Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

certin
Enhancing Cyber Security in India

CyberSmart Classroom

Scenario Based Cybersecurity Guide for Teachers & Students

ON THE OCCASION OF

National Cyber Security Awareness Month (October 2026)

"Build a Culture of Cyber Hygiene"

#CyberHygieneOurCulture

ISEA Information Security Education & Awareness

Digital India
Power To Empower

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

certin
Enhancing Cyber Security in India

Table of Contents

Preface 3

1 Social Engineering: “Trust or Trick?” 4

2 Phishing: “Spot the Red Flags” 5

3 AI Safety: “Would You Ask AI This?” 6

4 Malware: “How Does It Get In?” 7

5 Cybersecurity Escape Room 8

Contact us 9

certin
Enhancing Cyber Security in India

Preface

As students spend more time learning, communicating, collaborating, and creating online, understanding cybersecurity has become an essential life skill. Cyber threats are increasingly embedded in everyday digital experiences and may appear as a suspicious message, an unexpected login request, a misleading website, an unknown link, a deceptive voice or video, or a request for personal information. Equipping students with the knowledge to recognise these situations, pause, verify, and make informed decisions can help build safe and responsible digital habits from an early age.

The **Indian Computer Emergency Response Team (CERT-In's) CyberSmart Classroom: Scenario Based Cybersecurity Guide for Teachers & Students** provides teachers with practical and relatable scenarios that can be used to facilitate classroom discussions, activities, and interactive learning. Each scenario encourages students to identify potential risks, think critically, discuss possible responses, and understand simple cybersecurity best practices. By connecting cybersecurity concepts with situations students may encounter in their daily lives, the guide seeks to make cyber awareness engaging, relevant, and actionable, while fostering a culture of responsible digital citizenship.

This booklet has been published as part of **CERT-In National Cyber Security Awareness Month activities (October 2026)**, with the objective of strengthening cybersecurity awareness among students and educators. It is intended to support teachers in creating meaningful conversations around online safety and empowering students to make informed, secure, and responsible choices in the digital world.

1. Social Engineering: “Trust or Trick?”

A — AUTHORITY
I’m from IT.

U — URGENCY
Act immediately.

R — REWARD
Free download.

F — FAMILIARITY
It’s your friend.

SIGNALS

1. Someone calls claiming to be from the school IT department and asks for your password.
2. A person says they are your friend but is using a new account and asks for an urgent money transfer.
3. Someone offers a free game download in exchange for your login details.
4. A student receives a message saying their account will be deleted unless they act immediately.

DECISION PATH

🟢 Probably safe

🟡 Needs verification

🔴 Potential manipulation

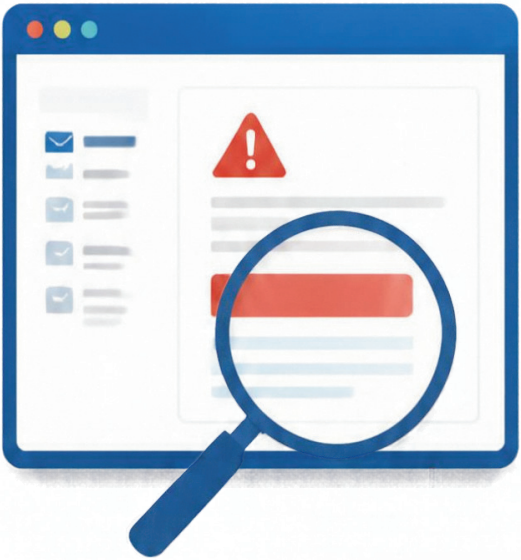
Key lesson:

Attackers may use urgency, authority, fear, curiosity, rewards, or familiarity to influence people.

2. Phishing: “Spot the Red Flags”

Rule students should remember:

STOP → CHECK → VERIFY → REPORT

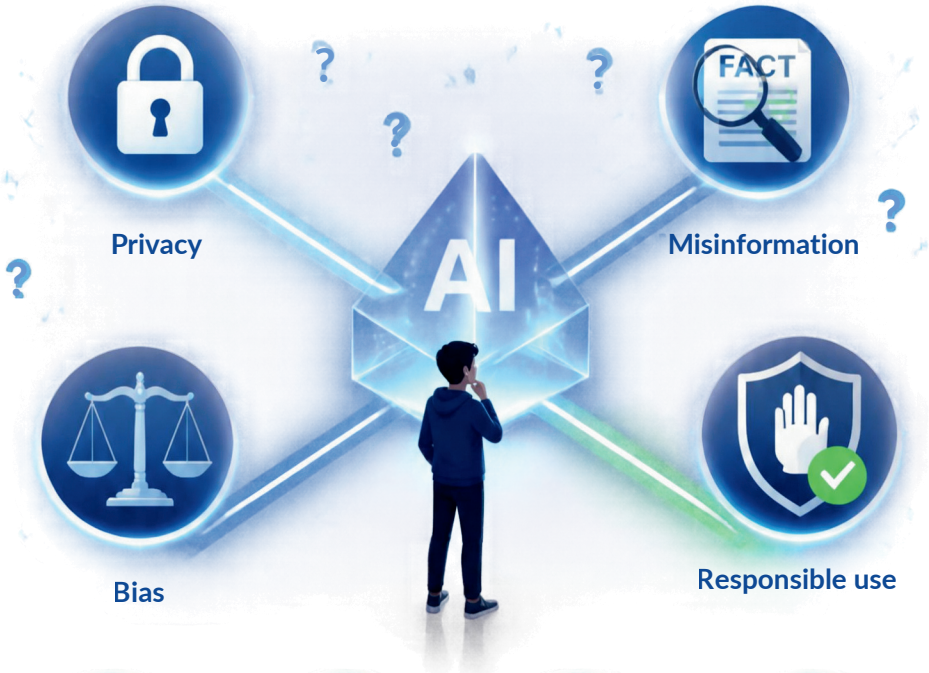


- Suspicious sender addresses
- Urgent or threatening language
- Unexpected attachments
- Requests for passwords or personal information
- Suspicious links
- Spelling/grammar inconsistencies
- Unusual payment requests
- Mismatched website addresses

SAFE | PHISHING

3. AI Safety: “Would You Ask AI This?”

Teach students about:

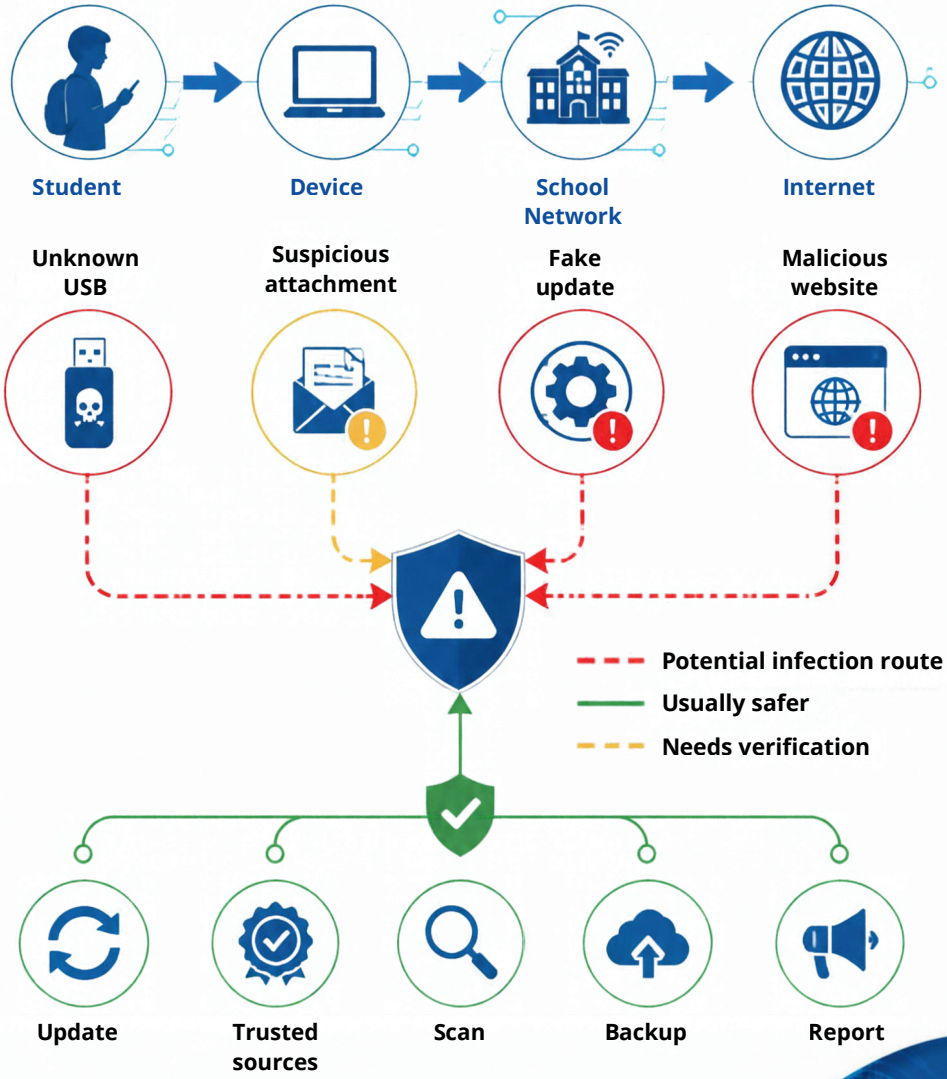


1. Protect personal information
2. Verify important information
3. Consider consequences
4. Responsible use

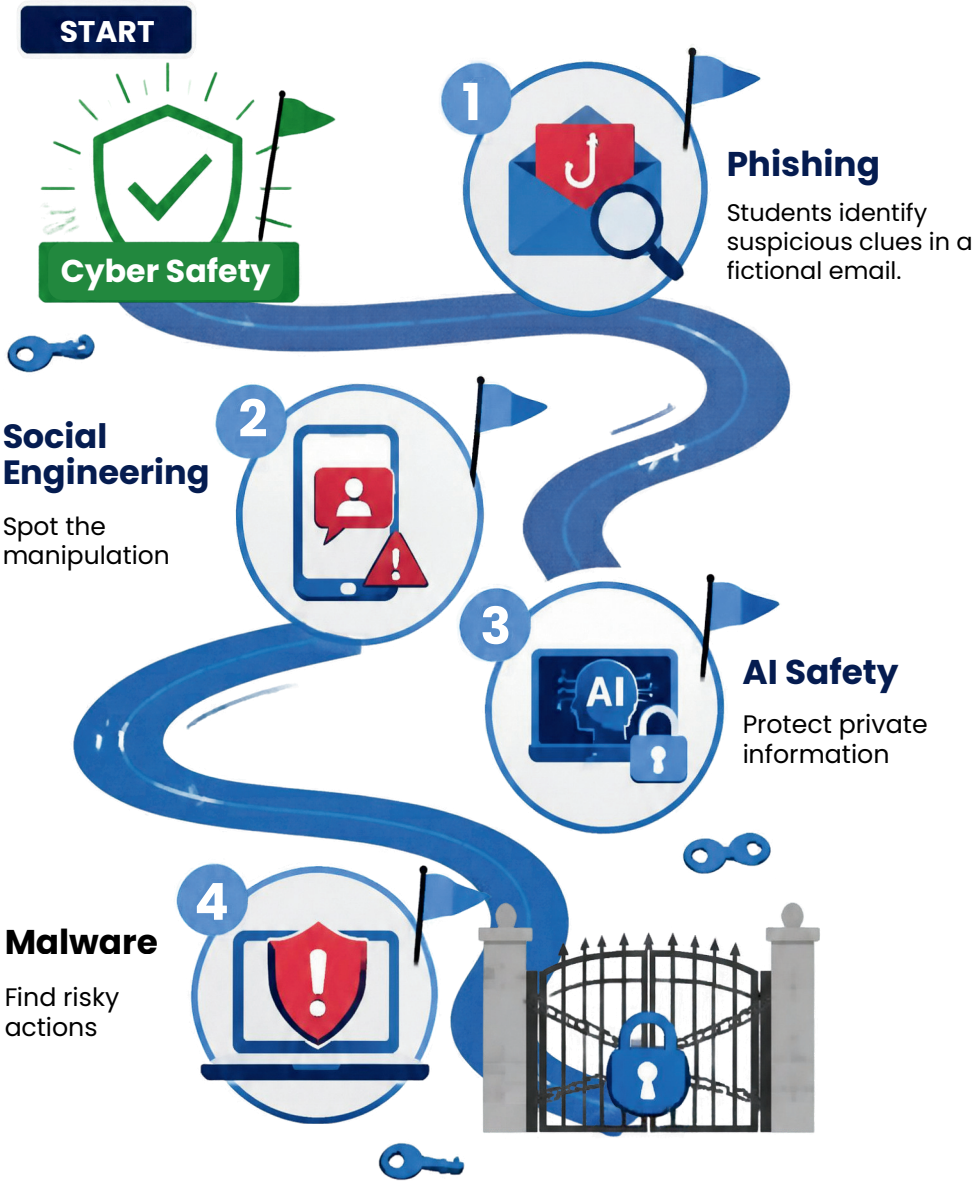
Key lesson

AI can be useful, but students should protect personal information, verify important information, and consider the consequences of what they generate and share.

4. Malware: “How Does It Get In?”



5. Cybersecurity Escape Room



Contact us

For reporting Cyber Security Incidents to CERT-In:

- **Visit website:** https://www.cert-in.org.in/
- **Email:** incident@cert-in.org.in
- **Toll Free Phone:** +91-1800-11-4949
- **Toll Free Fax:** +91-1800-11-6969

Information Desk

- **Phone:** +91-11-22902657

To participate in Training and Awareness sessions, email:

training@cert-in.org.in

FOLLOW US ON

@IndianCERT

@cert_india

AWARENESS BOOKLETS

https://www.cert-in.org.in/AwarenessBooklets.jsp

SECURITY TOOLS

https://www.csk.gov.in/security-tools.html

SCAN ME!