गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

सत्यमेव जयते

Indian Cyber Crime Coordination Centre

सहवीर्य करावहै • Working Together With Vigour

CYBER CRIME PREVENTION HANDBOOK

ESSENTIAL
DOS AND DON'TS
FOR LATEST CYBER CRIMES

STOP. THINK. TAKE ACTION

SHRI NARENDRA MODI

Hon'ble Prime Minister

I Dream of a Digital India Where Cyber Security Becomes an Integral Part of Our Nation.

SHRI AMIT SHAH

Hon'ble Union Home Minister

Cyberspace cannot be secured by any single organization alone; it requries the collective together on a unified platform working towards the same goal under a shared framework.

INDEX

SCAM ALERTS

SCAMS	Page No.
KYC Scam	4
Online Job Scam	5
Online Shopping Fraud	6
Digital Arrest	7
Investment Scam	8
Online Gaming	9
Lottery Fraud	10
Phishing	11
Vishing	12
Quishing	13
Search Engine Fraud	14
Social Media Impersonation	15

INDEX

SCAM ALERTS

SCAMS	Page No.
SMS, Email Scams	16
Debit/Credit Card Fraud	17
Mobile Application/ APK Scams	18
Cyber Slavery	19
SIM Swapping	20
Money Mules	21
Juice Jacking	22
Deepfake Cybercrime	23
Remote Access Fraud	24
Unsafe Browsing	25
Ransomware	26

KYC Scam

KYC Fraud involves cybercriminals exploiting identity verification processes to steal personal information, commit identity theft, or access financial accounts illegally. This can lead to significant financial losses and reputational damage for individuals, businesses, and financial institutions. Common tactics include tricking people, forging documents, and creating fake identities.

✓ Dos:

- **Verify Requests:** Contact your bank or financial institution directly to confirm any KYC update requests.
- **Use Official Contacts:** Obtain contact numbers or customer care details only from the official website or trusted sources.
- **Report Incidents:** Inform your bank or financial institution immediately if you suspect any cyber fraud.
- **Check KYC Update Methods:** Enquire with your bank about the available methods for updating KYC details.

× Don'ts:

- **Protect Credentials:** Never share your account login details, card information, PINs, passwords, or OTPs with anyone or on unauthorised websites/apps.
- **Secure Documents:** Do not share KYC documents or their copies with unknown or unidentified individuals or organisations.
- **Avoid Suspicious Links:** Do not click on suspicious or unverified links received via mobile or email.

Online Job Scam

Online Job Scams trick people looking for work. Scammers post fake jobs on websites, social media, or send emails, offering high pay and easy work. Their goal is to steal the victim's money or personal information.

✓ Dos:

- **Use Trusted Sources:** Refer to newspapers, job portals, or government portals for authentic private and government job listings.
- **Check Credentials:** For international job offers, verify the company's credentials and ensure you have the correct work visa.
- **Ask Questions:** During online interviews, ask detailed questions about the company and the interviewer.
- **Verify Emails:** Look out for email addresses that mimic genuine companies. For e.g., info@company.net in place of info@company.com.

× Don'ts:

- **Avoid Upfront Fees:** Do not pay any consulting fees without verifying the company's legitimacy.
- **Be Skeptical:** Do not trust sponsored search results or unsolicited job emails blindly.
- **Verify Advertisements:** Never apply for jobs without verifying the authenticity of advertisements, especially on social media platforms or groups.

Online Shopping Fraud

Online Shopping Fraud is a cybercrime where fraudsters deceive victims into making illegitimate purchases. They create fake websites or manipulate legitimate platforms, offer deals that are too good to be true, and steal personal and financial information, leading to financial losses and mistrust in online marketplaces.

✓ Dos:

- **Compare Prices:** Compare prices on different e-commerce websites.
- **Use Cash-on-Delivery:** If a website seems suspicious, opt for the cash-on-delivery payment method.
- **Choose Verified Sellers:** Prefer buying from "Verified" or "Trusted" sellers on e-commerce websites.
- **Verify Offers:** Be cautious of offers that seem too good to be true.
- **Secure Transactions:** Remember, you never need to enter a PIN, password, or OTP to receive money.

× Don'ts:

- **Avoid Public Networks:** Do not make e-shopping transactions using public computers or networks.
- **Protect Your Information:** Do not save your card details, date of birth, phone number, etc., on unreliable e-shopping websites.
- **Verify Sellers:** Do not make advance payments on C2C platforms like OLX, Quikr, etc., without verifying the seller's credentials.
- **Beware of QR Codes:** Do not scan QR codes to 'receive' money if an unknown person asks for it on WhatsApp or Telegram.

