STUDENT BULLETIN BOARD - JUNE 2026

CYBERSECURITY FOR TEENAGERS: STAYING SAFE IN A CONNECTED WORLD

Summary: An awareness article on digital threats, online safety, real-life risk scenarios, facts and figures, and responsible internet use.

The internet is not always what it seems

For today's teenagers, the internet is much more than a source of information. It is a classroom, a gaming zone, a social space, an entertainment hub and a place to build friendships. Smartphones and social media allow teenagers to learn new skills, express themselves and connect with people across the world. However, the same digital world can expose them to cyberbullying, identity theft, online scams, privacy violations and manipulation by people who conceal their true identities.

Cybersecurity is not just about protecting computers from viruses; it is about protecting our identity, privacy, money, reputation and emotional well-being. A teenager does not have to visit a suspicious website deliberately to become a victim. A seemingly harmless message from a friend, a free gaming reward, a fake social media profile or even a photograph shared online can become the starting point of a cybercrime.

The most dangerous online threats are often those that do not look dangerous at first. Understanding how these threats develop is the first step towards preventing them.

Cybersecurity: Why should teenagers care?

Cybersecurity refers to the practices, technologies and precautions used to protect digital devices, online accounts, networks and personal information from unauthorised access, misuse and attacks.

Teenagers are particularly exposed because they frequently use social media, messaging applications, online games, digital payment platforms and educational websites. They may also be more willing to trust someone who appears friendly, popular or similar in age.

A 2024 UNICEF India online-safety poll received 25,626 responses through its U-Report India platform. Among the findings, 40% of respondents reported spending more than four hours online daily. The poll also found that strangers were identified as perpetrators of cyberbullying by 70% of respondents, while peers were identified by 41%. These findings highlight the importance of online safety education and supportive relationships with parents and teachers.

Cybersecurity, therefore, should not be viewed as a technical subject meant only for computer experts. Every teenager who uses a smartphone needs basic digital safety skills.

How danger can occur without warning

Many cybercrimes begin with ordinary online interactions. The following illustrative scenarios demonstrate how a teenager can become vulnerable without initially realising it.

Story 1: The online friend who was not who they claimed to be

A 16-year-old student receives a friend request from someone claiming to attend another school. The person's profile contains photographs, friends, posts and interests that appear genuine. They begin chatting regularly, discussing music, school and personal problems. Gradually, the new friend asks for the student's school name, daily routine and photographs.

The student feels comfortable because the conversations have been friendly for weeks. However, the account may belong to an adult using stolen photographs and fabricated personal details. The information collected could be used to impersonate the student, track their routine, threaten them or manipulate them into sharing private material.

The hidden danger: Trust is built gradually, while the person's real identity remains unverified.

The lesson: An attractive profile, mutual followers or frequent conversations do not prove that someone is trustworthy. Avoid sharing your address, school timetable, live location, passwords or intimate photographs with online acquaintances.

Story 2: The free gaming reward that steals an account

A teenager playing an online multiplayer game sees a message offering free currency, exclusive skins or a rare gaming item. The message directs them to a website that looks almost identical to the game's official login page. Excited by the offer, the teenager enters their username, password and perhaps an email verification code.

The reward never arrives. Instead, the account is taken over, valuable gaming items disappear, and the attacker may use the compromised account to send malicious links to the teenager's friends.

The same technique can target social media accounts and email addresses. Criminals may also use stolen accounts to impersonate the victim and ask friends for money.

The hidden danger: The fake page may look completely genuine, and the victim may not notice anything suspicious until the account stops working.

The lesson: Never log in through unknown reward links. Use official applications and websites, enable two-factor authentication and never share verification codes—even with someone claiming to be a platform representative.

Story 3: The photograph that becomes a weapon

A teenager shares a personal photograph privately with someone they believe is a romantic interest. Later, that person threatens to circulate the image among classmates unless the teenager sends more photographs or transfers money.

