Principal)

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

AWARENESS POSTER DAY-1



CYBER LAW AND ETHICS - AN INTRODUCTION

UNDERSTANDING CYBER LAW

Legal rules governing computers, internet, and digital tech to prevent cybercrime, protect data, intellectual property, and cybersecurity, safeguarding individuals, businesses, and governments.

ETHICS IN THE CYBER WORLD

Ethical principles for responsible online behavior, promoting privacy, honesty, respect, and preventing harm like plagiarism or cyberbullying.

Designed By:-

Mukund Sewani
BCA Semester III

Organised By:-

Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day-2

Cyber Jurisdiction

"The legal authority over internet-based activities"

Working

Cyber jurisdiction decides which country's laws and courts handle an online crime, based on the location of the crime, people, or systems involved.

Procecution & Enforcement

Once jurisdiction is decided, the case moves to the court or authority of that country.

Law enforcement may need help from foreign agencies to arrest suspects or gather digital evidence.

Designed By -
Mohd. Munis
BCA semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

AWARENESS POSTER DAY - 3

Internet Opportunities & Risks

INTERNET OPPORTUNITIES

- Easy global communication
- Access to vast information
- Online education & learning
- E-commerce & job opportunities
- Social networking & collaboration

INTERNET RISKS

- Cybercrime & hacking
- Privacy loss & data theft
- Fake news & misinformation
- Online addiction & health issues
- Cyberbullying & harassment

Designed By:-

Yuvraj Singh
BCA Semester III

Organised By:-

Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

AWARENESS POSTER DAY-4

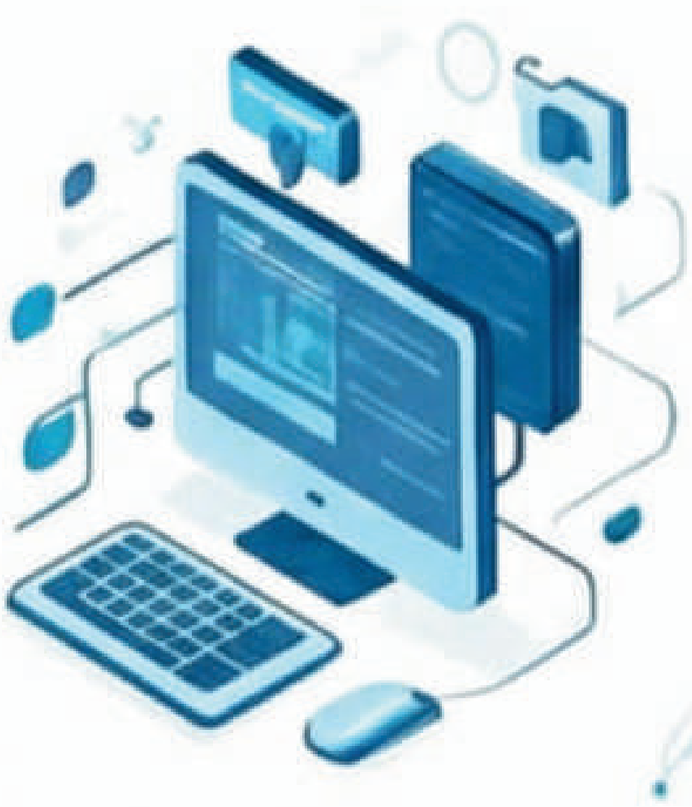
EVOLUTION OF THE CYBER WORLD

EARLY DAYS & INTERNET 1.0

1960s-1990s

The internet started as - ARPANET

- Used manly researchers as the military.
- Connections were used, Dial-up internet
- Information more static
- Basic inboxes like through basic search engine



MODERN ERA & WEB.2.0/5.0

2000s- Today

Rise of social media platforms like Facebook , found everywhere.

- Youtube for videos , podcasting , blogging fields are rising too
- Artifical Intelligence(NL In Ecommerce, and Virtual & Augmented Reality)

Designed By:-

Kripa Sunil
BCA Semester III

Organised By:-
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

AWARENESS POSTER DAY - 5

EVOLUTION OF THE CYBER LAWS

EARLY CYBER LAWS (1980S & 2000S)

- Computer Fraud and Abuse Act (USA, 1986)
- Computer Misuse Act (UK, 1990)
- India: IT Act, 2000

Focus on:

- Hacking & unauthorized access
- Electronic signatures & records
- Basic cybercrime laws

MODERN CYBER LAWS (2010S–TODAY)

- GDPR (EU, 2018) – Data privacy
- CCPA (California, 2020) – Consumer rights
- Stronger cybercrime & security laws

Focus on:

- Data protection & privacy
- Cyber terrorism & online frauds

Shaping a Safer Digital World

Designed By:-
Robin Shinu
BCA Semester III

Organised By:-
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

AWARENESS POSTER DAY - 6

VISHING ATTACK

WHAT IT IS:

A vishing attack is a type of phone scam where a scammer calls you pretending to be someone you trust (like a bank officer, government agent, or company representative) to steal your personal or financial information.

REAL-LIFE CASE EXAMPLE:

In February 2025, Italian police froze funds after a scam where attackers used AI to mimic the voice of Italy's Defence Minister and made calls asking business leaders for urgent financial assistance to supposedly release kidnapped journalists. About €1 million was transferred before authorities intervened.

LEGAL CHARGES / ACTS:

Section 66C, IT Act 2000 – Identity Theft
Section 419, IPC – Cheating by Personation
Section 471 – IPC: Using Forged Document as Genuine
Section 66D, IT Act 2000 – Cheating by Personation using Communication Devices

STAY ALERT. HANG UP. VERIFY.

Designed By -
Tushar Benedick
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

AWARENESS POSTER DAY - 6

VISHING ATTACK:

Know the Trap, Stay Safe!

Fraudutent Calls Stealing Your Info

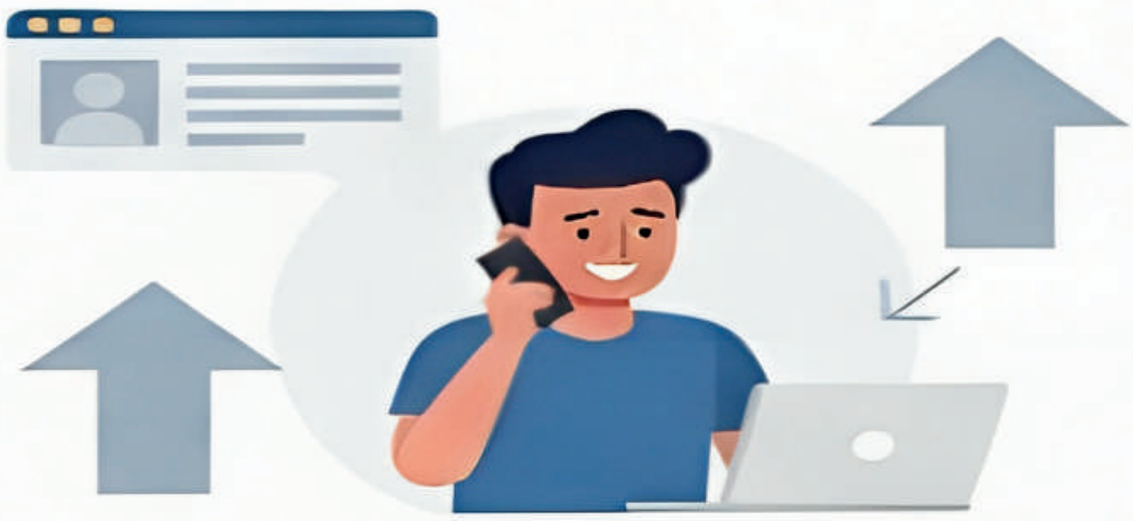
HOW IT HAPPENS

1. **Unsolicted Call** (Bank, (Bank, Tech Support, Govt,)

2. **Urgency/Threat** (Account Frozen, Virus Detected

3. **Manipiuate/Extract** (OTP, Card CVV, Password

HOW TO STOP IT



Verify Identity (Hang Up Call Back on Official #)

Never Share Info (OTP, CVV, PIN

Block & Report (To Bank, Police

Designed By -
Priyanshi Rajawat
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day - 7

DEEPFAKE ATTACK

A DEEPFAKE ATTACK IS A FORM OF CYBERCRIME THAT EMPLOYS HIGHLY REALISTIC, AI-GENERATED SYNTHETIC MEDIA—SUCH AS VIDEOS, AUDIO, OR IMAGES—TO IMPERSONATE A REAL INDIVIDUAL.

