DELNET
Developing Library Network

CyberPeace

CYBERPEACE ESSENTIAL

CYBER SAFETY AWARENESS HANDBOOK

About CyberPeace

CyberPeace is a global civil society organization, think tank of cybersecurity and policy experts with the vision of pioneering CyberPeace Initiatives to build collective resiliency against Cybercrimes & global threats of cyber warfare. CyberPeace is involved in Policy Advocacy, Research and Training related to all aspects of CyberPeace and CyberSecurity. Key areas of CyberPeace Foundation work are in Technology Governance, Policy Review and Advocacy, Capacity and Capability creation and building through partnerships with various government organizations, academic institutions and civil society entities.

CyberPeace's work towards Internet Governance and Cyber Security is aligned towards 6 UN's Sustainable Development Goals (SDGs).

Verticals of #CyberPeace

Popular Cyber Crimes

Cyberbullying: It is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation.

To understand the topic in detail

Scan the QR Code

Fake Profile and Impersonated Profile: Sometimes words like Fake profile and impersonated profiles are used interchangeably but they are two very different concepts, A Fake profile is of a person who doesn't even exist e.g. Glossy Angel, Waggy Tails, people with such names don't exist and someone else is at the other end. This may not be a criminal offence. Now talking about the impersonated profile in this case has a slight difference, one can make a social media profile with your name, your photograph and other relevant information, all of which or most of which is the correct information. This is the case of an impersonated profile.

To understand the topic in detail

Scan the QR Code

Popular Cyber Crimes

Social Engineering: It is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these "human hacking" scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems.

To understand the topic in detail

Scan the QR Code

Phishing: It is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

To understand the topic in detail

Scan the QR Code

Identity Thef: It is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss. The user may obtain the sensitive information by several means like phishing, sending some links to the victim via e-mail and asking to furnish confidential information, or obtaining the information through social engineering, using key-loggers, etc.

To understand the topic in detail

Scan the QR Code

Ransomware: It is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid. More modern ransomware families, collectively categorized as crypto ransomware, encrypt certain file types on infected systems and force users to pay the ransom through certain online payment methods to get a decryption key.

To understand the topic in detail

Scan the QR Code

Revenge Porn: It is popularly understood as the real or simulated portrayal of a person (or persons) in a sexually explicit way that is then circulated without the person's consent. Such portrayal is circulated with the sole intent of harassing, hurting and defaming the image of the child. The offending media is often created by a person who is the victim's partner or more often, former partner.

To understand the topic in detail

Scan the QR Code

Popular Cyber Crimes

Financial Fraud: It includes business fraud, mass marketing fraud, offering jobs overseas, Nigerian fraud, investment fraud, etc. where people are tricked into a trap by the promise of such opportunities and money or other valuables are deceived.

To understand the topic in detail

Scan the QR Code

Deepfake: There is a use of sophisticated AI algorithms that help manipulate or generate synthetic multimedia content such as videos, audio, and images. As a result, it has become increasingly difficult to differentiate between genuine and altered or fake content, and these AI-manipulated videos look realistic. There is a misuse of deepfake technology by bad actors to target innocent netizens.

To understand the topic in detail

Scan the QR Code

Data Breach: A data breach is any security incident in which unauthorized parties gain access to sensitive data or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) or corporate data (customer data records, intellectual property, financial information).

To understand the topic in detail

Scan the QR Code

Child Sexual Abuse Material (CSAM): Any picture or video of a minor being abused through sexual activity is considered child sexual exploitation (CSAM).

To understand the topic in detail

Scan the QR Code

Cyberstalking: It is a crime committed when someone uses the internet, social media and other technologies to harass or stalk another person online.

