CYBER SECURITY AWARENESS

"Guard Your Data, Guard Your Future!"

YOUTH FOR SEVA
experience the joy of giving

youth for seva®
experience the joy of giving

TOPICS:

- INTRODUCTION
- ONLINE GAMING - SIDE EFFECTS
- CYBERBULLYING
- HOW TO USE SOCIAL MEDIA
- CYBER PHISHING
- HOW TO REPORT

INTRODUCTION TO CYBER SECURITY

Cyber security refers to the practice of protecting systems, networks, programs, and data from digital attacks, theft, damage, or unauthorized access. As our world becomes increasingly reliant on technology, the importance of cybersecurity has grown exponentially, ensuring the integrity, confidentiality, and availability of sensitive information.

WHAT IS ONLINE GAMING ?....

Gaming refers to playing video games on various platforms like PCs, or mobile devices. It can be both a solo activity and a social experience through online multiplayer games.

Examples of Popular Online Games:

1. Multiplayer Online Battle Arenas (MOBAs): Games like League of Legends.
2. Battle Royale Games: Examples include Fortnite, PUBG, and Apex Legends.
3. Massively Multiplayer Online Role-Playing Games : Games like World of Warcraft
4. Mobile Games: Such as Clash of Clans or Among Us

NEGATIVE EFFECTS OF ONLINE GAMING

Physical Health Issues

- Eye strain and vision problems.
- Poor posture leading to back and neck pain.
- Sleep disturbances due to excessive gaming.

Mental Health Issues

- Compulsive gaming can lead to gaming disorder.
- Competitive gaming can trigger stress and anxiety.
- Excessive gaming can reduce face-to-face social interactions.

Impact on Academics

Decline in Academic Performance:

- Less time for studies due to gaming distractions.
- Procrastination and missed deadlines.

NEGATIVE EFFECTS OF ONLINE GAMING

Behavioral Changes

- Aggression:
- Exposure to violent games can influence aggressive behavior.

- Impatience:
- Fast-paced games can reduce attention spans.

Financial Concerns

- In-App Purchases:
- Spending money on virtual items or subscriptions.

- Risk of Scams:
- Falling victim to online fraud in gaming platforms.

Impact on Academics

Reduced Focus:

- Decreased concentration during lessons or while studying.

REGULATION AND BANS ON ONLINE GAMES

- States in India have banned certain online games, games like PUBG Mobile were banned in 2020 due to concerns about gaming addiction, security, and national security issues.

- In 2023, the government also introduced rules to regulate online gaming platforms, which include provisions for making gaming more transparent, ensuring that platforms follow responsible gaming practices, and preventing any form of gambling.

- Some states like Telangana and Tamil Nadu have proposed outright bans on certain online gaming apps.

REAL-WORLD EXAMPLES:

- New Delhi: 16-year-old boy killed his cousin in Nagaur, Rajasthan to pay off debts he amassed playing online games.

- Rajasthan: 16-year-old boy kidnapped his 12-year-old cousin and demanded ransom from his family. At present, such incidents are being reported all over the country, where children are stealing and committing crimes in their own homes to play online games.

- Chhattisgarh's Bilaspur: A**19-year-old** boy created a false story of **his kidnapping** because of online gaming addiction.

In a survey conducted in India last year, 65 percent of children under the age of 20 said that they were ready to give up food and sleep to play online games.

WHAT'S BEING DONE?

- Regulation: As mentioned earlier, the Indian government is trying to implement stricter regulations on online gaming, especially in areas concerning the well-being of users. The government has also moved to regulate "real money" gaming, particularly around fantasy sports and other games that involve betting.

- Awareness Campaigns: Many organizations and mental health experts are running campaigns to raise awareness about the risks of gaming addiction and to promote healthier gaming habits.

- Self-regulation by Industry: Some gaming companies are taking steps to address addiction and mental health issues, such as incorporating features that limit playtime or offer breaks for users who play too long.

CYBERBULLYING:

Cyberbullying is using digital platforms (social media, messaging apps, gaming platforms, etc.) to harm, harass, or intimidate others.

Examples:

- Sending hurtful messages or threats.
- Spreading rumors online.
- Sharing embarrassing photos or videos without consent.

HOW CYBERBULLYING HAPPENS?

Platforms Used:

Social Media
(Instagram, Facebook, TikTok).
Messaging Apps
(WhatsApp, Snapchat).
Online Games
(chat features).

Forms of Cyberbullying:

- Flaming: Aggressive arguments in public forums.
- Outing: Sharing private information publicly.
- Doxxing: Exposing someone's personal details online.

