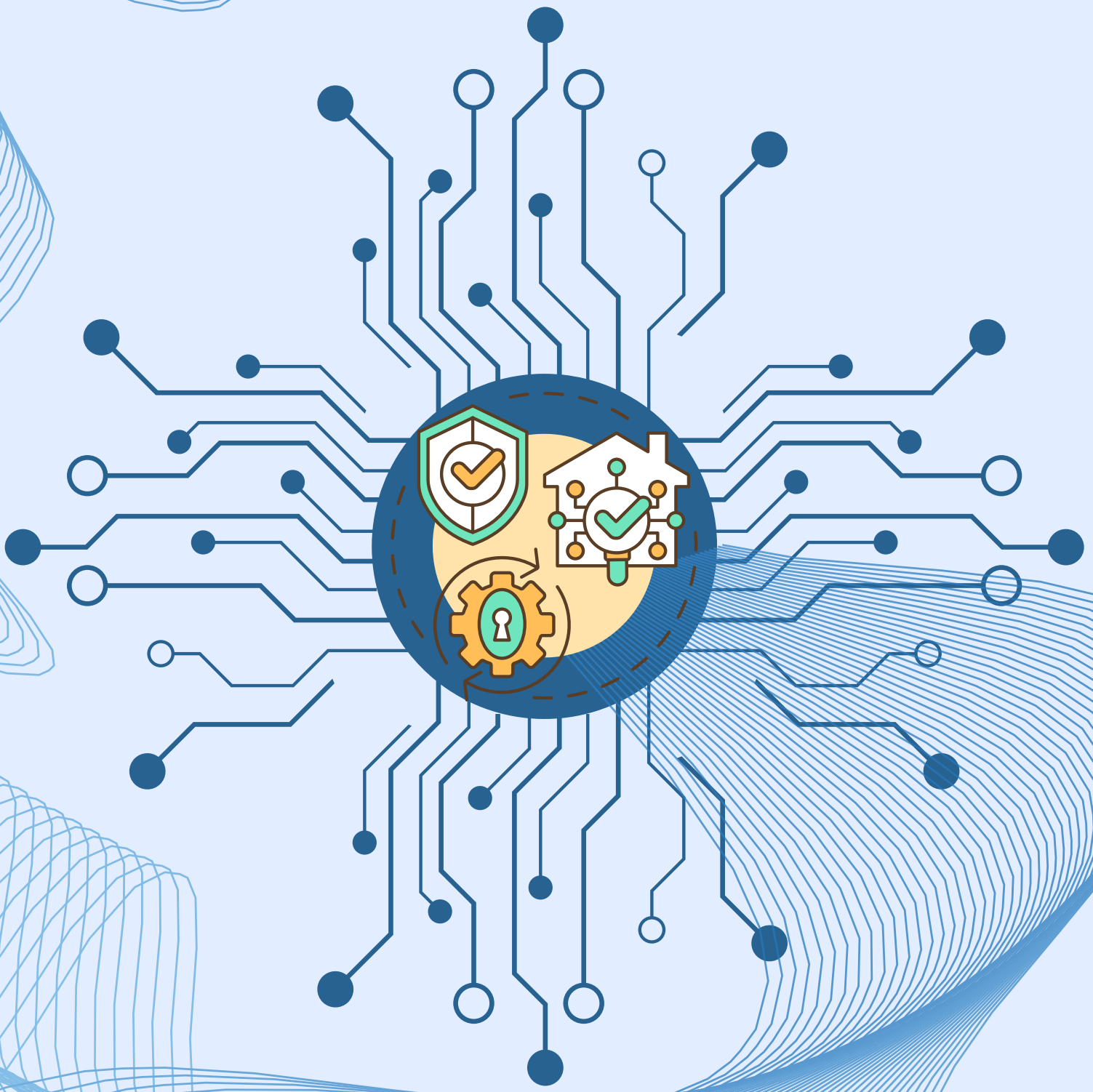
EMPOWERING CYBER AMBASSADORS

A Journey Through
Cyber Ambassador Program Phase III



INDEX

Hello Students,

Welcome to the Cyber Ambassador Platform, Phase-III a training program on Cyber Safety and Security. Women Safety Wing, Telangana Police as a part of Cyber Ambassador Platform so far trained around 12000 Students from 4000 Govt schools on Cyber Safety who in turn created awareness among all other students of the schools and also community at large. Now it is your turn to get trained on Cyber Safety which is the need of the hour. You are lucky enough to have innovative way of training in digital mode in the form of captivating Videos, Infographics, Comics and Quiz.

This course will help you to find all the positive practices of our day-to-day lives while using the internet. It is designed in a fun, interactive manner to allow you to assimilate the material easily. The entire course is covered over the span of five days where you will learn about Cyber Hygiene, Netiquettes, Online games, Cyber addiction, Online predators, Child online activity protection, Cyber Stalking, email and password threats, Credit card scams, Phishing, Mobile security, Social networking and many more.

Once you undergo this training you will be identified as ***CYBER AMBASSADORS*** and with the knowledge gained, you will be made to create awareness on Cybercrimes, Cyber safety and cyber security among other students of the school and also in your neighborhood by organizing community outreach programs in coordination with She teams thus creating a safe cyber space to all citizens. Our SHE teams will be coordinating with you through your mentor teachers and in case of any doubt you should feel free to contact them though the mentor teachers. Hope you will learn keenly and get benefit of the course. Upon successful completion of the course, you will receive a course completion certificate from Women Safety Wing, Hyderabad police department.

Ms. Shikha Goel, IPS
ADGP WSW, Telangana

Dear Cyber Ambassadors,

Congratulations on completing Phase III of the Cyber Ambassador Program! Your dedication and commitment to enhancing cyber awareness among your peers are commendable. As you embark on your journey as Cyber Ambassadors, equipped with knowledge and skills to navigate the digital world responsibly, we present to you "Empowering Cyber Ambassdors: A Journey Through Cyber Ambassador Program Phase III."

This book serves as a comprehensive resource, encapsulating the vital lessons and insights gained throughout your Cyber Ambassador journey. Through engaging infographics and concise explanations, it revisits the fundamental concepts and practices of cybersecurity, ensuring that you retain and reinforce your understanding of crucial topics.

In this digital era where technology permeates every aspect of our lives, the need for cyber awareness and vigilance has never been more critical. As Cyber Ambassadors, you play a pivotal role in promoting a safer online environment within your school community and beyond. This book not only aids in revising the materials covered in Phase III but also empowers you to continue educating others about cyber threats, data privacy, online safety, and responsible digital citizenship.

Remember, knowledge is power, and with it comes the responsibility to act. Let this book be your companion as you advocate for cyber awareness, inspire your peers to adopt secure online practices, and champion a culture of digital responsibility.

We applaud your dedication to becoming proactive agents of change in the digital landscape. Together, let us strive to create a safer and more secure cyber world for all.

Best wishes,
Dr. Vishnu Ramdeo,
Chief Executive Officer,
Cyber Secura Pvt. Ltd.