In other cases, the criminal may never have received an intimate image at all. They may simply claim to possess one, use a publicly available photograph to create a manipulated image, or threaten to produce a fake image using artificial intelligence.

This form of abuse can involve sextortion, in which someone uses threats or the possibility of exposing intimate material to coerce another person. The Federal Bureau of Investigation (FBI) warns that offenders may initially pose as teenagers or potential romantic partners on social media, messaging platforms and gaming services.

The hidden danger: A friendly conversation can turn into intimidation, and fear of embarrassment may prevent the victim from seeking help.

The lesson: Never give in to threats or blame yourself for being manipulated. Stop responding, preserve relevant evidence, block and report the account, and seek help from a trusted adult and the appropriate authorities. Do not pay or send additional material; payment does not guarantee that the threats will stop.

Facts and figures: The scale of the problem

Cyber threats affecting children and teenagers are not merely hypothetical. Official reports provide evidence of the growing need for digital awareness.

25,626 responses in UNICEF India's 2024 online-safety poll

40% reported spending over four hours online daily

1,823 cybercrime cases against children registered in India in 2022

1,902 cases registered in India in 2023, according to a 2026 government parliamentary response

Source: UNICEF India U-Report and Government of India, Ministry of Home Affairs.

The figures on registered crimes represent cases reported to authorities, not the total number of incidents that actually occurred. Many victims do not report online abuse because of fear, shame, lack of awareness or uncertainty about where to seek help.

International evidence also demonstrates the seriousness of online exploitation. In January 2024, the FBI reported that it and Homeland Security Investigations had received more than 13,000 reports of financially motivated sextortion involving minors between October 2021 and March 2023. These reports involved at least 12,600 victims. The FBI warned that the threats could have devastating consequences for young people.

These statistics demonstrate why cybersecurity awareness must begin before an incident occurs, rather than after a teenager loses an account, faces blackmail or experiences online harassment.

Other cyber threats teenagers should recognise

Cyberbullying and cyberstalking

Cyberbullying includes sending abusive messages, spreading rumours, posting humiliating photographs, creating fake profiles and excluding someone deliberately from online groups. Unlike bullying in a physical setting, online harassment can continue after school hours and spread rapidly to a large audience.

For example, a student shares a funny photograph in a class group. Another student edits it into an embarrassing meme and forwards it to other groups. Within hours, hundreds of students may have seen it. Even if the original post is deleted, screenshots and copies may continue circulating.

Cyberstalking occurs when someone repeatedly monitors, contacts, threatens or tracks another person online. Repeated unwanted messages, attempts to discover someone's location and demands to know their whereabouts should not be dismissed as harmless attention.

Phishing and digital payment fraud

A teenager may receive a message stating that a gaming account will be suspended, a parcel cannot be delivered, or a scholarship payment is pending. The message asks the recipient to click a link and enter personal details.

The link may lead to a fake website designed to steal passwords, banking details or one-time passwords (OTPs). Fraudsters may also impersonate customer-care representatives, school administrators or even relatives.

The important lesson is that a familiar logo, convincing language or urgent message does not establish authenticity. Verify requests independently through official applications or known contact details. Never share an OTP, PIN or password.

Artificial intelligence and deepfakes

Artificial intelligence has made it easier to create convincing fake photographs, voices and videos. A criminal may use a teenager's publicly available photograph to produce a misleading image or imitate the voice of a family member asking for urgent money.

A manipulated image can be used for bullying, reputational damage or blackmail. A voice message that sounds like a friend or parent may also be used to pressure a teenager into revealing information or taking action.

Before believing or forwarding shocking content, verify it with the person concerned through a separate, trusted channel. Avoid sharing personal photographs publicly when unnecessary, and report manipulated content used to threaten or harass someone.

Practical cybersecurity habits every teenager should adopt

Cybersecurity becomes effective when safe behaviour is practised consistently. The following measures can significantly reduce exposure to common threats.