- THE MAIN OBJECTIVES BEHIND THESE ATTACKS ARE EITHER FINANCIAL FRAUD OR SOCIAL ENGINEERING, WHERE ATTACKERS TRICK VICTIMS INTO TAKING ACTIONS THEY TYPICALLY WOULDN'T CONSIDER, SUCH AS:

- **TRANSFERRING FUNDS** TO A FRAUDULENT ACCOUNT (E.G., MIMICKING A CEO DURING A VIDEO CALL).
- **DISCLOSING SENSITIVE INFORMATION** (E.G., PRETENDING TO BE A RELATIVE IN AN URGENT VOICE CALL SCAM).

Designed By -
Risabh Gupta
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day 7:

DEEPFAKE ATTACK

What is a deepfake?

- AI-generated audio, video that i nitates someone's voice or face
- Used to mislead, emparrass, extort, or defame.

Immediate actions

- Don't share suspicious videos or messages.
- Screenshot • save original file/URL.
- Report to the platform
- File a police complaint / eyber cell FIR
- Contact a lawyer for takedown • damages

Real-life examples

- **Bollywood actors file suits over explicit AI deeptakes**

  High profile legal action after sexualized AI-generated videps used actors likenesses without consent.

- **Man arrested for sharing deeptake of the Prime Minister in a WhatsApp group**

  Police registered cases after a manipulated video that could cause public rear was enculated accused charged under cyber't public-order provi-

State government warnings after AI vdeo mistepresents a Chief Minister

Designed By -
Ashutosh pandit
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

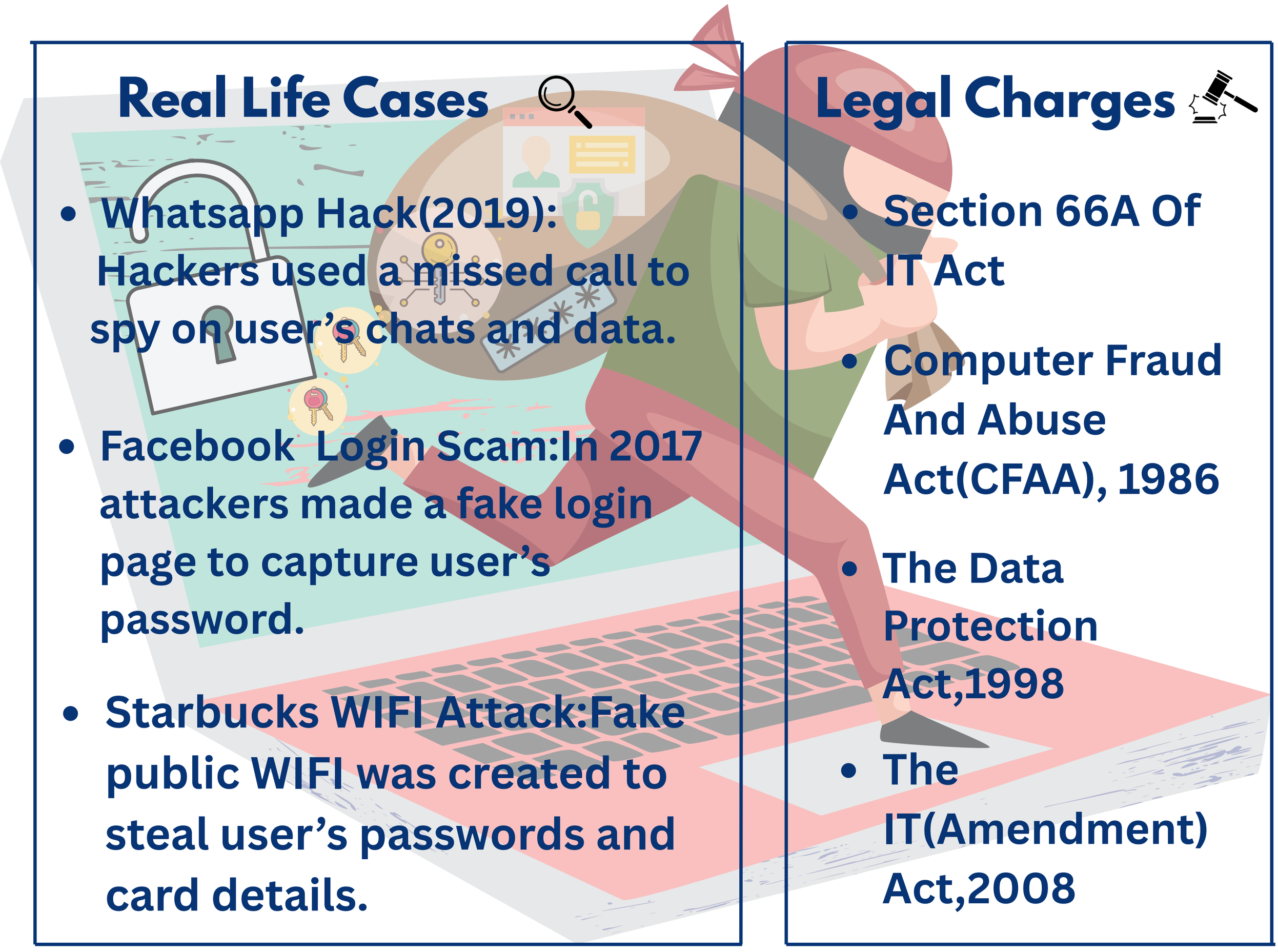
St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

AWARENESS POSTER DAY 8:

Man In The Middle Attack:

An attacker secretly intercepts communication between two parties



Real Life Cases

- **Whatsapp Hack(2019): Hackers used a missed call to spy on user's chats and data.**
- **Facebook Login Scam:In 2017 attackers made a fake login page to capture user's password.**
- **Starbucks WIFI Attack:Fake public WIFI was created to steal user's passwords and card details.**

Legal Charges

- **Section 66A Of IT Act**
- **Computer Fraud And Abuse Act(CFAA), 1986**
- **The Data Protection Act,1998**
- **The IT(Amendment) Act,2008**

"Your clicks can be trapped – think before you tap!"

Designed By -
Hansika Sisodiya
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day 9:

Forgery of Digital Signature

-know the risk

What is it?

Forgery of a digital signature means tricking a system or person into accepting a fake or unauthorized signature — often by stealing a private key or exploiting trust.

Common Methods

- **Stolen private keys**
- **Phishing or malware**
- **Fake or misused certificates**
- **Reused or backdated signatures**
- **Weak cryptography or bugs**

Warning Signs

- **Invalid or expired certificates**
- **Missing or suspicious timestamps**
- **Unknown or untrusted signers**
- **Unexpected file changes or signers**

Protect Yourself

- **Use secure key storage**
- **Always verify signatures and timestamps**
- **Revoke compromised certificates**
- **Never share or export private keys**

Digital signatures ensure trust — protect them like passwords!