CYBER HYGIENE

CYBER SECURA

Cyber hygiene is a set of habitual practices for ensuring the safe handling of critical data and for securing networks.

Cyber hygiene is one of the most underrated things now a days. People use the internet for fun or work purposes but some people use internet for their criminal activities.

DO's for Cyber Hygiene

- Never visit unknown website.
- Always check website permissions or its cookies or data access.
- Always access unknown or untrusted websites using VPN only.
- Be careful while downloading programs from the internet because they can carry malware or malicious codes. So always can the program first before downloading.

DONT's for Cyber Hygiene

- Never share your bank details on untrusted websites.
- Never share personal identity with anyone on internet.
- Never use easy-to-guess passwords which are available in a dictionary.
- Never bully aur troll anyone on internet.

Cybercrime in India has increased **400%** as compared to the last year.

49% of cyber attacks target small businesses.

NETIQUETTES

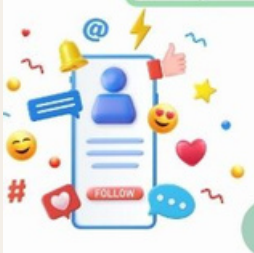
By practicing netiquette, we create a positive and respectful online environment. Let's strive to communicate with courtesy, empathy, and respect to build a thriving online community.

Email Etiquette:

- Use a professional tone and proper greetings.
- Keep emails concise and to the point.
- Use clear and relevant subject lines.

Social Media Etiquette:

- Be respectful and considerate in your interactions.
- Avoid offensive language and personal attacks.
- Respect others' privacy and permissions.



Online Communication:

- Use proper grammar and spelling to enhance clarity.
- Avoid using all caps, as it signifies shouting.
- Be mindful of cultural differences and language nuances.

Cyberbullying Prevention:

- Treat others with kindness and empathy even when you are online.
- Report and block abusive behavior.
- Do not engage in or share harmful content.

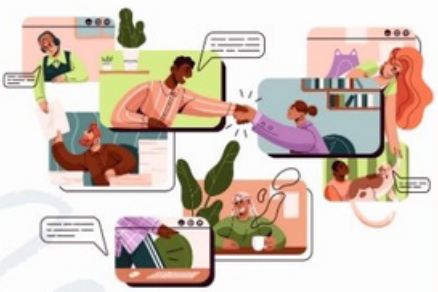
Copyright and Attribution:

- Respect copyright laws and intellectual property.
- Give proper credit and attribution when using or sharing others' content.

Privacy and security:

- Protect your personal information and privacy online.
- Use strong, unique passwords and enable two-factor authentication.
- Be cautious of phishing attempts and online scams.

Online Community Etiquette:



- Embrace diversity and respect different opinions.
- Avoid hate speech or discriminatory language.
- Engage constructively and contribute positively to discussions.

Online class netiquettes

By practicing netiquette in online classes, you can create a positive and conducive learning environment. Let's engage with courtesy, respect, and professionalism to make the most of our online class experience.

Video Conferencing Etiquette

- Mute yourself when you are not speaking to minimize background noise.
- Maintain eye contact by looking at the camera.
- Dress appropriately and maintain a professional appearance.

Participating in Discussions

- Be respectful to peers and instructors in your responses.
- Stay on topic and contribute meaningfully to discussions.
- Avoid disruptive behavior like talking over others or using inappropriate language.

Timeliness and Preparedness

- Log in to the class on time and be prepared with the required materials.
- Meet deadlines for assignments and submissions.
- Communicate in advance if you anticipate any challenges in meeting deadlines.

Professional Communication

- Use clear and concise language in your online communication.
- Use proper grammar, spelling, and punctuation.
- Avoid using informal language or excessive abbreviations.

Respecting Peers and Instructors

- Listen actively and respectfully to others' viewpoints.
- Value diversity of opinions and engage in constructive discussions.
- Use respectful and appropriate language and tone in all interactions.

Technical Troubleshooting

- Check your internet connection and ensure it is stable.
- Keep your software and applications up to date.
- Reach out to technical support for assistance with any technical issues.

Public Computers & WiFi

Benefits of Public Computers and Wi-Fi

- Convenient access to the internet and digital resources.
- Increased connectivity for work, study, and communication.
- Accessibility for individuals without personal devices.

Risks of Public Computers and Wi-Fi

- Security threats like malware, keyloggers, and hacking attempts.
- Privacy concerns due to shared devices and networks.
- Potential exposure to phishing attacks and scams.

Protecting Personal Information

- Never enable automatic login on public computers.
- Use strong, unique passwords for each account.
- Log out of accounts and clear saved credentials.

Wi-Fi Safety

- Connect to trusted networks and avoid open or unsecured networks.
- Use a virtual private network (VPN) for encrypted connections.
- Avoid accessing sensitive information (e.g., online banking) on public networks.

Reporting Suspicious Activity

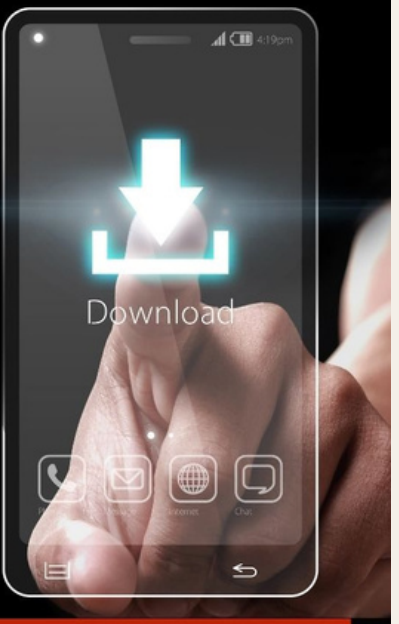
- Report any unusual or suspicious activity encountered on public computers.
- Notify authorities or staff about security breaches or concerns.
- Help protect others by sharing information about potential risks.

Responsible Usage and Cleanup

- Respect others' privacy and avoid accessing personal files.
- Log out of all accounts and close all applications before leaving.
- Safely discard any temporary files or documents saved during your session.

CYBER SECURA

Download Safe

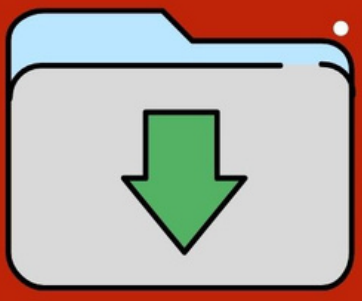


Just as you would take precautions for safe online shopping, you should be equally careful when you download files to your device. Viruses, malware, and Trojans (misleading malware) are more rampant than ever—which is why you should take caution before you download something.

How to download safely?

- **Download only from reputable sites and sources**

- One step you should always take before you download anything is to scan it for viruses. If you download a file before you scanned for viruses, be sure not to open or run the file until you've made sure it's clean.



- Download executable files (.exe) with extreme caution. These are files used by programs to run on your computer. However, they are also commonly used in viruses.

MALWARE VS VIRUS

A program designed to gain access to computer systems, normally for the benefit of intruders, without the user's permission.

The full form of malware is Malicious software.

Various types of malware are viruses, trojan, worm, spyware, adware, and ransomware.