Digital Arrest

Digital Arrest is when someone is detained or restricted through digital means (like video calls) instead of traditional physical arrest methods. This often involves scammers impersonating government officials to extort money.

✓ Dos:

- **Know the Facts:** Police or government officials never conduct interrogations via video calls.
- **Don't Share Personal Info:** No government official will ask for money or personal details via video calls.
- **Stay Calm:** If you receive such calls, report them immediately on the **"Report Suspect Tab"** of cybercrime.gov.in.
- **Understand the Law:** There is no such thing as a "digital arrest" process in India.

× Don'ts:

- **Don't Panic:** Stay calm and avoid falling for scams.
- **Don't Give In to Scammers:** Don't send money if someone pressures you through a video call.
- **Don't Engage for Long:** Avoid getting trapped in long video calls that seem suspicious.
- **Don't Trust Unverified Calls:** Ignore any video calls claiming to be from government authorities asking for money.

Investment Scam

An Investment Scam involves fraudulent schemes that promise high returns, often too good to be true. These scams pay earlier investors with the money of new investors instead of generating profits through legitimate economic activity. It is also known as ponzi scheme.

✓ Dos:

- **Invest with Registered Entities:** Deal only with SEBI-registered intermediaries for investments.
- **Verify Investment Products:** Always invest through regulated financial entities.
- **Stay Informed:** Follow trusted information sources of regulated entities and financial products.
- **Report Suspicious Activity:** Call 1930 or report on cybercrime.gov.in.

× Don'ts:

- **Don't Panic:** Stay calm and verify the offer.
- **Don't Trust Unbelievable Returns:** Avoid schemes promising high returns with no risk.
- **Don't Join Dubious Groups:** Stay away from social media groups promoting suspicious trading apps.
- **Don't Ignore Red Flags:** Be cautious if the returns seem too consistent or too high over time.

Online Gaming

Online Gaming has become a hotspot for cybercriminals, with threats ranging from virtual theft and account breaches to real-world financial fraud and identity theft. Attackers exploit platform shortcomings and target players through phishing scams, malware, and social engineering.

✓ Dos:

- **Supervise Access:** If you are a parent, provide access to online games under supervision.
- **Be Cautious with Real Money Apps:** Many real money gaming apps may be fraudulent. Stay cautious and avoid apps that seem suspicious.
- **Judicious App Permissions:** Be careful before granting, permissions like Contacts, Storage, and Location to the app.
- **Protect Personal Information:** Keep safe your sensitive personal information, such as your full name, address, or bank account details, etc.

× Don'ts:

- **Avoid Suspicious Sources:** Do not download gaming apps from unreliable sources.
- **Beware of Assured Returns:** Do not install gaming apps that promises assured returns on social media or through advertisements.
- **Keep Information Private:** Do not share confidential information with unknown fellow players.
- **Limit Social Media Sharing:** Avoid oversharing your gaming achievements on social media to prevent becoming a target of harassment or cyberattacks.

Lottery Fraud

Lottery Fraud scams deceive people into believing they've won a prize to trick them into sending money or sharing personal information. These schemes exploit the hope of financial gain but are always too good to be true.

✓ Dos:

- **Don't Pay Fees:** Fraudsters often demand taxes, shipping fees, or handling charges for fake prizes. Never send money for any lotteries.
- **Question Unsolicited Claims:** Be cautious of unexpected lottery win messages or calls.
- **Report Fraud:** Notify authorities if you suspect a lottery scam.
- **Stay Skeptical:** Remember, no one gives away huge amount of money for free.

× Don'ts:

- **Don't Share Credentials:** Never provide secure details or make payments for lottery claims.
- **Beware Fake Authorities:** The RBI doesn't hold public accounts, solicit deposits, or request personal/bank details.
- **Ignore Fake Messages:** Avoid responding to offers promising prize money, government aid, or KYC updates tied to prizes.

Phishing

Phishing is a common cybercrime tactic that deceives victims into clicking on fake links. These links appear as emails or websites from trusted sources but redirect users to fraudulent sites designed to steal sensitive data, such as login credentials, personal information, or financial details. Phishing can also install malware, giving cybercriminals unauthorised access to your device.

✓ Dos:

- **Be Suspicious:** Treat unexpected messages from known sources with caution.
- **Check URLs:** Hover over links to reveal the genuine destination and spot discrepancies.
- **Verify Senders:** Contact the sender through a trusted method if you're unsure about a message's authenticity.
- **Update Regularly:** Keep your software and systems up-to-date to close security gaps.
- **Phishing Report:** Alert the relevant authorities or platforms if you encounter phishing attempts.