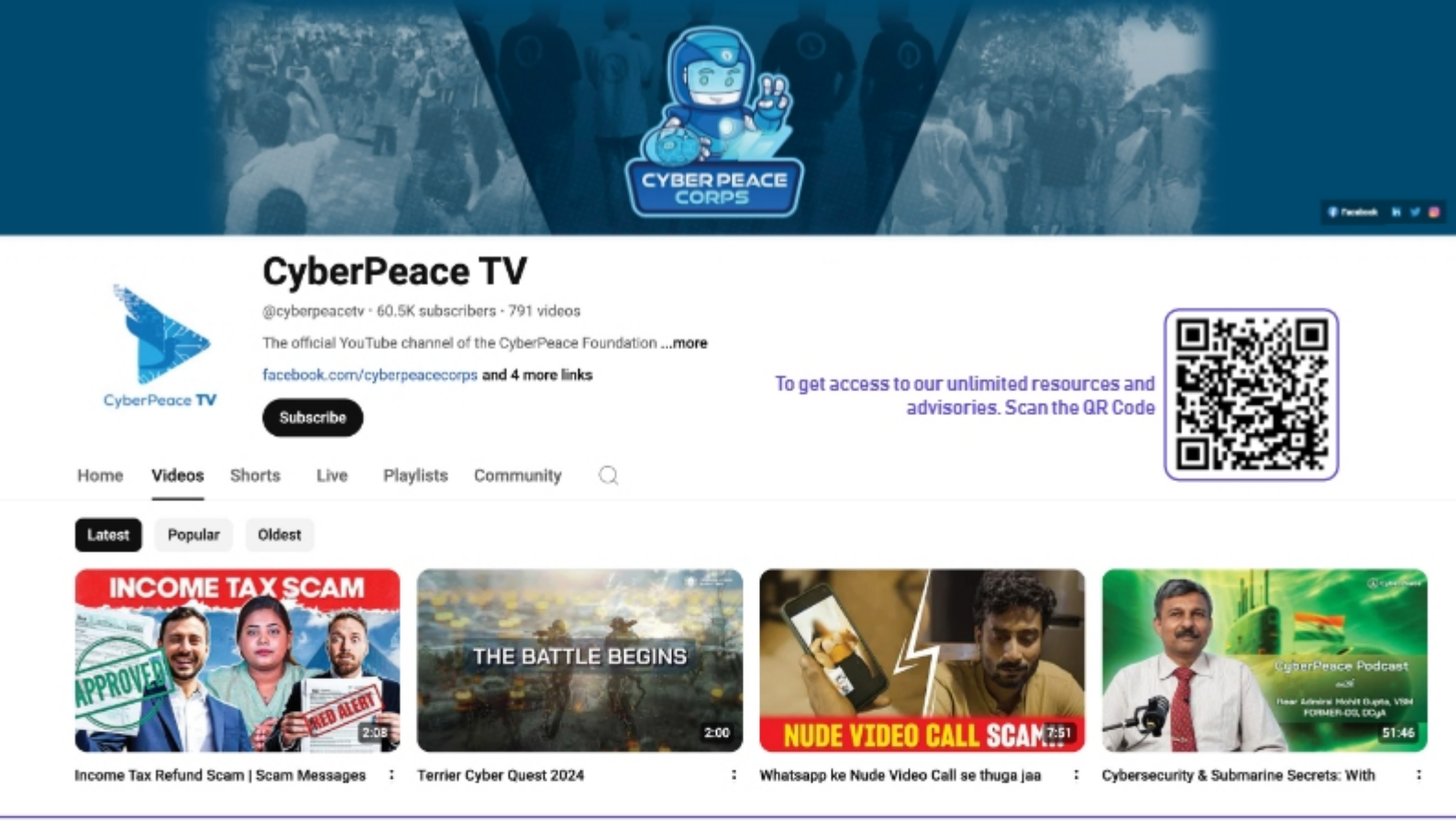
To understand the topic in detail

Scan the QR Code

Cyber-enabled Human Trafficking: Cyber-enabled human trafficking is the use of technology to facilitate the recruitment, transportation, and exploitation of human beings. Traffickers commonly utilise social media to gather information on victims and create false profiles to create virtual relationships in order to groom innocent netizens. Thus, the misuse of the Internet by bad actors facilitates victim-trafficker relationships.

To understand the topic in detail

Scan the QR Code



Responsible Online Behavior

The internet is an uncontrolled space where one tends to see no bounds. However, we must keep in mind that our actions online can have the same repercussions as those offline. One unwanted message/post can cause a lot of problems for both the sender/poster and the receiver/audience. Users need to be vigilant and take precautions to safeguard themself online as responsible netizens. To ensure that you are not stuck in such a situation we have created this handbook.

"WOULD YOU DO SOMETHING ONLINE THAT YOU WOULDN'T DO OFFLINE?"

Responsible Sharing

- **Never share false information.** Always verify the source and the contents of the post before sharing it.
- **Be respectful and empathetic towards others**; don't post anything offensive or obscene.
- **Visit only websites you are confident about.** Look for the padlock icon in your browser's URL bar to make sure that the website is secured and encrypted.
- **Personal information that you share online** may be used against you. Review the content that you wish to share online and only provide information that is essential.
- **Use trusted sources for downloading online.** Downloading songs and movies from untrusted or free sources may be illegal. Use trusted websites or platforms, like Google Play Store, Apple App Store, Gaana.com, Saavan, Netflix, etc.

Digital Devices, Mobile Phones and Tablets Security

Security Lock

Use a number code, pattern lock, fingerprint or Face ID to lock a device when not in use.

Encryption

Encrypt the entire device or just the sensitive data

Remote Wipe

In case of phone is stolen or lost, remote wipe the device

Backup data

Regularly backup your data

Applications

Do not install anything from an unknown source and research in depth before installing any applications.