Designed By -
Ritu Kanwar
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

CYBERCRIMES THROUGH THE DARK WEB

Unmasking Hidden Threats & Legal Repuresctions

REAL-LIFE CASE STUDIES

THE SILK ROAD
- Case: Online black market for **illegal goods.**
- **Impact: Drug Trafficking, Mnions**
- **Legal: U.S. & International Statutes.**

DARKBYTES BREACH
- Impact: Solen personal/ Financial data (millions & users).
- Identity Theft, CCPA violations

WANNCARY RANSOWARE
Case: Onlivare enccyted dats Glatt, Bc, Wality, HIPA, Fraud Cybert Espacanige, Untahoncter (The National Laws Pahte)

PROTECT YOURSELF: AWARENESS & PREVENTION

DIGITAL SELF-DEFENSE
Strong Unique Passwords
- **2-Factor Authentication (2FA)**
- Be Wary HIPA Secure traced downloads

RECOGNIZE THE RISKS
- **Trans Web is NOT Anonymous)**
- **Report Suspicious activity**
- **Keep OS & Antivrius Updated**

LEGAL EMPOWERMENT
- **Know af Rights**
- **Understand Cyber Laws**
- **Report Crimes to Authorities**
  Seak Legal Aid

STAY INFORMED. STAY SECURE. BE A RESPONSIBLE DIGITAL CITIZEN

Designed By:-
Kelvin Benny Koshy
BCA Semester III

Organised By:-
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

AWARENESS POSTER DAY-10

CYBERCRIMES THROUGH THE DARK WEB

ATTACK SCENARIO	OFFENDER'S ACTION	APPLICABLE LAGAL CHARGES
1 . Data Theft & Identify Fruad	A hacker steals customer financial data (credit card and Aadhaar information) from a firm and sells it on a Dark Web forum.	IT Act, 2000: Section 43 (Penalty for damage to computer system), Section 66 (Hacking), Section 66B (Receiving stolen data)
2. Ransomware and Extortion	Cyber criminals use malware purchased on the Dark Web to lock a major hospital's network and demand a Bitcoin ransom to release patient records.	IT Act, 2000: Section 66F (Cyber Terrorism), IPC Section 383 (Extortion)
3. Illegal Drug Trafficking	A Dark Web market operator runs an anonymous website, facilitating the sale and delivery of illegal narcotics and weapons worldwide.	IT Act, 2000: Section 67 (Obscene/Illegal Material in Electronic Form). NDPS Act (Narcotic Drugs and Psychotropic Substances Act, 1985). IPC Section 120B (Criminal Conspiracy).

Designed By -
Guneet Gautam
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan

Accredited with A Grade by NAAC (First Cycle, 2025)

An ISO 14001:2015 Certified Institution

WARNING POSTER-1

CYBER TRAPS: SOCIAL MEDIA SCAMS

SWIPE LEFT ON STRANGERS, OR YOUR BANK ACCOUNT MIGHT GO RIGHT

Scammers are everywhere – pretending to be someone you trust, offering "too good to be true" deals, or sending links designed to trap you.

EVERY 39 SECONDS,

a cyberattack hits someone online.
Don't be the next victim.

- Fake Giveaways & Contest Links
- Impersonation of Friends or Influencers
- Phishing Messages Asking for Details
- Fake Job or Investment Offers
- Report suspicious emails and messages

UNPLUG BEFORE THEY DECIDE

Designed By :-

Divyansh Choudhary
BCA Semester III

Organised by :-
Department of Computer Science
in collaboration with the
Student Cyber Saftey Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

SPECIAL POSTER-1

SPECIAL APPS & WEBSITES

Vishing Attack

App: SlashNext-
AI-powered phishing protection with high detection rate and real-time blocking of scams.

Website :
[https://www.consumer.ftc.gov/articles/0076-phone-scams]

Man-in-the-Middle Attack

App: Build 38 Mobile Security-
Provide strong mobile app security SDK to detect and block MITM attacks.

Website :
[https://owasp.org/www-community/attacks/Man-in-the-middle]

Deepfake Attacks

App: Sensity AI-
Advanced AI deepfake detection across audio, video, and images with enterprise grade accuracy.

Website :
[https://www.technologyreview.com/2020/12/10/1013144/mit-deepfake-detection]

Dark Web Cybercrime

App: Breachsense-
Real-time dark web monitoring and breach detection alerts to prevent identity theft.

Website :
[https://www.bbc.com/news/technology-41179600

Designed By:-

Mukund Sewani
Divyansh Choudhary
BCA Semester III

Organised By:-

Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

SPECIAL POSTER-1

Specials Apps & Websites

Vishing Attack

Act : Information Technology Act, 2000 - Section 66D (cheating by impersonation using communication devices)
Website : [https://www.consumer.ftc.gov/articles/0076-phone-scams]

Deepfake Attack

Act : IT Rules 2021 (Intermediary Guidelines), IPC Sections 469 & 500 (forgery and defamation)
Website : [https://www.technologyreview.com/2020/12/10/1013144/mit-deepfake-detection]

Man-in-the-Middle Attack

Act : IT Act, 2000 - Sections 66, 43 (unauthorized access and data theft)
Website : [https://owasp.org/www-community/attacks/Man-in-the-middle]

Forgery of Digital Signature

Act : IT Act, 2000 - Sections 66C & 73 (identity theft and digital signature misuse)
Website : [https://csrc.nist.gov/publications/detail/sp/800-106/final]

Cybercrimes through Dark Web

Act : IT Act, 2000 - Sections 66F (cyber terrorism), 67, 67A, 67B (illegal content)
Website : [https://www.bbc.com/news/technology-41179600]

Designed By -
Yuvraj Singh
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St Xavier's College Jaipur

Affiliated to University of Rajasthan, Jaipur
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

AWARENESS DAY POSTER -13

CYBER TERRORISM

ATTACK VECTOR:
CRITICAL INFRASSTUCTURE

TARGETS:
POWER GRIDS,
FINANCIAL SYSTEMS

IMPACT: WIDEMADE DISRUPTION,
ECONOMIC COLLAPSE, LOSS OF

THREAT ACTORS:
STATE-SPONDSRED GROUPS,
HACKTITISTS
CRMINAL ORGANIZATIONS

DEFENSE:
ADVANCED FIREMLYICS, AI
INTERNATIONAL COOEPRATION

PREPARKDEDS:
SIMULATION TRAINING,
CYBER HYGIENE EDUCATION

THE DIGITAL BATTLEFFIELD:
ANALYING THLEW FRONITER OF GLOBAL CONFLICT

DATE: OCTOBER 26. 2023 / ORGANIZED BY:
GLOBAL CYBERSECURICTY FORUM

Designed By -

Aashish Anthony
BCA Semester III

Organized By -

Department of Computer Science
in Collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

AWARENESS POSTER DAY-14

AADHAAR DATA LEAK (2018 - INDIA)

Reported Misuses / Frauds : - 2018 saw many reports of Aadhaar frauds: fake/forged Aadhaar cards, banking frauds involving Aadhaar, etc.
- Cases where Aadhaar numbers, names etc appeared on public portals.

Aadhaar details of 81.5 cr people leaked in India's 'biggest' data breach

By HT News Desk, New Delhi

Oct 31, 2023 12:23 PM IST

The hacker claims to have extracted the information from the Covid-19 test details of the citizens registered with ICMR.

Impact :

- Citizens' personal data became vulnerable.
- Risk of identity theft and fraud increased.
- Public trust in Aadhaar system declined.
- Legal and policy debates intensified.
- Weak third-party systems exposed flaws.

Outcome :

- Sparked nationwide concern over privacy.
- Led to stricter data security measures.
- Encouraged transparency and accountability.
- Resulted in the Data Protection Act (2023).
- UIDAI introduced Virtual ID and Masked Aadhaar.