The virus is a malicious executable code of the malware family, attached to another executable file that can harm by modifying or deleting data.

The full form of the virus is Vital Information Resource Under Seize.

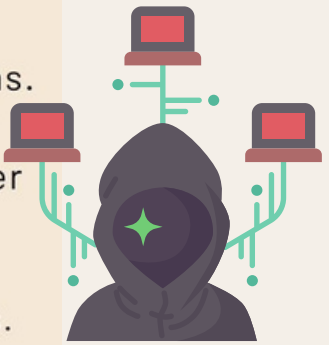
Types of viruses are boot sector, multipartite, space filler, file infector, resident, direct action, macro.

HOW TO SAVE A COMPUTER FROM MALWARE?

1. Use an effective antimalware program.

2. Learn how to recognize malicious programs. Keep an eye out for applications that look or behave suspiciously, as well as your computer running slowly or overheating.

3. Avoid downloads from suspicious websites.
4. Use a firewall.



WOMEN SAFETY WING

TELANGANA POLICE

MISSION

Our objective is to support partners to become self-reliant and capable of leading their own development journeys. We make progress toward this by reducing the reach of conflict, providing necessary support, and reducing transactional crime and other safety Issues. We promote women prosperity through skill training and other necessary support systems.

VISION

Our vision is to establish a 'gender equal' state where women are partners in progress. TSWSW seeks to create a level playing field promoting excellence devoid of gender discrimination working in tandem with partners locally and in national coalitions.

If you ever need help or guidance regarding today's issues and your safety, don't hesitate to reach out to us on social media.

FACEBOOK :
https://www.facebook.com/tswomensafety
https://www.facebook.com/TelanganaSheTeams
https://www.facebook.com/TSAHTofficialPage
https://www.facebook.com/PridePlace.WSW.TS/
https://www.facebook.com/BharosaWomenSafetyWing/

TWITTER :
https://twitter.com/ts_womensafety
https://twitter.com/TS_SheTeams
https://twitter.com/TSAHTofficial
https://twitter.com/PridePlace_WSW
https://twitter.com/Bharosa_TSWSW

INSTAGRAM :
https://instagram.com/womensafetywing_ts
https://www.instagram.com/tsahtofficial/
https://www.instagram.com/telanganasheteams/
https://www.instagram.com/prideplace.wsw.ts/

Website:
https://www.womensafetywing.telangana.gov.in/
She team state what's app number: 9441669988
Reception number: 9440700906

CHILD LINE NUMBER	CYBER CRIME NUMBER	CYBER CRIME WEBSITE
1098	1930	CYBERCRIME.GOV.IN

ONLINE GAMES

CAUSES OF ONLINE GAME ADDICTION

Easy Accessibility:

- The widespread availability of online games makes them easily accessible to children.
- The convenience of playing games on various devices contributes to addiction.

Social Interaction:

- Online games often provide a platform for social interaction, which can be addicted for children seeking companionship and acceptance.

SYMPTOMS OF ONLINE GAME ADDICTION

Withdrawal Symptoms:

- Restlessness, irritability, and mood swings when not playing online games.
- Difficulty in controlling impulses to play games.

Neglected Personal Hygiene and Sleep Patterns:

- Neglecting personal hygiene, skipping meals, and irregular sleep patterns due to excessive gaming.

Decline in Academic Performance:

- A noticeable decline in school performance, reduced interest in studies, and poor concentration.

Social Isolation:

- Spending less time with family and friends, withdrawal from social activities, and preferring online interactions over real-life connections.

PREVENTION TIPS

Set Clear Boundaries:

- Establish clear rules regarding screen time and gaming schedules.
- Encourage children to balance gaming with other activities.

Encourage Alternative Activities:

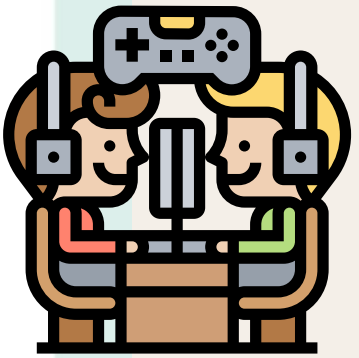
- Promote participation in physical activities, hobbies, and social interactions to divert attention from online games.

Foster Open Communication:

- Create an environment where children feel comfortable discussing their gaming habits and concerns.
- Encourage dialogue about the consequences of excessive gaming.

Seek Professional Help:

- If the addiction persists or worsens despite preventive measures, seek professional guidance from therapists or counselors specialized in gaming addiction.



CYBER ADDICTION

WHAT IS CYBER ADDICTION?

- Cyber addiction refers to the excessive and compulsive use of digital devices and online activities.
- It leads to a loss of control over one's online behaviors and negatively impacts various aspects of life.

SIGNS OF CYBER ADDICTION

- Spending excessive time online, neglecting personal responsibilities.
- Experiencing mood swings, irritability, or restlessness when disconnected.
- Withdrawing from real-life social interactions and preferring online interactions.

RISKS OF CYBER ADDICTION

- Impact on Mental Health:
  - Increased risk of depression, anxiety, and feelings of loneliness.
  - Difficulty in managing emotions and reduced self-esteem.
- Impact on Physical Health:
  - Sedentary lifestyle leading to weight gain and decreased physical fitness.
  - Sleep disturbances and disrupted sleep patterns due to excessive screen time.

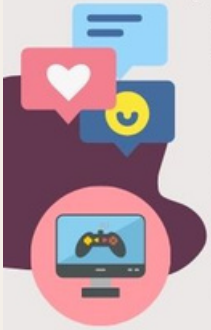
STRATEGIES FOR FINDING BALANCE

1. Engaging in Offline Activities:
   - Encourage participation in physical activities, hobbies, and social interactions.
   - Explore new interests and engage in activities that do not involve digital devices.
2. Practicing Digital Detox:
   - Take periodic breaks from digital devices.
   - Allocate time for relaxation, meditation, or pursuing offline activities.
3. Building a Support Network:
   - Foster open communication with family and friends about digital habits.
   - Share experiences, challenges, and strategies to maintain a healthy digital lifestyle.

ONLINE PREDATORS AND CHILD ONLINE ACTIVITY PROTECTION

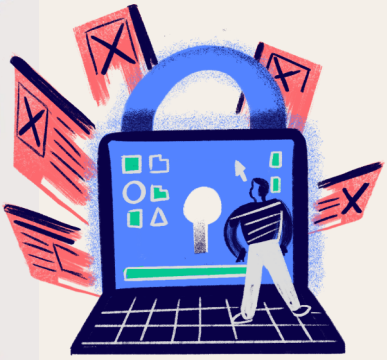
1 What are Online Predators?

- Online predators are individuals who use the internet to target and exploit children for various purposes, including grooming, exploitation, or identity theft.
- They often disguise their true identities and intentions to gain trust and manipulate children.



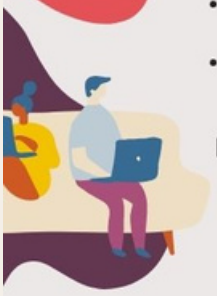
2 Signs of Online Predation:

Signs may include secretive behavior, excessive time spent online, receiving gifts or money from unknown individuals, or sudden changes in mood or behavior.