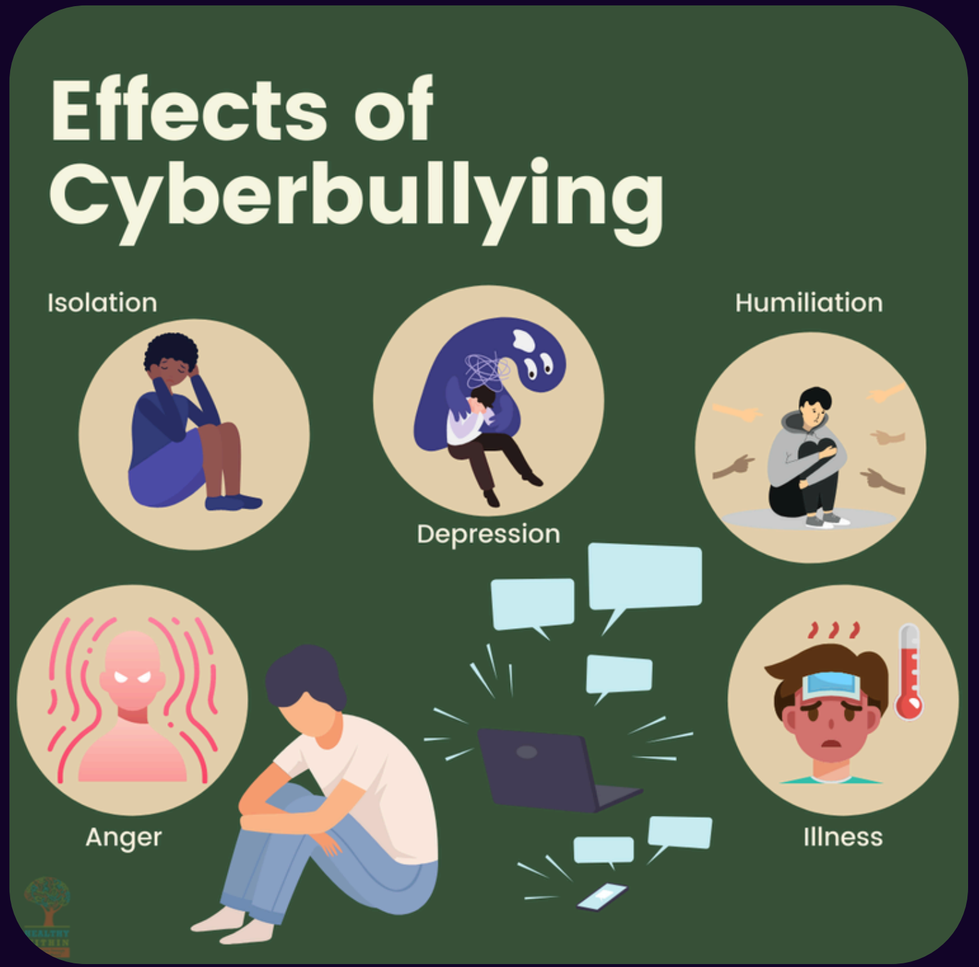
Children have a variety of experiences with Cyber Bullying.

IMPACT OF CYBERBULLYING

Emotional Effects:
Anxiety, depression, and low self-esteem.
Feelings of isolation or helplessness.

Academic Effects:
Difficulty concentrating on studies.
Decline in academic performance.

Physical Effects:
Sleep disturbances and health issues caused by stress.



SIGNS SOMEONE IS BEING CYBERBULLIED:

1. Avoiding social media or online interactions.
2. Changes in mood or behavior (e.g., becoming withdrawn or irritable).
3. Unexplained drop in grades or lack of interest in activities.
4. Refuse to use their phone or computer.

RESPONDING TO CYBERBULLYING

1. Talk to a trusted adult, teacher, or counselor.
2. Document the Abuse.
3. Block and Report.
4. Do Not Respond in Anger.

THE TIMES OF INDIA

Opinion | Times View | Times Evoke | City | India | World | Entertainment | Sports | Spirituality | Business | Environment | ...

NEWS / VOICES / INDIA / "Cyberbullying in India: A growing concern for parents and educators"

INDIA

"Cyberbullying in India: A growing concern for parents and educators"

- India has the highest rate of cyberbullying worldwide, at over **85% of children** reporting it.
- In India, **46% of children reported cyberbullying a stranger**, compared to 17% globally, while 48% reported cyberbullying they know, compared to 21% of children in other nations.
- Spreading false rumours (39%), being excluded from chats or groups (35%), and name-calling (34 per cent) were the top three types of cyberbullying reported in India.