Designed By -
Swapandeep Kachhap
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

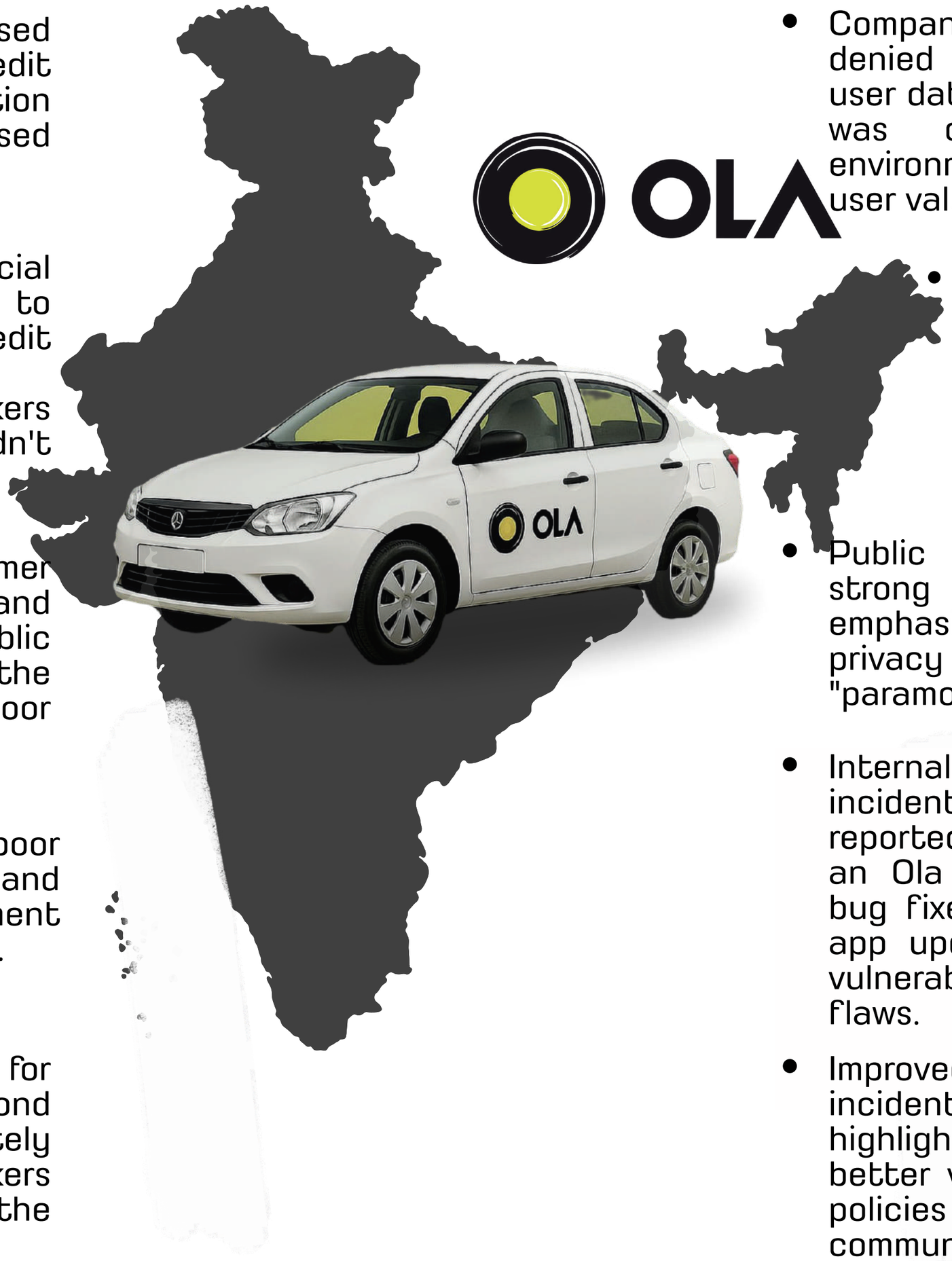
Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

AWARENESS POSTER DAY-15

OLA CABS DATA LEAK 2014

Loss/Impact (Alleged by Hackers/Media)

- Allegedly accessed User Details, Credit Card Transaction History, and Unused Vouchers.
- Potential for financial fraud due to compromised credit card/transaction history (though hackers claimed they wouldn't misuse it).
- Major loss of customer trust and brand reputation due to public disclosure of the security lapse and poor security structure.
- Direct exposure of poor application design and weak development server configuration.
- Ola was criticized for failing to respond promptly or adequately to the ethical hackers who reported the vulnerability.



Resolution (Ola's Response & Subsequent Actions)

- Company Denial: Ola officially denied a security lapse on user data, claiming the breach was on a staging/test environment with only dummy user values.
- Damage Control: Claimed no real customer financial data was compromised, thus mitigating direct financial loss from the alleged breach.
- Public Statement: Issued a strong public statement emphasizing the security and privacy of customer data as "paramount."
- Internal Review/Fixes: The incident, along with other reported vulnerabilities (like an Ola Wallet hack), led to bug fixes and the release of app updates to address API vulnerabilities and security flaws.
- Improved Protocols: The incident (and similar ones) highlighted the need for better vulnerability disclosure policies and prompt communication with security researchers to secure systems faster.

Protecting Your Journey, Securing Your Data

Designed By -
Mohommad Mahir Khan
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

AWARENESS POSTER DAY 15 :

OLA CABS

DATA LEAK 2014

- The Server Type:

  The hackers later clarified, and Ola emphatically stated, that the compromised server was a "staging" or "development" environment, not the live production database.

- Vulnerability:

  The hackers claimed the server was "weakly configured" and the application design was "very poor."

- Company Stance:

  Ola Cabs officially denied any security lapse to real user data, claiming the compromised server contained only "dummy user values" for internal testing.

- Alleged Compromised Data:

  The group claimed to ha accessed a database containi user details, credit ca transaction history, and unus vouchers.

- Hacker Group:

  A group named "TeamUnknown" public claimed to have breached Ola's servers

- The Underlying Risk:

  Security experts noted that t attack exposed the poor secur practices on their testing serv including the use of the we MD5 hashing algorithm passwords.

"Assume that any data you share with an app, including payment information, is at risk of a breach."

Designed By -
Mohommad Mahir Khan
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day 15 :

OLA CABS DATA BREACH

2014 SCANDAL

IMPACT:

1. MILLIONS OF USERS EXPOSED
2. PERSONAL INFO LEAKED (NAMES, PHONLS, LOCATIONS).
3. EROSION OF CUSTOMER TRUST
4. FINANCIAL LOSSES FOR OLA
4. REPUBTATIONL FOR OLA
5. REPULTATIOAL DAMAGE

OUTCOMES:

1. INCREASED SECURITY MEASURES
2. REVISED PRIVACY POLICIES
3. GOVERNMENTAL SCRUTINY
4. INDUSTRY-WIDE SCRUTINY
4. INDUSTRY-WIDE ALERTS
5. LESSONS IN CYBERSECURSITY

DATA PRIVACY IS NOT A LUXURY. IT'S A RIGHT.

Designed By -
Diksha Sharma
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day 15 :

OLA CABS DATA BREACH

2014 SCANDAL

IMPACT:

1. MILLIONS OF USERS EXPOSED
2. PERSONAL INFO LEAKED (NAMES, PHONLS, LOCATIONS).
3. EROSION OF CUSTOMER TRUST
4. FINANCIAL LOSSES FOR OLA
4. REPUBTATIONL FOR OLA
5. REPULTATIOAL DAMAGE

OUTCOMES:

1. INCREASED SECURITY MEASURES
2. REVISED PRIVACY POLICIES
3. GOVERNMENTAL SCRUTINY
4. INDUSTRY-WIDE SCRUTINY
4. INDUSTRY-WIDE ALERTS
5. LESSONS IN CYBERSECURSITY

DATA PRIVACY IS NOT A LUXURY. IT'S A RIGHT.