3 Protecting Children Online:

- Set clear boundaries and guidelines for internet usage.
- Encourage the use of strong, unique passwords and safe online practices.
- Regularly update and monitor privacy settings on social media platforms.
- Educate children about the risks of engaging with strangers online.

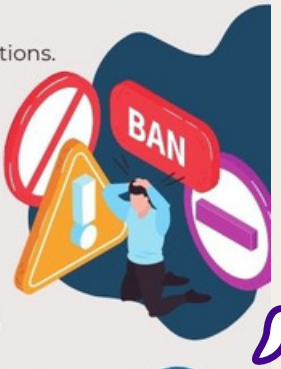


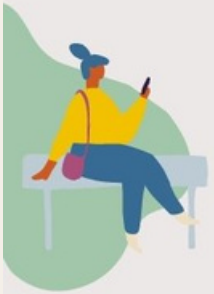
4 Parental Controls and Monitoring:

- Limit access to inappropriate content.
- Track online activities and screen time.
- Receive alerts for potentially risky or harmful behavior.
- Use filtering systems to block or restrict certain websites or applications.

5 Communication and Trust:

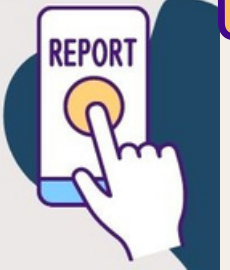
- Create a safe and non-judgmental space for children to discuss their online experiences.
- Encourage them to seek help if they feel uncomfortable or threatened online.
- Assure them that they can rely on you for support and guidance.





6 Reporting Suspicious Activity:

- Instruct them to save any evidence, such as messages or screenshots.
- Provide information on relevant reporting channels or organizations, such as local law enforcement or the National Center for Missing and Exploited Children (NCMEC).



CYBER SPACE AND PREVENTION MEASURES

1 What is Cyber Space?

- Cyber space refers to the interconnected digital world where information is exchanged, accessed, and shared.
- It encompasses the internet, networks, devices, and digital communication platforms.

2 Protecting Personal Information:

- Avoiding oversharing on social media platforms.
- Using secure Wi-Fi connections, especially for sensitive activities.
- Being cautious with online transactions and only providing necessary information to trusted websites.

3 Social Media Safety:

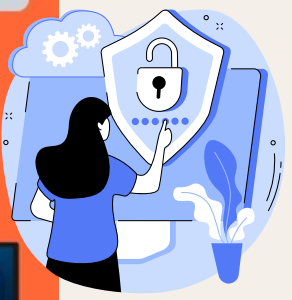
- Adjusting privacy settings to control who can view your profile and posts.
- Being mindful of what you share publicly and considering the potential consequences.
- Avoiding interactions with unknown individuals and being cautious of friend requests or messages from strangers.

4 Cyber Hygiene:

- Regularly backing up your data to protect against loss or ransomware attacks.
- Managing your devices securely by using strong passwords, biometric authentication, or device encryption.
- Practicing safe file sharing, scanning attachments for malware, and being cautious when downloading files from the internet.
- Using reputable websites and ensuring they have secure payment gateways (look for "https" and a padlock symbol).

5 Reporting Cyber Incidents:

- Contacting your local law enforcement or cybercrime reporting agencies.
- Informing relevant organizations, such as your internet service provider or the website/platform where the incident occurred.



Cyber Stalking

What is Cyber Stalking?

- Cyber stalking is the malicious and persistent harassment, intimidation, or tracking of an individual using digital means.
- It involves unwanted and intrusive behaviors carried out through online platforms, emails, social media, or messaging apps.

IMPACT OF CYBER STALKING:

- **Emotional Distress:** Victims may experience fear, anxiety, and loss of privacy.
- **Psychological Harm:** It can lead to stress, depression, and a sense of powerlessness.
- **Social Isolation:** Victims may withdraw from friends, family, and online activities due to fear or mistrust.

RECOGNIZING CYBER STALKING

- **Persistent and Unwanted Contact:** Receiving repeated and unsolicited messages or friend requests.
- **Stalking Behavior:** Frequent monitoring of online activities, comments, and interactions.
- **Invasion of Privacy:** Unwanted dissemination of personal information or images without consent.

PROTECTING YOURSELF

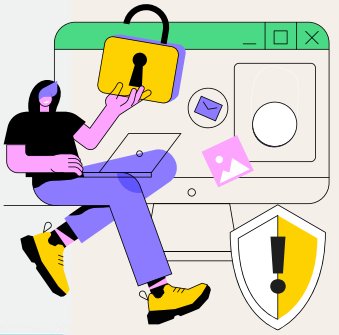
- **Use Strong Privacy Settings**: Regularly review and update privacy settings on social media platforms.
- **Be Mindful of Sharing Personal Information:** Avoid sharing sensitive details publicly or with unknown individuals.

ONLINE COMMUNICATION SAFETY

- **Create Strong Passwords:** Use a combination of letters, numbers, and symbols for secure passwords.
- **Be Cautious with Clicking Links:** Avoid clicking on unknown or suspicious links in emails, messages, or social media.
- **Beware of Phishing Attempts:** Be skeptical of requests for personal information or financial details from unknown sources.

REPORTING CYBER STALKING

- **Document Evidence:** Save screenshots, messages, or any evidence of cyber stalking incidents.
- **Report to Authorities:** Contact local law enforcement or specialized cybercrime units to report the incidents.
- **Utilize Online Reporting Tools:** Report cyber stalking incidents to relevant platforms or social media networks.



ENCOURAGE INDIVIDUALS TO STAY INFORMED, BE VIGILANT, AND PRIORITIZE THEIR ONLINE SAFETY.

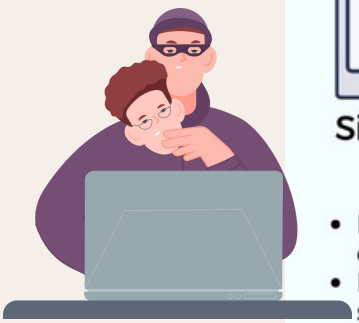
ONLINE GROOMING

What is Online Grooming?

Online grooming is the process in which a predator builds trust with a potential victim online, often with the intention of exploiting them emotionally, sexually, or financially.

2 Common Grooming Tactics:

- **False Identity:** Predators create fake profiles or use stolen identities to appear trustworthy.
- **Building Trust:** Predators invest time and effort to develop a bond with the victim, gaining their confidence.
- **Emotional Manipulation:** Predators exploit their victims' vulnerabilities, making them dependent on the relationship.
- **Secrecy and Isolation:** Predators encourage victims to keep the relationship secret and cut ties with friends and family.
- **Exploitation:** Once trust is established, predators may request explicit photos, engage in sextortion, or attempt offline meetings.



Signs of Grooming: 3

- Excessive secrecy about online activities.
- Drastic changes in behavior, such as withdrawal from family and friends.
- Receiving gifts or money from an unknown person.
- Spending excessive amounts of time online, especially during odd hours.
- Becoming emotionally attached to someone they only know online.