Messages

Beware of social engineering scams like phishing and smishing that target your personal and financial data.

No Rooting

Avoid rooting or jailbreaking your device as it opens doors to malware and security risks.

Update System

Keep your system updated to patch vulnerabilities; enable automatic updates.

Mobile Internet Security

Use firewall and antivirus to protect your mobile device from cyber attacks.

Switch Off Wifi Bluetooth and NFC

Turn off when not in use. Use a VPN when connecting to a Public Wifi network.

Juice Jacking

Juice jacking is a type of cyber attack involving a charging port that doubles as a data connection, typically over USB. This often involves either installing malware or surreptitiously copying sensitive data from a smartphone, tablet, or other computer device. Cybercriminals can hack your phone using or exploiting some public charging stations such as those at airports, malls, hotel rooms, etc. Hence it is important to think twice before using public charging spots, as it might lead to serious consequences such as malware, data leaks and hacking. Hence, users are advised to avoid using public charging stations. As netizens and technology consumers, our safety is in our hands and it is extremely important to give priority to best practices and stay protected in the evolving digital landscape.

Wifi Security

Admin Password
Change Default Admin Password

Change SSID
It is recommended to frequently change the SSID

ISP Password
Change the ISP default Username and Password

Hide SSID
Hide the SSID from being broadcast

Use WPA2
It is essential to use the latest and best form of encryption to protect your router

Router Firewall
Router firewall should be enabled along with your OD firewall

Router Relocation
The router should be placed centrally for better coverage and to limit the signal reach

Disable WPS
Turn off the WPS in the settings of the router

Disable Guest
Disable Guest network if not required

MAC Filtering
Enable MAC filtering in your router

Update Firmware
Update the firmware as soon as you see an update / Enable Automatic updates

Online Shopping / Banking Security

Beware of Fake Websites

Cross-check a website for spelling errors, older logos or anything else that raises an alarm

Rush Buying

Don't get fooled. Beware of websites which give to good to believe offers like iPhone 13 in just INR 5000

Internet Security Application

Use an Antivirus / Internet Security Application like Quickheal / Bitdefender Internet Security for your digital device

Two-Factor or Multi-Factor Authentication

Always use the Two-Factor or Multi-Factor Authentication mechanism to add an additional layer of verification.

Avoid shoulder surfers

Make sure that the area behind you is clear when you enter the password

Security Questions

Use Security Questions which can be difficult for a cybercriminal to guess

Use VPN

Use a VPN like Proton VPN / Express VPN when accessing public Wifi. It protects your data packets. VPN encrypts all incoming and outgoing data packets making it almost impossible for a cybercriminal to hack. Avoid logging in on Public WiFi networks or untrusted devices.

Always use HTTPS to access any website

Beware of Fake Wifi Networks

Use Strong and unique passwords for all your shopping and banking websites

Always keep an eye on your bank transactions. If something suspicious crops up then inform the bank immediately

Email Security

- Choose strong passwords (e.g. 5H^%PO@#fc)
- Use different email accounts for personal and professional use
- Activate Two-Factor Authentication
- Never click on links in suspected Emails or Emails that are too good to be true.
- Try avoiding public Wi-Fi, and even if you do use it, make sure it is from a trusted source or service provider and never use it to log-in to your accounts.

Computer Security

- Keep your antivirus updated
- Use passwords for your computer
- Disconnect your webcam if it is not in use or if you have a laptop, put a sticker on it
- Keep your Operating System up-to-date and install regular security patches
- Never hand your debit/ credit card to someone else

Social Media Security

- Check your social media privacy settings
- Activate Two Factor Authentication for all your online Log-ins
- Share information wisely
- Never share your password with anyone
- Think before you post
- Always check the URL of the website while visiting a website
- Never download files from untrusted sources
- To save passwords safely and easily, use Password Manager
- Do not share your location on public social media sites.
- Be cautious while interacting with strangers as they might turn out to be bad actors.

How to spot fake news

Check the Source
Who is sharing the information? Is the source trustworthy?

Check the Language
Are there a lot of errors? Is there uniformity in the message?

Read Beyond
Are the headlines catchy? Is the information too good to be true?

Cross Check Photos/Video
Has the photo been morphed? Are things being taken out of context?

Check a Quote or Statement
Did the person being quoted actually say it?

Stay connected with **reputed expert organisations** that regularly do fact-checking and debunks viral claims.

Misinformation may proliferate due to the rapid pace at which information is shared on social media sites, and so users are advised to not share any information without being certain of its authenticity as doing so might cause one to inadvertently contribute to spreading false narratives.