Designed By -
Diksha Sharma
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day - 16

THE PEGASUS SPYWARE

A Global Surveillance Crisis

Exposing the Dark Side of Digital Espioonce

1. What is Pegasus?

Developer: NSO Group (Israel)
Function: Highly intrusve spwirre, Remotely infrriiates
Capabilities: Full acess o messages, photos, location, camera, encrypted apps (WhatsApp, Signal)
Infilration: 'Zer-click' explots (no user action needed).

2. The Investigation: The Pegasus Project

Led By: Forbeden Stories & Anrsty Intsnational Security Lab.
Collaboration: 80+ journalists, 17 media numbery /boons targeted
Discoiery: Leaked list of 50,000+ phoes taigted by NSO clients since since 2016.
Evidence: Foresstic analysis confimed Pegasseus infections on targeted phones.

3. Who Was Targeted?

- Journalists
- Paidical of State
- Human Rights Activists
- Jamal Krashoggi's family
- Political Dissidents
- Oppsidion figures
- Presidents, PM
- Lawyers & Academics

4. Major Impacts

Human Rights: Invasion of privacy. foedom of expression.
Democracy chilling effect on disent
Jouraalism: Compranises sources, endeders repoters.
Global Security.tsck of overright.

5. The Fallout & Response

International Cuttry: UN & EU inquries.
Legal Action: Apple Meta (WhatSAp) sue NSO.
Government Sanctions: U.S. blackilists NSO.
Ongoing Debate: Need for regulation.

Designed By -
Francis Xavier
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day 16 :

PEGASUS SPYWARE CASE

Pegasus is a powerful spyware developed by the Israeli company NSO Group, capable of secretly accessing a person's calls, messages, photos, and even the microphone or camera of a smartphone

It was allegedly used to spy on journalists, activists, and political figures in several countries, including India, raising serious concerns over privacy, surveillance, and human rights violations.

Key Issue:
🔒 Violation of Right to Privacy (Article 21 of the Indian Constitution)
Impact:
⚠️ Threat to democracy, freedom of speech, and digital security.
Message:
🛡️ Protect Privacy – Strengthen Cyber Laws & Digital Freedom!

Designed By -
Rudra Naruka
BCA Semester III

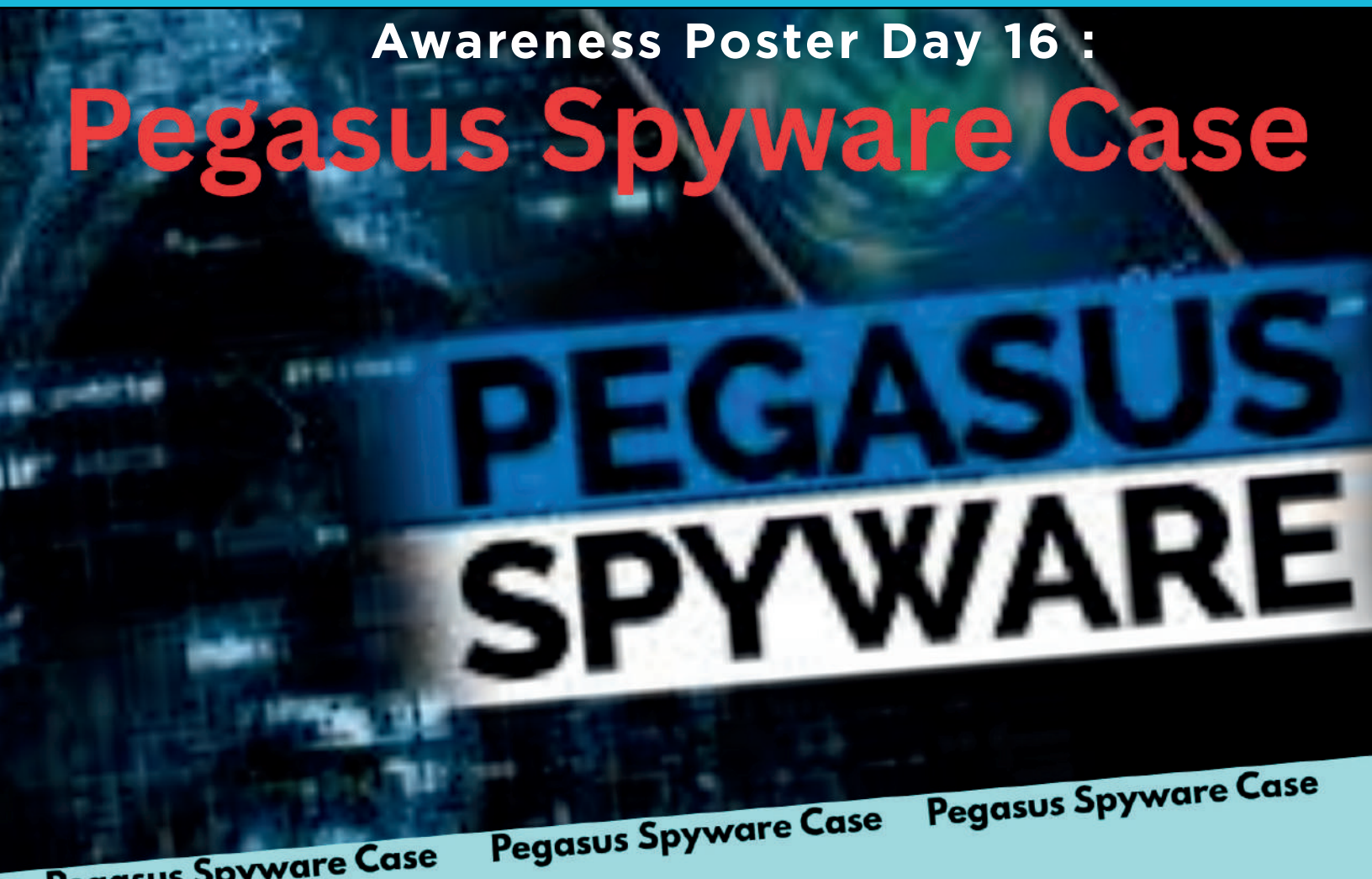
Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day 16 :

Pegasus Spyware Case



Pegasus Spyware Case Pegasus Spyware Case Pegasus Spyware Case

HOW TO PROTECT AGAINST PEGASUS SPYWARE

- Keep devices updated to patch vulnerabilities, avoid suspicious links and third-party app stores, use strong passwords, and consider a factory reset if an infection is suspected.
- Advanced users can use specialized tools like the Mobile Verification Toolkit (MVT) for detection, but for serious threats, it's best to contact a security expert or replace the device entirely.
- Keep Software Updated
- Be Cautious of Links
- Use Official App Stores
- Review Permissions
- Use Strong Security Tools
- Reboot Daily

Sections

-The Pegasus spyware case in India primarily invokes violations of the Information Technology Act, 2000 (specifically sections 66 and 69) .

-The Indian Telegraph Act, 1885 (specifically section 5(2)).