4 Protecting Yourself from Grooming:

- **Education and Awareness:** Learn about the dangers of online grooming and share this knowledge with others.
- **Privacy Settings:** Regularly review and adjust your privacy settings on social media platforms and online accounts.
- **Strong Passwords:** Use unique, complex passwords for your online accounts and update them regularly.
- **Think Before Sharing:** Be cautious about sharing personal information, photos, or videos with strangers online.
- **Trust Your Instincts:** If something feels uncomfortable or suspicious, trust your instincts and seek help from a trusted adult.
- **Open Communication:** Maintain open and honest communication with your parents, guardians, or teachers about your online activities.

EMAIL THREATS

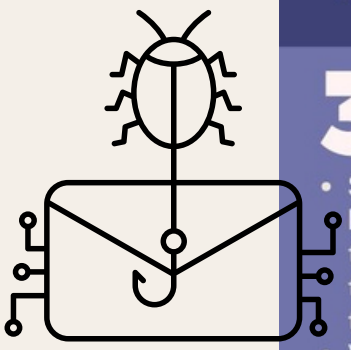
Email threats are a common method used by cybercriminals to gain unauthorized access to personal information or infect systems with malware. Being aware of these threats and knowing how to protect yourself is crucial. Let's explore key points about email threats and how to stay safe in your inbox.

1 Phishing Attacks

- Phishing attacks involve emails that appear legitimate but aim to trick recipients into revealing sensitive information.
- Look out for suspicious emails asking for account credentials, financial details, or personal information.
- Be cautious of urgent or threatening language, grammatical errors, or unusual email addresses.

2 Malware and Attachments

- Malicious attachments can contain malware, viruses, or ransomware.
- Avoid opening attachments from unknown or suspicious senders.
- Be wary of email attachments with unusual file extensions such as .exe, .zip, or .bat.



3 Spoofed Emails

- Spoofed emails mimic legitimate senders, tricking recipients into thinking they are from a trusted source.
- Verify the sender's email address for any inconsistencies or slight variations.
- Hover over links to check if they lead to legitimate websites before clicking on them.

4 Email Scams

- Email scams attempt to deceive recipients into providing money or sensitive information.
- Be skeptical of unsolicited emails promising prizes, inheritance, or lottery winnings.
- Ignore requests for financial assistance or wire transfers from unknown individuals.

5 Protecting Yourself

- Keep your email software and antivirus programs updated to protect against known vulnerabilities.
- Enable multi-factor authentication (MFA) for your email accounts to add an extra layer of security.
- Be cautious when sharing your email address online and only provide it to trusted sources.
- Regularly review and delete suspicious or unsolicited emails from your inbox.

6 Reporting Suspicious Emai

- Report phishing emails to your email provider or IT department to help protect others from falling victim.
- Forward suspicious emails to the Anti-Phishing Working Group (reportphishing@apwg.org) or the Federal Trade Commission (spam@uce.gov).

PASSWORD THREATS

COMMON PASSWORD THREATS

- Brute Force Attacks: Hackers use automated software to guess passwords by trying various combinations.
- Password Cracking: Cybercriminals use advanced techniques to decrypt encrypted passwords.
- Phishing Attacks: Scammers trick users into revealing their passwords through deceptive emails or websites.
- Password Reuse: Using the same password across multiple accounts increases the risk of a breach.

CREATING STRONG PASSWORDS

- Length: Choose a password that is at least 12 characters long to increase complexity.
- Complexity: Include a mix of uppercase and lowercase letters, numbers, and special characters.
- Avoid Personal Information: Don't use names, birthdates, or easily guessable information.
- Passphrase Approach: Consider using a memorable phrase with spaces or special characters between words.

TWO-FACTOR AUTHENTICATION (2FA)

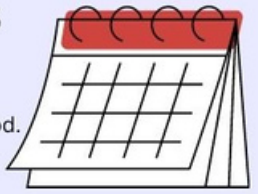
- Enable 2FA whenever available. It adds an extra layer of security by requiring a second verification step.
- Common methods include SMS codes, authenticator apps, or biometric verification.

PASSWORD MANAGEMENT

- Use a reputable password manager to securely store and generate strong passwords.
- Password managers help you remember complex passwords and automatically fill them in when needed.
- Ensure the password manager has strong encryption and a master password for added security.

REGULAR PASSWORD UPDATES

- Change passwords regularly, especially for critical accounts.
- Avoid using the same password for an extended period.
- Set reminders or use password management tools to help you remember to update passwords.



AVOIDING PHISHING SCAMS

- Be cautious of suspicious emails or messages asking for your password or personal information.
- Check for signs of phishing, such as misspelled URLs, grammatical errors, or urgent requests.
- Always verify the legitimacy of a website before entering your password.

MONITORING ACCOUNT ACTIVITY

- Regularly review your account activity and set up alerts for any suspicious or unauthorized access.
- Report any suspicious activity to the respective service provider or platform.

BEWARE OF CREDIT CARD SCAMS:

PROTECT YOURSELF

1 TYPES OF CREDIT CARD SCAMS

1. Phishing:
- Scammers use deceptive emails or websites to trick you into revealing credit card details.

2. Skimming:
- Criminals install devices to steal credit card details at ATMs or point-of-sale terminals.
- Be cautious of unusual devices attached to card readers and check for tampering.

3. Card-not-present Fraud:
- Scammers use stolen credit card information for online or over-the-phone purchases.

4. Identity Theft:
- Thieves steal personal information to open fraudulent credit card accounts.

2 WARNING SIGNS

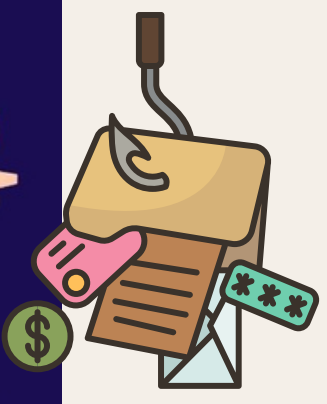
- Unauthorized charges or unusual activity on your account.
- Suspicious emails or calls requesting personal or credit card information.
- Unexpected credit card offers or account notifications.

3 PREVENTION TIPS

- Be cautious when sharing credit card information online or over the phone.
- Monitor credit card statements regularly and report any suspicious activity.
- Keep credit card information secure and avoid sharing it with untrusted sources.
- Use strong, unique passwords for online accounts and enable two-factor authentication.

4 WHAT TO DO IF YOU'RE A VICTIM

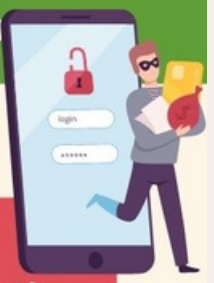
- Contact the credit card issuer or bank to report unauthorized charges.
- Place a fraud alert on your credit reports to prevent further fraudulent activity.
- File a report with the local law enforcement agency.
- Consider freezing your credit reports to prevent new accounts from being opened.