1. Create strong, unique passwords. Avoid using birthdays, names, school details or the same password for every account. Use a reputable password manager if appropriate.
2. Enable two-factor authentication. This provides an additional layer of protection if a password is stolen.
3. Review privacy settings. Restrict who can see posts, contact you, tag you in photographs or access your location.
4. Think before clicking. Avoid suspicious links, unknown attachments, unofficial applications and offers that appear too good to be true.
5. Keep devices updated. Install operating-system and application updates, and download software from official sources.
6. Protect personal information. Do not publish your home address, phone number, live location, school identity card, travel plans or private documents unnecessarily.
7. Be careful with public Wi-Fi. Avoid accessing sensitive accounts on untrusted networks, and never ignore browser security warnings.
8. Check before sharing. A photograph, screenshot, voice note or private conversation may be copied and distributed without your permission.
9. Be respectful online. Do not forward humiliating content, participate in harassment or share someone else's private information.
10. Speak up early. If a message feels threatening, manipulative or uncomfortable, stop engaging and consult a trusted adult.

These recommendations align with online-safety guidance from UNICEF India and cybersecurity awareness material published by India's Computer Emergency Response Team (CERT-In).

What should a teenager do if something goes wrong?

The response to a cyber-incident can make a significant difference. A teenager who discovers that an account has been hacked should immediately change the password from a secure device, secure the associated email account, enable two-factor authentication and sign out other active sessions where possible.

If someone is being bullied, stalked or blackmailed, they should preserve relevant messages, usernames, links and screenshots when safe to do so. They should block and report the offending account, but avoid deleting evidence before seeking advice. If intimate material is involved, do not forward or circulate it, particularly when a minor is depicted.

Most importantly, teenagers must understand that asking for help is not an admission of failure. A victim should not be blamed for trusting someone, clicking a deceptive link or being manipulated. Parents, teachers and counsellors should respond calmly and help the young person take appropriate action.

In India, cybercrime can be reported through the official National Cyber Crime Reporting Portal. The cybercrime helpline 1930 is available for reporting financial cyber fraud. For an immediate threat to personal safety, contact the local police or emergency services.

In a Nutshell: Be digitally smart, not digitally careless

The internet offers teenagers extraordinary opportunities to learn, create, communicate and prepare for their futures. The goal of cybersecurity is not to make young people afraid of technology, but to help them use it confidently and responsibly.

A teenager may be technically skilled at operating a smartphone yet remain vulnerable to emotional manipulation, fake identities and sophisticated scams. Digital awareness requires more than knowing how to use an application; it requires the ability to question, verify, protect and seek help.

Every click, post, message and online friendship involves a choice. Before sharing personal information, accepting a request or responding to an urgent demand, pause and consider the possible consequences.

Remember these five rules: Think before you click. Verify before you trust. Protect before you share. Report before the harm spreads. Ask for help without fear.

Cybersecurity begins with awareness, grows through responsible habits and becomes stronger when teenagers, parents, teachers and technology platforms work together to make the digital world safer.

References:

- https://india.ureport.in/story/1215/?utm_source=chatgpt.com
- https://www.fbi.gov/news/press-releases/sextortion-a-growing-threat-targeting-minors?utm_source=chatgpt.com
- https://www.fbi.gov/news/stories/the-financially-motivated-sextortion-threat?utm_source=chatgpt.com
- https://www.cert-in.org.in/AwarenessBooklets.jsp?utm_source=chatgpt.com
- https://www.unicef.org/india/stay-safe-online?utm_source=chatgpt.com
- https://www.unicef.org/india/reports/my-digital-diary?utm_source=chatgpt.com
- https://cybercrime.gov.in/?utm_source=chatgpt.com
- https://www.pib.gov.in/?utm_source=chatgpt.com

-X-X-X-X-X-X-X-