Designed By -
Merlyn Maclean
BCA Semester I

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

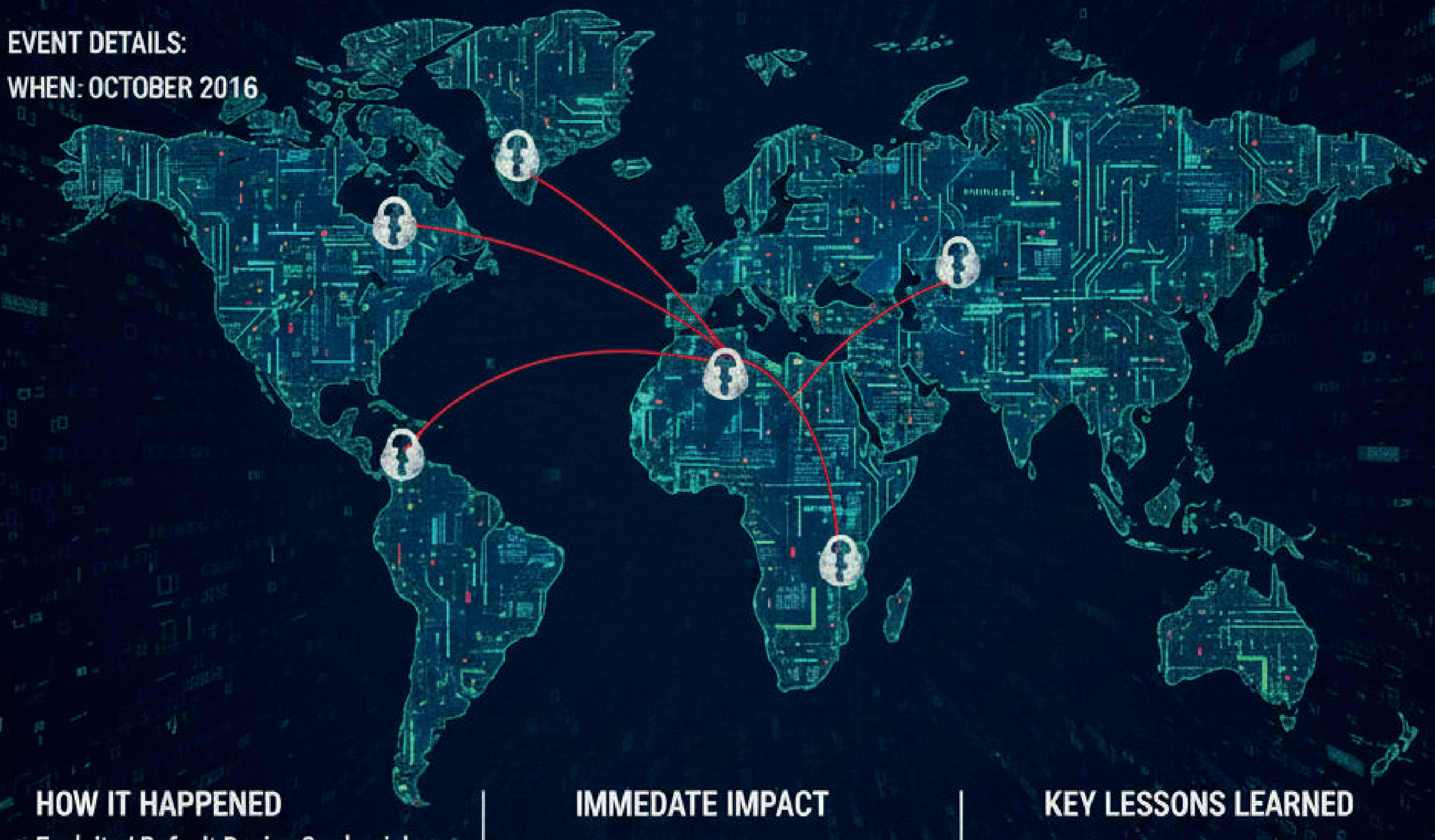
AWARENESS POSTER DAY-17

MIRAI BOTNET ATTACK GLOBAL 2016

A CASE STUDY IN CYBERSCEURITY FAILURE

EVENT DETAILS:

WHEN: OCTOBER 2016



HOW IT HAPPENED

- Exploited Default Device Credemials (Mirai Malved (Mlrvare)
- Massive Distribuied Denial of-c-Device DDOS Attacks

IMMEDATE IMPACT

1. DISRUPTION OF ONLINE SERVICES Websites Down)
3. ECONOMIC LOSS
3. PUBLIC SAFETY CONCERNS) (Critical Infrnastructure Risk)

KEY LESSONS LEARNED

1. URGENT IOT SECURITY
2. CHANGE DEFAULT PASSIDARDS SFFCHING
4. DEVICE MANAGEMENT & PATCHING
4. CRTICAL INFRSECWR PIOTECTION
5. REPHANED VENDOR MANAGEMENT

PROTECT YOUR DEVICES. CHANGE DEFAULT PASSWORDS.

Designed By -
Muskan Saxena
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

ST. XAVIER'S COLLEGE JAIPUR

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day 17 :

MIRAI BOTNET ATTACK GLOBAL 2016

Distributed Denial of Service (DDoS) attack

The Mirai botnet attack of 2016 was a series of massive, record-breaking Distributed Denial of Service (DDoS) attacks that exploited the weak security of Internet of Things (IoT) devices globally.

WHAT HAPPENED?

- Attack (DDoS)
- IoT (Compromised)
- Defaults (Exploited)
- Massive (Volume)
- Dyn (Targeted)
- Outages (Resulted)
- Code (Leaked)
- Vulnerability (Exposed)
- Warning (Global)

KEY TARGETS

- Dyn (DNS provider)
- OVH (Webhost)
- Krebs (Security blog)
- Netflix (Streaming)
- Amazon (E-commerce)
- Reddit (Social media)
- GitHub (Software)
- Liberia (National internet)
- Telekom (German ISP)

Designed By -
Mohammad Mahir Khan
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

WARNING POSTER -2

PUBLIC WIFI

⚠ THINK BEFORE YOU CONNECT! ⚠

Hacked Information
(Steal your: Bank Details, Card Number)

Login Credentials
(Passwords of Email-ID & Social Media A/C)

Sensitive Personal Information
(Emails Documents, Private Messages)

Public Wi-Fi may look free—
but nothing online is truly free!

A hacker can be sitting right next to you, turning your connection into an open door.

✔ DO'S

- Verify network names to avoid fake hotspots (Evil Twin attacks).
- Prefer your mobile data (4G/5G) for important tasks.
- Turn off auto-connect to open networks.

✘ DON'TS

- Logging into sensitive accounts
- Accepting software updates or downloads while connected.
- Clicking on links or opening attachments from unknown sources.

Stay Smart! Stay Secure!

Designed By:-
Hardik Natani
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Cell

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

SPECIAL POSTER -2

SPECIAL APPS & WEBSITES

AADHAR DATA LEAK : MAadhaar app

The app has been launched to ensure the safety of an individuals biometric data stored in the Aadhaar system. mAadhaar app enables users to lock and unlock their biometrics at their convenience.

CYBER TERRORISM : CyberCOP

CyberCOP Application stands at the forefront of the battle against cybercrime, serving as a comprehensive platform designed to empower users, raise cyber awareness, and combat digital threats effectively.

PEGASUS SPYWARE ATTACK APPDOME

Appdome's dynamic Prevent Trojan Spyware plugin for Android and iOS identifies and blocks zero-click exploits, unauthorized remote access, and spyware injections used by Pegasus.

MIRAI BOTNET :SIEM SIEM

A SIEM solution with advanced threat detection capabilities can help you prevent Mirai from laying its botnet foundation on your network. SIEM can help you protect your devices with a range of predefined detection rules.

Designed By:-
Darshik Khandelwal
BCA Semester III

Organised By:-
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affiliated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day - 20

DATA PROTECTION:

YOUR PRIVACY MATTERS!

Why it's important?

- Every click, post, and download leaves a digital footprint.
- Data breaches can expose your personal, financial, and social information.
- Protecting data means protecting your identity!