5 CONCLUSION:

Staying vigilant and informed is crucial in protecting yourself from credit card scams. By following these tips and being aware of potential threats, you can safeguard your financial well-being.

PHISHING: PROTECTING YOURSELF FROM ONLINE SCAMS."



Common Phishing Techniques:

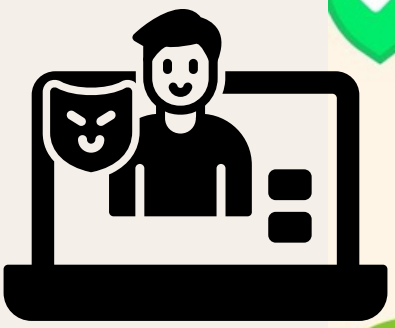
- **Email Spoofing:** Sending emails that appear to be from a reputable source but are actually fraudulent.
- **Deceptive Links:** Embedding malicious links within emails or messages that redirect to fake websites.
- **Fake Login Pages:** Creating counterfeit login pages to steal usernames, passwords, or other personal information.

How to Identify Phishing Attempts:

- **Misspelled URLs:** Pay attention to slight variations or misspellings in website addresses.
- **Urgent Requests:** Be cautious of emails or messages that create a sense of urgency or demand immediate action.
- **Suspicious Attachments:** Avoid opening attachments from unknown senders or suspicious emails.

Protecting Yourself from Phishing:

- **Verify the Source:** Double-check the legitimacy of emails, messages, or websites before providing any personal information.
- **Be Cautious with Links and Attachments:** Hover over links to view the actual URL and scan attachments for malware before opening them.
- **Secure Your Personal Information:** Avoid sharing sensitive data online or over insecure channels.

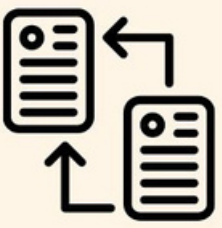


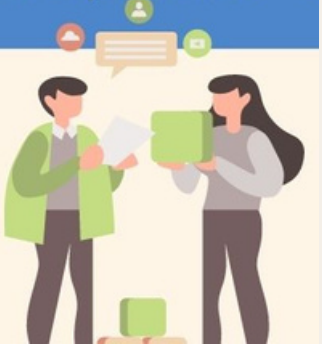
Stay Updated with Security Software:

- Install and regularly update antivirus and anti-malware software on your devices.
- Use a reliable firewall to protect against unauthorized access.

Report Suspicious Activity:

- If you encounter phishing attempts, report them to the appropriate authorities or organizations.
- Forward suspicious emails or messages to your email provider or the Anti-Phishing Working Group (APWG).





EMAIL LOTTERY

ALSO KNOWN AS THE NIGERIAN LETTER SCAM

This scam, perhaps one of the longest-running internet frauds, you'll receive an emotional message from someone claiming to be an official government employee, businessman, or member of a abundantly wealthy foreign family asking you to help them retrieve a large sum of money from an overseas bank.
In exchange, the person promises to give you some of the money. They may even produce fake paperwork that makes the deal look legitimate

WHAT CAN BE DONE TO AVOID SUCH SCAM?

It's best to ignore these messages and report them.

REPORT SCAM

CYBER BULLYING

Cyberbullying occurs when someone shares negative, harmful, false, or mean content about someone else. It takes place over digital devices like cell phones, computers, and tablets.

FREQUENCY OF CYBERBULLYING

CYBER SECURA

According to 2019 School Crime Supplement indicates

16% of students in grades 9–12 experienced cyberbullying.

The 2019 Youth Risk Behavior Surveillance System says

15.7% of high school students were bullied electronically.

TACTICS

- Posting comments or rumors about someone online that are mean, hurtful, or embarrassing.
- Pretending to be someone else online in order to solicit or post personal or false information about someone else.
- Threatening to hurt someone or telling them to kill themselves.
- Creating a mean or hurtful webpage about someone.

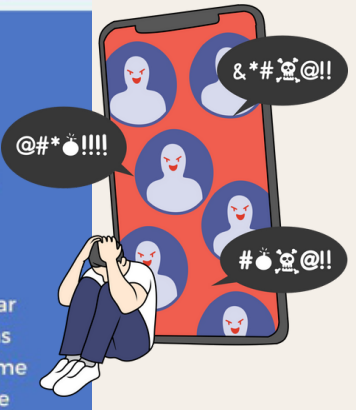
PREVENTION

DOCUMENT

Keep a record of what is happening and where. Take screenshots of harmful posts or content if possible. Most laws and policies note that bullying is a repeated behavior, so records help to document it.

SUPPORT

Peers, mentors, intervene publicly to positively influence a situation where negative or hurtful content posts about a child. Try to find if more professional support is needed for those involved.



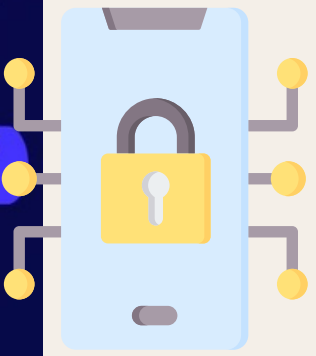
REPORT

Social media platforms and schools have clear policies and reporting processes. If a child has received physical threats, or if a potential crime or illegal behavior is occurring, report it to the police.

MOBILE SECURITY

LOCK YOUR DEVICE

- Set a strong PIN, password, or biometric authentication (fingerprint or face recognition) to prevent unauthorized access.
- Enable auto-lock after a period of inactivity for added security.
- Updates often include security patches that fix vulnerabilities.



INSTALL TRUSTED APPS ANDBE CAUTIOUS OF PUBLIC WI-FI

- Download apps only from official app stores (e.g., Google Play Store, Apple App Store).
- Check user reviews, ratings, and app permissions before installing.
- Avoid connecting to unsecured public Wi-Fi networks that lack encryption.
- Use a virtual private network (VPN) for secure browsing on public networks.

SECURE MOBILE BROWSING AND ENABLE FIND MY DEVICE

- Use secure websites (HTTPS) when entering personal information or conducting financial transactions.
- Be cautious of clicking on suspicious links in emails, messages, or websites.
- find my device feature can help protect your data and prevent unauthorized access.

APP PERMISSIONS

- Review and manage app permissions to control what information apps can access.
- Only grant necessary permissions to apps you trust.
- Avoid clicking on suspicious links or providing personal information to unknown sources.

BACKUP YOUR DATA

- Regularly back up your mobile device to prevent data loss in case of theft, loss, or system failure.
- Use cloud storage or connect to a computer to backup important files.

EDUCATE YOURSELF

- Stay informed about the latest mobile security threats and best practices.
- Be mindful of social engineering tactics and scams targeting mobile users.

SOCIAL NETWORKING

1. Choose Strong Privacy Settings

- Review and adjust your privacy settings on social networking platforms.
- Limit the visibility of personal information to trusted connections.

2. Be Mindful of What You Share

- Think before you post: Avoid sharing sensitive information that could be used against you.
- Be cautious of sharing personal details, financial information, or travel plans publicly.