Cyber Crimes and the Indian Regulatory Landscape

To combat cybercrime, The Information Technology Act, of 2000 was enacted wherein certain cybercrimes have been made punishable. The recently-enacted Digital Personal Data Protection Act, 2023 aims to protect the digital personal data of individuals and place certain obligations on Data Fiduciaries to abide by, in order to protect the individuals' digital personal data. There are provisions in place in Bharatiya Nyaya Sanhita, 2023, taking into its purview the concern of cyber crimes. Section 111 of the Bharatiya Nyaya Sanhita (BNS), 2023, is a comprehensive legal provision aimed at combating organized crime and will be useful in persecuting people involved in large-scale cyber scams.

Important Sections under IT Act, 2000

Offences	Sections
Penalty and compensation for damage to computer, computer system, etc.	Section 43
Tampering with computer source documents.	Section 65
Computer related offences.	Section 66
Punishment for dishonestly receiving stolen computer resource or communication device.	Section 66B
Punishment for identity theft.	Section 66C
Punishment for cheating by personation by using computer resource.	Section 66D
Punishment for violation of privacy.	Section 66E
Punishment for cyber terrorism.	Section 66F
Punishment for publishing or transmitting obscene material in electronic form.	Section 67
Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form	Section 67A
Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.	Section 67B

Important Section under Bhartiya Nyaya Sanhita, 2023

BNS Provisions	Particulars	BNS Provisions	Particulars
Section 75	Sexual Harassment and Punishment for Sexual Harassment	Section 308	Extortion
Section 77	Voyeurism	Section 356	Defamation
Section 78	Stalking	Section 111	Organized Cyber Crimes

Data Privacy and Important Rights under the Digital Personal Data Protection Act, 2023

The Act empowers individuals, i.e., data principals, with the following rights

Right to Information

Individuals have the right to receive information about their personal data.

Right to Correction and Erasure of Data

Individuals have the right to correct inaccurate/incomplete data and erase data that is no longer required for processing.

Right to Grievance Redressal

Individuals have the right to seek a grievance to be provided by a Data Fiduciary or consent manager with respect to handling an individual's personal data as per provisions underlined under the act.

Right to Nominate

Individuals have the right to nominate 'another individual' to exercise the right of the individual in case of death or incapacity.

Reporting a Cyber Crime

There is a way to deal with almost every problem that you may face online. First and foremost is collecting evidence of the wrong that is happening/ being committed. You can collect proof of the incident/cybercrime by:

- Saving the URL of the profile in question/save the email or any other conversation
- Take a screenshot of the entire PC or mobile screen with a time stamp.
- Saving any information related to the IP address of the perpetrator that you receive on email when someone tries to access your account etc.
- Not deleting IDs, messages or any other communication.

The next step is alerting, the simplest step is to report what you feel is inappropriate. This will help take down content or the profile that you feel is problematic. You also have the choice to block persons that you feel need to stay away from.

If blocking/ reporting doesn't seem to solve issues, you can always approach your local police station and cyber cells to report any instance of cybercrime.

Reporting Crimes Related to Women

You can report a crime related to women on ncwapps.nic.in The portal is run and maintained by the NCW, Ministry of Women and Child Development, Government of India.

Reporting on ncwapps.nic.in

The portal is run and maintained by the NCW, Ministry of Women and Child Development, Government of India.

Reporting Crimes Related to Children

You can report a crime related to children on ncpcr.gov.in The portal is run and maintained by the Ministry of Women and Child Development, Government of India.

Reporting on ncpcr.gov.in

The portal is run and maintained by the Ministry of Women and Child Development, Government of India

National Cyber Crime Reporting Portal and Helpline

The 24x7 Cyber Crime Helpline 1930 and its Reporting Platform cybercrime.gov.in have been made operational by the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs. It is a citizen-centric initiative for enabling citizens to report cyber crimes online.

Reporting on cybercrime.gov.in

Grievance Appellate Committee (GAC)

The Grievance Appellate Committee (GAC) serves as an online dispute resolution mechanism established under the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules")**, made under the Information Technology Act, 2000. Digital Nagriks aggrieved by decisions of Grievance Officers of social media intermediaries and other intermediaries regarding complaints of users or victims against violation of the IT Rules and any other matters pertaining to the computer resources made available by the intermediaries can file an appeal with the Grievance Appellate Committee at **gac.gov.in.**

CyberPeace Helpline

You can also contact CyberPeace when you encounter or have any issues or know someone who is going through a tough situation. We would be happy to help. Netizens can contact CyberPeace at **CyberPeace Helpline +919570000066 and helpline@cyberpeace.net** to get assistance in reporting their cases.

Cyberspace has become the next dimension of one's life. It has become imperative to talk about and protect this space and individuals who practically lead their lives.

The world needs it today for the internet to be peaceful, trustworthy and safe enough for its users.

DELNET
Developing Library Network

CyberPeace