Dos

- Use strong, unique passwords (mix letters, numbers & symbols).
- Enable two-factor authentication (2FA) wherever possible.
- Use secure Wi-Fi connections and trusted websites (https)
- Backup your data on encrypted drives or cloud storage.

Don'ts

- Don't share personal info (like OTPs or bank details) online.
- Don't click suspicious links or pop-ups in emails or messages.
- Don't reuse the same password across different sites.
- Don't ignore privacy settings on your social media accounts.

Did You Know?

- Over 80% of cyberattacks are caused by weak passwords.
- Human error accounts for 90% of data breaches.
- India's Digital Personal Data Protection Act, 2023 ensures your rights to privacy and Data security.

Remember: "Protect Data, Protect Yourself."

Be smart. Stay alert. Stay secure.

Designed By -
Sudhanshu Gandhi
BCA Semester I

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day - 20

Protect Your Digital Life:

Data Protection Matters!

Data Protection:-

Data protection is the process of safeguarding sensitive information from corruption, loss, and compromise by using security strategies and processes. Its goal is to ensure data integrity, availability, and privacy, and to restore data to a functional state if it is lost or damaged. This involves a combination of data security measures, data backup and recovery, & compliance with legal & regulatory requirements.

Importance of Data Protection:-

- Prevents Data Theft
- Maintains Privacy
- Builds Trust

Do's & Don'ts for Data Protection

DO's

- Strong, Unique Passwords
- 2FA (Two-Factor Authencication
- Skeptical Emails-Links
- Software Updates
- Secure Public Wifi

DON'Ts

- Share Recklessly
- Public PCS for Sensitive Transactions
- Click Unverified Attachments
- Ignore Security Alerts
- Use Default Passwords

Make Data Protection Your Priority!

#CyberSecurityAwarenessMonth #DataProtection #StaySafeOnline

Designed By -
Divyansh Mahawar
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

AWARENESS POSTER DAY-20

PROTECTING YOUR DIGITAL WORLD

Secure. Private. Yours.

Two-Factor Authentication

Add an extra layer of security to your accounts

Anonymous Browsing

Keep your internet activities private

Threat Detection

Identify and mitigate potential threats

Secure Backup

Safeguard your data with regular backups

Real-time Monitory

Continuous surveil-lance for your netw

Incident Response

Swiftly address security incidents

Firewall Security

Prevent unauthorized access to your network

Stay Vigilant. Stay Protected. Your Digital Fortress.

Designed By -
Kripa Sunil
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

AWARENESS POSTER DAY- 21

CYBER BULLYING SAFEGUARDS

CYBER BULLYING

CYBER BULLYING SAFEGUARDS

- ONLINE HARASSMENT OR INTIMIDATION
- HURTFUL MESSAGES AND RUMORS
- EMOTIONAL AND MENTAL EFFECTS
- SIGNS: WITHDRAWAL OR DISTRESS
- BLOCK, REPORT, SAVE EVIDENCE
- USE PRIVACY AND SAFETY SETTINGS
- REPORT SERIOUS THREATS IMMEDIATELY

- ALWAYS KEEP YOUR ACCOUNT PRIVATE
- USE STRONG, UNIQUE PASSWORDS
- THINK BEFORE POSTING ONLINE
- DON'T SHARE PERSONAL INFO
- BLOCK AND REPORT BULLIES
- SAVE PROOF OF ABUSE
- TALK TO TRUSTED ADULTS

Designed By:-
Mukund Sewani
BCA Semester III

Organised By:-
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affiliated to University of Rajasthan, Jaipur
Accredited with A Grade by NAAC (First Cycle,2025)
An ISO 14001:2015 Certified Institution

AWARENESS POSTER DAY - 21

Cyberbullying Safeguard

CYBER SHIELD:
SAFEGARDING OUR DIGITAL SPACE

1. THINK BEFORE YOU YOU POST:
Pause & consider.
Kindness is key.

2. REPORT & BLOCK:
Don't engage.
Seek help from trusted adults/platforms.

3. BE AN ALLY:
Support victims.
Promote positivity.

UNITED AGAINST CYBER BULLYING. PROTECT. RESPECT. CONNECT.

Designed by:
Aryavardhan Singh
BCA Semester III

Organised By-
Department of Computer Science With Student Cyber Safety Cell

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day - 22

STRONG PASSWORD

Creating a strong password is one of the simplest yet most powerful ways to protect yourself online. A secure password should be long, unique, and include a mix of uppercase and lowercase letters, numbers, and special symbols. Avoid using common words, personal information, or easily guessable patterns like "123456" or "password". At least 12 characters and a different password for every account. Enabling two-factor authentication adds another layer of safety. Reused passwords are responsible for over 80% of data breaches.

Do's

- ✓ Enable Two-Factor Authentication (2FA) wherever possible.
- ✓ Change passwords immediately if you suspect a breach.
- ✓ Regularly update your passwords every few months.
- ✓ Keep your passwords private – don't share them with anyone.

Don'ts

- ✗ Don't reuse the same password across multiple sites.
- ✗ Don't write passwords on paper or save them in plain text.
- ✗ Don't use personal details (like your name, birthday, or numbers).
- ✗ Don't click on suspicious links or pop-ups asking for login info.

General Awareness

1. Cyber attackers often use brute force or guessing attacks on weak passwords.
2. Strong passwords act as the first line of defense against identity theft.
3. Weak passwords can compromise not only personal accounts but also corporate and financial systems.

Designed By -
Mohommad Mahir Khan
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day -23

CALL RECORDING

STAY AWARE

IMPORTANT FACTS

°Call recording is legal in many jurisdictions.

°You must inform the other party before recording.

°Recording can be used as evidence.

DO'S

- Inform the other party
- Use secure apps
- Store recording securely

DONT'S

- Record without consent
- Share recording publicly
- Use recording maliciously

Designed By -
Bhumika Bhatt
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day -24

NEVER IGNORE THE GREEN DOT ON YOUR SCREEN

What Does the Green Dot Mean?

That small green dot on your screen is more powerful than it looks.
It appears whenever your camera or microphone is active —
even if you didn't open them yourself.
It's your device's silent way of saying,
"Hey, someone might be watching!"

Why You Should Never Ignore It

In today's digital world, our devices know everything about us —
what we say, where we go, and what we look like.
Hackers or untrusted apps can secretly use your camera
to invade your privacy and steal your personal information.
Ignoring that green dot could mean letting strangers
peek into your private space.

How to Protect Yourself

Review and control which apps have access to your camera or microphone.
Avoid clicking on suspicious links or downloading random files.
Use camera covers or tape when not in use.
Keep your device's security settings updated.
And most importantly — stay alert whenever the green dot appears.

That tiny green light could be your only warning !

Designed By -
Uday Agrawal
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day 24 :
NEVER IGNORE THE GREEN DOT ON THE SCREEN

🟢 What Does the Green Dot Mean?

That tiny green light beside your camera signals it's on.
Whether you turned it on or not, it means your camera is active, and someone could be watching.

⚠️ Why You Should Never Ignore It

Hackers can hijack webcams to spy, record, or steal private data.
Ignoring the green dot could expose your personal moments to the internet.

🔒 How to Protect Yourself

Cover your webcam when not in use.
Check app permissions regularly.
Use strong passwords and updated antivirus software.
Your privacy starts with awareness.

Privacy isn't automatic. Protect it!

Designed By -
Neil Majumdar
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Warning Poster - 3

Not every link is a door... Some are traps!!