× Don'ts:

- **Avoid Clicking Links:** Don't click on suspicious links; delete messages from unknown senders immediately.
- **Unsubscribe & Block:** Unsubscribe from emails with suspicious links and block the sender's email.
- **Visit Official Websites:** Always go directly to the official website for financial transactions and verify website security (HTTPS with a padlock).

Vishing

Spam/Vishing Calls (voice phishing) are a deceptive form of cybercrime. Fraudsters use social engineering to trick victims into revealing sensitive information, like personal or financial data. They often impersonate legitimate entities, such as banks or government agencies, using tactics like caller ID spoofing and urgency to gain trust and steal information.

✓ Dos:

- **Use Call Blockers:** Install call-blocking apps and report spam calls.
- **Be Cautious:** Exercise caution when answering calls from unknown numbers.
- **Spread Awareness:** Educate others about common phone scams.
- **Enable Security:** Use voicemail passwords for added protection.

✕ Don'ts:

- **Don't Share Personal Info:** Never provide personal or financial information to unknown callers.
- **Don't Trust Caller ID:** Caller ID can be spoofed, so don't rely on it.
- **Avoid Unknown Numbers:** Don't return calls from unfamiliar or international numbers.
- **Protect Your Data:** Genuine institutions never ask for sensitive info like usernames, passwords, or OTPs. Never share these, even with family.

Quishing

Quishing Scams are on the rise. The scammer lure victims with promises of deals or convenience by asking to scan QR codes but ultimately initiate unauthorised financial transactions. Malicious codes can redirect users to phishing sites, steal login credentials, or transfer money directly to the scammer's account.

✓ Dos:

- **Scan Trusted Sources:** Only scan QR codes from official websites or verified businesses.
- **Verify Before Acting:** Scammers often create urgency—take your time to verify.
- **Report Suspicious Codes:** If you suspect a scam, report the code to the legitimate source and relevant authorities.

✕ Don'ts:

- **Be Cautious with Payments:** Avoid scanning QR codes with payment apps, as they may contain embedded account details for fraudulent transfers.
- **Don't Scan to Receive Money:** Never scan QR codes to receive funds. Legitimate transactions don't require scanning codes or entering banking details like m-PIN or passwords.
- **Avoid Unknown Sources:** Don't scan codes from emails, texts, or unfamiliar sources.

Search Engine Fraud

Search Engine Fraud occurs when fraudsters manipulate search results to display fake contact information, posing as legitimate entities. Victims who unknowingly call these numbers may reveal sensitive information, such as passwords and account details, leading to financial loss, identity theft, and other severe consequences.

✓ Dos:

- **Visit Official Websites:** Always check the official website for contact details, rather than relying on search results.
- **Verify Contacts:** Double-check phone numbers and websites using caller ID or trusted directories before sharing personal info.
- **Watch for Red Flags:** Be wary of urgency, scare tactics, or suspicious offers. Legitimate companies don't pressure immediate action.

✕ Don'ts:

- **Don't Trust Search Results:** Never call numbers listed in search engine results; fraudsters often disguise themselves as iillegitimate entity.
- **Don't Share Info Unprompted:** Only share personal details over the phone if you've initiated the contact.

Social Media Impersonation

Social Media Impersonation happens when someone sets up a fake account mimicking a real person or organisation. These fraudulent accounts are used to deceive others, often leading to identity theft, financial scams, reputational damage, and the spread of false information.

✓ Dos:

- **Verify Accounts:** Look for blue checkmarks, consistent usernames, and familiar profile pictures to confirm authenticity.
- **Be Cautious:** Avoid unsolicited messages and never share personal details or click suspicious links.
- **Report Impersonation:** Inform the platform and the real person or organisation being impersonated.

× Don'ts:

- **Confirm Fund Requests:** Verify requests for money from friends or relatives through a phone call or in-person meeting.
- **Don't Make Payments:** Avoid paying unknown individuals online and Untrusted / unverified charities.
- **Keep Info Private:** Never share personal or confidential details on social media.

SMS/ Email Scams

SMS, Email, and Call Scams are used by fraudsters to deceive victims with fake offers . They impersonate trusted NBFCs by using their logos and fake IDs, gaining credibility. Scammers may send counterfeit sanction letters or cheques, asking for upfront payments. Once the payment is made, the fraudsters disappear with the money.