WHAT IS SOCIAL MEDIA?

Social media refers to digital platforms and apps that enable users to create, share, and interact with content, such as text, images, and videos, and to connect with others online.

Here are some of important steps you should take to protect yourself and your information while using social media platforms:

1) Do not accept friend requests from strangers on social networking sites.
2) Do not trust online users unless you know and can trust them in real life.
3) Do not share your personal information such as address, phone number, date of birth etc. on social media. Identity thieves can easily access and use this information.
4) Do not share your sensitive personal photographs and videos on social media.

5) Share your photos and videos only with your trusted friends by selecting right privacy settings on social media.
6) Immediately inform the social media service provider, if you notice that a fake account has been created by using your personal information.
7) Always use a strong password by using alphabets in upper case and lower case, numbers and special characters for your social media accounts.
8) Do not share your vacations, travel plans etc. on social media.
9) Do not allow social networking sites to scan your email account to look for your friends and send spam mails to them without your consent or knowledge.
10) Always keep location services turned off on your devices unless necessary.

11) Do not announce your vacations, travel plans etc. on social media. Criminals can use it as an opportunity for theft etc.

12) When chatting with someone online and you feel suspicious about your chat partner, try asking some unrelated scientific or mathematical questions. If it does not answer or acknowledge the question, it may mean that you are chatting with an automated computer bot.

13) Do not use public computer/ cyber cafe to access social networking websites, it may be may be infected/ installed with a key logger application which will capture your keystrokes including the login credentials.

14) Many social networking sites prompt you to download third-party applications that lets you access more pages. Do not download unverified third-party applications without doing research about its safety.

15) Do not hesitate to report, if someone is posting offensive and abusive content on social media.

16) Do not share or forward unverified posts/ news on social media forums. These may contain fake news or contain sensitive information which may mislead people.

CYBER PHISHING

Cyber phishing is a way scammers trick people into giving away sensitive information like passwords, credit card details, or personal data.

It usually happens through emails, social media, fake websites, text messages, or phone calls.

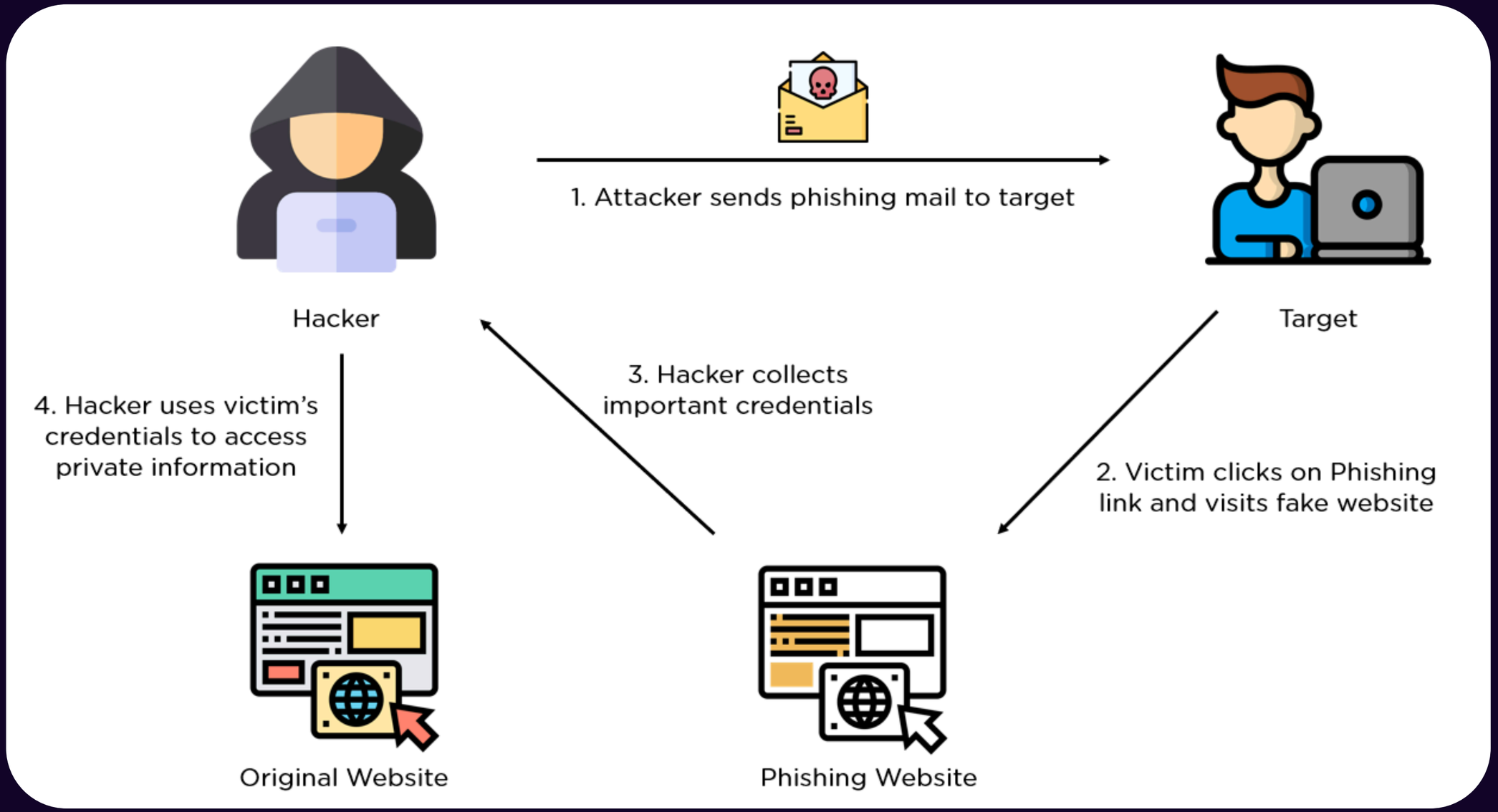
It's important for students to recognize phishing since it can target anyone, even through school emails or social media accounts.