ONE CLICK.
THAT'S ALL IT TAKES
TO OPEN A DIGITAL NIGHTMARE

The links can steal your data, drain your money,
can even spy on you through your own device

Useful sites

- 🔍 *VirusTotal – Scan suspicious links or files.*
- 🔗 *CheckShortURL – Preview hidden or shortened links safely.*
- 💬 *Cyber Crime Portal (India) – Report phishing or cyber frauds.*
- 👨‍💻 *CSK.gov.in – Government cyber safety knowledge portal (India).*

Useful Tips

- ✅ *Hover over links before clicking check the real URL.*
- 🔐 *Keep your system and browser updated.*
- 🚫 *Avoid links from unknown messages or emails.*
- 🧠 *Use multi-factor authentication for all important accounts.*

Designed By-
Neha Sharma
Hardik Natani
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

SPECIAL POSTER DAY -3

SPECIAL APPS & WEBSITES

CALL RECORDINGS

Cyber Crime Reporting Portal
https://www.cybercrime.gov.in
→ File complaints about illegal call recordings, online fraud, or harassment.

National Cyber Helpline – 1930
Report financial or phone scams instantly.

Indian Computer Emergency Response Team (CERT-In) → https://www.cert-in.org.in
→ For reporting hacking, call data leaks, or other cyber incidents.

STRONG PASSWORDS

Bitwarden → https://bitwarden.com
→ Free, open-source password manager for all devices.

Password / LastPass → https://1password.com | https://www.lastpass.com
→ Generate strong, unique passwords and store them securely.

Have I Been Pwned → https://haveibeenpwned.com
→ Check if your email or password has been leaked online.

CYBER BULLYING

Cyber Crime Reporting Portal → https://www.cybercrime.gov.in
→ Official Indian government portal to report cyberbullying, threats, or abuse.

StopBullying.gov → https://www.stopbullying.gov
→ Global awareness and support platform.

ReThink App → https://rethinkwords.com
→ Stops hurtful messages before they're sent.

DATA PROTECTION

Stay Safe Online (MeitY India) → https://www.staysafeonline.in
→ Government initiative promoting data privacy and safe browsing habits.

Cyber Dost (Govt. Awareness Handle) → https://twitter.com/Cyberdost
→ Daily updates on online scams, fake links, and cyber safety tips.

NordVPN / ExpressVPN → https://nordvpn.com | https://www.expressvpn.com
→ Secure your internet connection and protect personal data.

Designed By:-
Darshik Khandelwal
BCA Semester III

Organised By:-
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day - 27

STOP CYBER CRIME • • REPORT IT. •

Don't be a victim. Be a reporter.

IMMEDATE STEPS:

1. Disconnect Device
2. Preserve Evidence
3. Contact Authorities

NATIONAL CYBER CRIME HELEPINE
1930 www.cybercrime.gov.in

Designed By -
Lakshika Agarwal
BCA Semester I

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affiliated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day - 27

SECURE YOUR DIGITAL LIFE: REPORT CYBERCRIME!

REPORT IT IMMEDATELY:

1. Disconnect Device
2. Preserve Evidence
3. Contact Authorties

PREVENT IT:

- Strong Passwords
- Two-Factor Authenication
- Secure-WIFI
- Antivirus Software

NATIONAL CYBER CRIME HELIPINE

1930 (24/7 Toll-Free)
www.cybercrime.gov.in

TYPES OF CYBERCRIME: Fraud, Identity Theft Harassment, Hacking, Scams, CSAM.

Ministry of Home Affairs, Government of India

Designed By -
Lakshika Agarwal
BCA Semester I

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day - 27

CYBER CRIME REPORTING PORTAL

to Stay safe in the online world,it is important to follow important cyber safety practices WHICH MAY HELP IN PROTECTING ourselves.

protect your child from watching more social media

Designed By -
NAKUL GUPTA
BCA Semester I

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affiliated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day - 27

Designed By -
Lakshika Agarwal
BCA Semester I

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day- 28

CERT-In & CYBER SWACHHTA KENDRA (CSK: INDIA'S CYBER SAFETY SHIELD

Protecting India's digital world through awareness, detection, and defense cyber threats.

ABOUT CERT-In

(Computer Emergency Response Team- India)

- National agency under the Ministry of Electronics and IT.
- Handles cyber security incidents, phishing, malware attacks, and vulnerabilities.
- Issues alerts, advisories, and guidelines to safeguard users and organizations.

MOTTO:- "RESPOND-RECOVER-REINFORCE
MOTTO: "RESPOND. RECOVER. RENFORCE".

Safety Tips:-

- ✅ Keep software and OS updated regularly.
- ✅ Don't click on suspicious links or attachments.
- ✅ Report cyber incidents to incident@cert-in.org.in.
- ✅ Follow official advisories and alerts.

ABOUT(CYBER SWACHHTA KENDRA)

- A botnet cleaning and malware analysis centre launched by MeitY.
- Provides free tools to detect and remove malware & botnets from computers and smartphones.
- Promotes digital hygiene and safe cyber practices among citizens.

KEY TOOLS BY CSK:

BOT REMOVAL
to clean infected systems

APP PRATIRODH
prevents unauthorized applications from running

APP SAMVID
protects from malware via USB devices

M-KAVACH
secures Android devices from cyber threats

Safety Tips:-

- ✅ Use CSK tools like Bot Removal Tool
- ✅ Regularly scan your system for malware.
- ✅ Avoid using public Wi-Fi for sensitive activities.
- ✅ Promote cyber hygiene among family and friends.

"STAY CLEAN. STAY SECURE. STAY CYBER SWACHH!"

Designed By -
Hardik Natani
BCA Semester-III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day - 28

Stay Cyber Safe with CERT-In!

A national agency that handles cybersecurity threats and incidents in India.

CERT-In Works To:

- Monitor and respond to cyber incidents.
- Issue alerts and advisories about online threats.
- Provide guidance on cybersecurity best practices.
- Help organizations recover from cyberattacks.
- Promote safe internet use across India.

Cyber Safety Tips (Side Section or Box)

- Use strong passwords and change them regularly.
- Don't click on unknown links or attachments.
- Keep your software and antivirus updated.
- Enable two-factor authentication (2FA).
- Report suspicious activity to CERT-In or cybercrime.gov.in

"Your Data, Your Responsibility!"

Designed By -
Dakshita Yadav
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

AWARENESS POSTER DAY - 29

NATIONAL CYBER SECURITY POLICY

Securing Our Digital Future. Trust. Resillence. Innovation.

Key Initiatives:

- Threst Intelligence
- Data Analytics
- Secure Cloud
- Incident Response

Strategic Pillars:

- Digital Forensics
- Critical Infra Defense
- Privacy Safeguards
- Global Cooperation

Stay Agile, Stay Protected.
Together We Build a Safer Tommorow

Designed By -
Kripa Sunil
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

Awareness Poster Day-29

NATIONAL CYBER SECURITY POLICY 2013/DRAFT 2021

Based on the National Cyber Security Policy 2013 and the Draft National Cyber Security Strategy 2021, India's cybersecurity approach has evolved from a foundational, reactive policy to a comprehensive, proactive strategy.

Designed By -
Chetanya Shekhawat
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee

St. Xavier's College Jaipur

Affilated to the University of Rajasthan
Accredited with A Grade by NAAC (First Cycle, 2025)
An ISO 14001:2015 Certified Institution

WARNING POSTER DAY-4

IMPORTANT FACTS:

-Your data might exposed.
-Passwords can a stolen.
- Identity theft is a real threat

SAFETY TIPS:

Use strong, unique passwords
-Enable Two-Factor Authentication (2fA)

DO'S:

- Monitor financial statements
- Update software regularly

DON'TS

-Reuse passwords
- Click suspicious links

WARNING:
Have You Ever Been PWNED?

Designed By -
Tushar Benedick
BCA Semester III

Organized By -
Department of Computer Science
in collaboration with the
Student Cyber Safety Committee