3. Exercise Caution with Friend Requests

- Only accept friend requests from people you know and trust.
- Be wary of suspicious or fake profiles seeking access to your personal information.

4. Be Aware of Phishing Attempts

- Watch out for phishing scams through messages, comments, or links on social networks.
- Be skeptical of requests for personal information or login credentials.

5. Think Before You Click

- Avoid clicking on suspicious links, even if they are shared by friends or appear to be from reputable sources.
- Verify the authenticity of links before interacting with them.

6. Regularly Review App Permissions

- Regularly review the permissions granted to apps connected to your social networking accounts.
- Remove unnecessary permissions to limit access to your data.

7. Stay Informed About Privacy Policies

- Stay updated on the privacy policies of social networking platforms.
- Understand how your data is collected, used, and shared by the platform.

8. Be Mindful of Location Sharing

- Be cautious about sharing your location on social networking platforms.
- Disable location services or limit access to trusted connections only.

How to Identify Fake Applications

Verify the Developer

- Research the developer's reputation.
- Check their website, reviews, and ratings.

Check App Permissions

- Be cautious of excessive or unnecessary permissions.
- Grant only relevant permissions.

Read User Reviews

- Look for security concerns or suspicious behavior.
- Pay attention to poor performance reviews.

Analyze App Description and Screenshots

- *Check for detailed descriptions and high-quality screenshots.*
- *Beware of grammatical errors or low-resolution images.*

Check App Store Authenticity

- Use official app stores like Google Play or Apple App Store.
- Be wary of third-party app stores.

Cross-Check Official Websites

- Visit the app's official website.
- Ensure consistency and professional design.

Avoid Unusual Download Sources

- Stick to trusted sources and avoid random links.
- Sideloading from unofficial platforms is risky.

Look for SSL Certificates

- Check for a secure connection (https://) and padlock symbol.
- Ensure data protection before entering personal information.

Remember: Prevention is key! Stay vigilant and prioritize your online safety.

DESKTOP SECURITY

KEEP SOFTWARE UPDATED

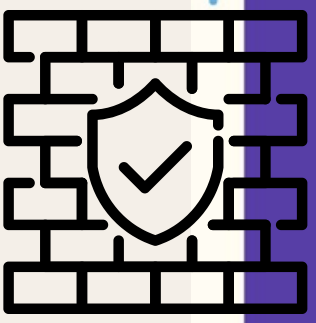
- Regularly update your operating system, antivirus software, and applications.
- Updates often include security patches.

STRONG AND UNIQUE PASSWORDS

- Create strong, unique passwords.
- Use a combination of uppercase and lowercase letters, numbers, and special characters.
- Avoid easily guessable information.

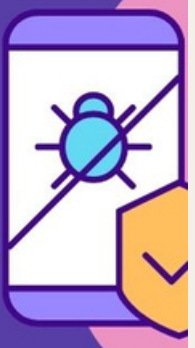
TWO-FACTOR AUTHENTICATION (2FA)

- Enable 2FA for an extra layer of security.
- Requires a second verification step, like a code sent to your mobile device.



FIREWALL PROTECTION

- Activate and maintain a reliable firewall.
- Monitors and controls network traffic.
- Blocks unauthorized access and malicious activities.



SECURE WI-FI CONNECTION

- Use a secure Wi-Fi network with encryption enabled.
- Change default router password.
- Use WPA2 or WPA3 encryption protocols.

REGULAR DATA BACKUP

- Frequently back up important files and documents.
- Use external hard drives, cloud storage, or backup software.

ANTI-MALWARE SOFTWARE

- Install reputable anti-malware software.
- Keep it updated.
- Run regular scans to detect and remove malware.

SAFE BROWSING PRACTICES

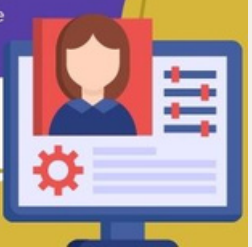
- Be cautious when clicking on links or downloading files.
- Avoid untrusted sources.
- Watch out for phishing emails, suspicious websites, and pop-up ads.

USER ACCOUNT MANAGEMENT

- Create separate user accounts for each individual.
- Limit administrative privileges to reduce risks.

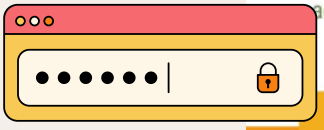
REGULAR SYSTEM MAINTENANCE

- Perform routine system maintenance tasks.
- Disk cleanup and defragmentation.
- Optimize performance and remove unnecessary files.



SECURITY AWARENESS ON WEARABLE GADGETS

Wearable technology is a category of electronic devices that can be worn as accessories, embedded in clothing, implanted in the user's body, or even tattooed on the skin



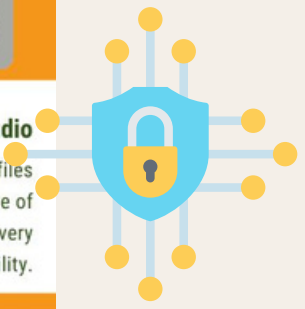
WEARABLE TECHNOLOGY SECURITY ISSUES FOR CONSUMERS

Easy Physical Access to Data

There is often no PIN or password protection, no biometric security, and no user authentication required to access data on a wearable. If it falls into the wrong hands, there is a risk that sensitive data could be accessed very easily.

Ability to Capture Photos, Videos and Audio

It is easy for someone to take photographs or record video or audio files using something like a smartwatch or smart glasses. Secret capture of confidential information, and videos and images of sensitive data, is a very real possibility.



Insecure Wireless Connectivity

The fact that wearable devices tend to connect to our smartphones or tablets wirelessly using protocols such as Bluetooth, NFC and Wi-Fi creates another potential point of entry. Many of these wireless communications are insufficiently secure to guard against a determined brute-force attack.

Lack of Encryption

Some third-party apps neglect basic security standards and send or store information that is not encrypted. The kind of data that is automatically being collected by wearables is very valuable to the right people.

SECURITY VULNERABILITIES AND ATTACKS

- Eavesdropping and spyware
- QR photobombing malware
- Wi-Fi-hijacking
- Phishing
- Brute force attack

CYBER SECURA

User Identity and Data Privacy

Embedded sensors such as cameras and microphones, capture data about the individual and also the surroundings, often without their consent. These data are often personal, confidential, and sensitive, which invade users' privacy and pose privacy challenges such as surveillance.

Time and location-based privacy

GPS embedded inside wearable able to track a person's location at a specific time. It brings greater benefits for people to do navigation, but it also poses greater risks as well. It raises serious issues on the user's privacy if the location of the people can be tracked.

HOW TO AVOID EYE STRAIN WHILE WORKING ON ELECTRONIC GADGETS

CAUSES, SYMPTOMS AND SOLUTIONS

CAUSES

Avoid **"turtling"**-sitting with your back rounded, chin jutting forward and head tilted back to get closer to your screen. If you can't see your screen clearly with good posture, visit an eye doctor.

Eye strain can be caused by **excessive lighting.** Overhead lighting should be no brighter than your screen.

Sitting too close to the screen can cause eye fatigue and blurred vision.