TYPES OF PHISHING ATTACKS

- **Email Phishing:** Fake emails pretending to be from teachers, schools, or companies like Netflix.
- **Spear Phishing:** Targeted attacks that use information about you, like your school or hobbies.
- **Whaling:** Scams aimed at important people like school administrators or parents.
- **Clone Phishing:** Duplicating real emails but changing links to steal your info.
- **Smishing and Vishing:** Phishing through text messages and phone calls.

HOW PHISHING WORKS?

- **Bait Creation:** Scammers create convincing messages or fake websites.
- **Delivery:** Sending emails, texts, or social media messages.
- **Hooking Victims:** Getting you to click a link, download something, or share personal info.
- **Exploitation:** Stealing your information or installing harmful software.
- **Execution:** Using your data for fraud, identity theft, or other crimes.


Hacker
1. Attacker sends phishing mail to target
Target
4. Hacker uses victim's credentials to access private information
3. Hacker collects important credentials
2. Victim clicks on Phishing link and visits fake website
Original Website
Phishing Website

REAL-WORLD EXAMPLES

Over 1,000 Indian schools, colleges targeted in cyberattacks in Jun-Sep: Report

Cybercriminals prefer email services like Gmail as they are free, easy to register, and widely used. To make emails look legitimate, attackers would send emails loaded with terminology such as principal, head of department, school

CONSEQUENCES OF FALLING FOR PHISHING:

1. Losing access to your accounts, like social media or email.
2. Having your personal information stolen, leading to identity theft.
3. Financial losses if scammers get your bank details.
4. Embarrassment if your accounts are used to scam others, like your friends or classmates.

HOW TO STAY SAFE FROM PHISHING?

Learn to Spot Scams

Stay informed about common phishing tactics.

https://phishtank.org/

Double-Check

Verify emails, links, or requests before clicking.

https:/who.is/

Use Tech Tools

- Enable multi-factor authentication (MFA) on your accounts.
- Keep your software and apps updated.
- Use spam filters to catch suspicious emails.

EMERGING TRENDS IN PHISHING:

AI and Deepfakes

Scammers using advanced technology to create fake videos or voices.

Gaming & Social Media Scams

Targeting students where they hang out online.

Personalized Attacks

Using info from social media to create more convincing scams.

3 Easy Ways to Report Cyber Crime in India;

Everything You Should Know

1. **Report cybercrime via phone call.**
   You can report any type of cyber fraud by dialing the helpline number of the National Cyber Crime Reporting Portal which is 1930.

2. Report cybercrime via the online portal: https://cybercrime.gov.in

3. **Alternative Ways to report cybercrime.**
   You can also report cyber crime to the respective website on which the incident has happened. Most social media websites including Facebook, YouTube, Twitter, and Instagram have the option of reporting offensive content.

THANK YOU!

youth for seva®
experience the joy of giving