Are you sitting in a **bad chair**? your back should be supported so you can sit upright and at a comfortable viewing distance from your screen.

Don't wear glasses with an **old prescription**. For maximum comfort, ask your eye doctor about custom computer eyeglasses.

SYMPTOMS

Dry eyes
Irritated eyes
blurred vision
tired eyes
neck & back pain
headaches

WHAT YOU CAN DO

- Wear protective eyewear and glasses designed to block out eye strain caused by blue light.

- Remember the 20-20-20 rule: Every 20 minutes, take a break and look at something 20 feet away for 20 seconds.

- Reduce overhead lighting to eliminate screen glare that worsens eye strain.

- Make sure your screen is a "high-five" distance from where you are sitting.
- Eye Exercise

MENTAL HEALTH

Early warning sign

Difficulty Concentrating

Trouble focusing leads to poor performance, and hyperactivity.

Drastic weight changes

Signs of mental illness include: overeating, demonstrating a loss of appetite, vomiting, or using laxatives.

Mood Changes

Feelings of sadness or withdrawal, ongoing anger or irritability, severe mood swings, isolation, avoiding activities that were previously enjoyed.

Physical Symptoms

Physical symptoms of mental illness that some people experience are: chronic headaches, stomachaches, other types of aches, and sleep deprivation.

Stress and Anxiety

Depression and loneliness

Warning signs to look out for that indicate gadgets addiction

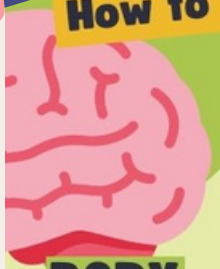
- You cannot keep off your phone even when conversing with someone.
- You are having trouble with concentration and cannot finish work and other chores. You are forever distracted because you want to check your phone.
- You begin to experience sleep problems.
- You need to be on your phone, or you start to feel anxious and irritable.
- You think you are missing something when you are not on your phone.

Taking charge of your mental health

DON'T FORGET!

- Surround yourself with family and friends
- Continue doing what you love: reading, sports, writing, nature walks, creating art.
- Create a schedule & stick to your routine.

How to deal with stress and anxiety



MIND

- Accept that you cannot control everything.
- Do your best.
- Maintain a positive attitude.

BODY

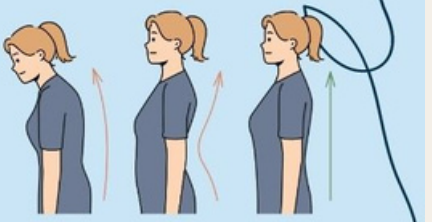
- Eat well-balanced meals.
- Get enough sleep.
- Exercise daily.

ACTION

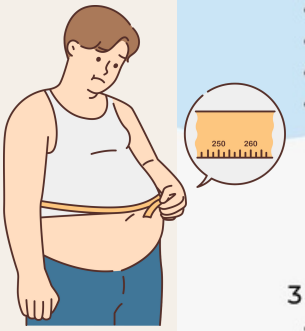
- Take deep breaths-slowly count to 10.
- Take time out for yoga, listen to music, and meditate.
- Talk to friends & family and tell them how you're feeling.

The Impact of Excessive Gadget Use on Physical Health

Symptoms



1. Posture Problems:
   - Rounded shoulders
   - Forward head posture
   - Slouched back
   - pain in fingers



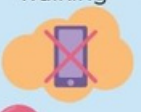
2. Sedentary Lifestyle:
   - Lack of physical activity
   - Weight gain
   - Poor cardiovascular health

3. Sleep Disturbances:
   - Difficulty falling asleep
   - Poor sleep quality
   - Insomnia

Helpful tips :

1. Practice Good Posture:
   - Sit up straight with your back supported
   - Keep your feet flat on the ground
   - Adjust your screen to eye level

2. Take Regular Breaks and Move:
   - Set reminders to stand up and stretch every hour
   - Engage in physical activities such as walking or exercising



3. Create a Device-Free Wind-Down Routine:
   - Avoid gadget use at least one hour before bedtime
   - Engage in relaxing activities like reading or meditation

4. Set Screen Time Limits:
   - Use apps or built-in features to track and limit screen time
   - Allocate time for offline activities and social interactions

CONCLUSION:

Excessive gadget use can have detrimental effects on our physical health. By being aware of the symptoms and implementing these tips, we can mitigate the impact and promote a healthier lifestyle. Remember to strike a balance between gadget use and maintaining a physically active routine, allowing for improved overall well-being.

Turning Off Computers

Save your work

- Before shutting down, save all open documents and close running programs.
- Prevents data loss and ensures you can resume work later.

Close applications

- Close all open applications and browser tabs.
- Frees up system resources and improves performance.

Log out of accounts

- Sign out of all active user accounts and applications.
- Protects sensitive information from unauthorized access.

Eject external devices

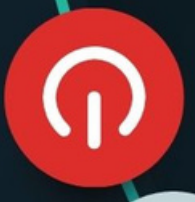
- Safely eject connected external devices (e.g., USB drives, external hard drives).
- Prevents data corruption and damage to devices.

Run updates

- Check for system updates and install them if available.
- Updates often include important security patches and bug fixes.

Shut down properly

- Click on the Start menu or Apple menu and select "Shut Down" or "Power Off."
- Wait for the computer to complete the shutdown process before turning off the power.



Power off peripherals

- Turn off connected peripherals (e.g., monitors, printers, speakers).
- Saves energy and prolongs device lifespan.

Unplug when necessary

- Consider unplugging the computer from the power source if not in use for an extended period.
- Protects against power surges and reduces energy consumption.

CYBER LAW IN INDIA

1 INFORMATION TECHNOLOGY ACT, 2000

- Legal recognition to electronic records and digital signatures.
- Defines cybercrimes and their penalties.

2 CYBERCRIMES AND OFFENSES

- Hacking, identity theft, online fraud, and data breaches.
- Penalties for cyber offenses.
- Unauthorized access, computer-related offenses, cyber terrorism.

3 DATA PROTECTION AND PRIVACY

- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- Protection of personal data.
- Security practices for entities handling sensitive personal information.
- Procedures for data breaches and data subject consent.

4 CYBER FORENSICS

- Investigation and collection of digital evidence.
- Admissible in court for cybercrime prosecution.
- Empowers law enforcement agencies.

5 CYBER APPELLATE TRIBUNAL (CAT)

- Established under the Information Technology Act, 2000.
- Appeals against decisions of Adjudicating Officers.
- Ensures efficient implementation of Cyber Law.

6 REPORTING CYBERCRIMES

- Encourages reporting cybercrimes to authorities.
- Promotes a safer online environment.
- Facilitates effective law enforcement.

7 HELPLINE:

- Portal: https://cybercrime.gov.in/
- Toll-free number: 1930

In case of Emergency, please contact us on :

Women Safety Wing
www.womensafetywing.telangana.gov.in/

She Team Whatsapp
9441669988

Reception Number
9440700906

Child Helpline Number	Cyber Crime Number	Cyber crime website
1098	1930	Cybercrime.gov.in