✓ Dos:

- **Verify Authenticity:** Always cross-check sender details and contact official sources directly.
- **Report Suspicious Messages:** Forward any fake messages to official reporting channels and warn others.

× Don'ts:

- **Don't Trust Unsolicited Offers:** Never trust loan offers via phone, email, or text without verification.
- **Don't Share Sensitive Info:** Avoid giving personal or financial details without confirming the legitimacy of the offer.
- **Don't Click Links or Open Suspicious Emails:** Don't click on links or open emails from unknown sources with attachments or links.
- **Don't Pay Upfront Fees:** Genuine lenders don't require upfront payments for loan processing.

Debit/Credit Card Fraud

Debit and Credit Card Fraud occurs when your card details are used without your consent for unauthorised transactions. Criminals may steal your physical card, skim your details, or trick you into sharing sensitive information through phishing scams.

✓ Dos:

- **Deactivate Unused Features:** Turn off online, international, or NFC transactions when not needed.
- **Check Before You Pay:** Verify the amount on the screen before entering your PIN and check pos machine for skimming device.
- **Keep Your Card in Sight:** Always watch your card during transactions.
- **Shield Your PIN:** Cover the keypad when entering your PIN at ATMs or POS machines.

× Don'ts:

- **Don't Share Details:** Never share card information or PIN with anyone.
- **Don't Store PIN:** Avoid writing down or saving your PIN in easy-to-access places.
- **Avoid Public Wi-Fi:** Don't use your card on unsecured networks.
- **Don't Ignore Alerts:** Report suspicious transactions to your bank immediately.

Mobile Application/ APK Scam

Cybercriminals create **Fake Mobile Banking Apps** that closely resemble legitimate ones, using similar logos and interfaces. These apps are distributed through unofficial channels like third-party app stores or phishing links. Once installed, they steal your banking credentials and personal data, leading to financial fraud and identity theft.

✓ Dos:

- **Download from Official Stores:** Always download banking apps from trusted sources like Google Play Store or Apple App Store or bank websites.
- **Verify App Authenticity:** Check the developer details and read reviews before installing any banking app.
- **Keep Software Updated:** Ensure your phone's OS and security software are always current.
- **Enable Two-Factor Authentication (2FA):** Add an extra layer of security to your accounts.
- **Regularly Monitor Bank Accounts:** Review your bank account statements regularly for any unauthorised transactions.

× Don'ts:

- **Don't Download from Unofficial Links:** Avoid clicking on links or downloading apps from suspicious emails or websites.
- **Don't Enter Sensitive Info in Unknown Apps:** Never share banking details in unfamiliar apps or sites.
- **Don't Jailbreak Your Device:** Rooting your device makes it vulnerable to malware and attacks.
- **Don't Share Credentials:** Never share your banking PIN or OTP with anyone, even if they claim to be support staff.

Cyber Slavery

Cyber Slavery involves the exploitation of individuals through digital platforms, where they are coerced or manipulated into working without fair compensation. It overlaps with human trafficking and forced labour but specifically uses the internet and digital tools for exploitation.

✓ Dos:

- **Apply through Verified Agents:** Only apply for jobs through government-approved agencies.
- **Verify Job Offers:** Carefully check the legitimacy of job offers before accepting.
- **Be Cautious of "Too Good to Be True" Jobs:** Watch out for online opportunities that promise high pay for little work.
- **Research Employers:** Always investigate the company or platform offering the job.
- **Report Suspicious Activity:** If you suspect any fraud or exploitation, report immediately on the **"Report Suspect Tab"** of cybercrime.gov.in.

✗ Don'ts:

- **Avoid Quick-Fix Offers:** Don't trust opportunities that promise easy money with little effort or transparency.
- **Never Use a Tourist Visa for Work:** Do not work in a foreign country on a tourist visa.
- **Don't Trust Unverified Social Media Ads or Offers:** Avoid believing ads or offers from unknown people or groups on social media.

SIM Swapping

SIM Swapping is a cybercrime where fraudsters transfer your phone number to their SIM card. This gives them access to your calls, texts, and two-factor authentication codes, enabling identity theft, account hijacking, and financial fraud. Scammers often pose as network staff offering upgrades or benefits to trick you into revealing personal details.

✓ Dos:

- **Enable 2-Factor Authentication:** Add extra security to your accounts.
- **Use Strong PINs:** Set unique and hard-to-guess PINs for your accounts and SIM.
- **Stay Updated:** Keep your phone's software and apps regularly updated.
- **Report Suspicious Activity:** Contact your network provider immediately if you notice unusual activity or lose your SIM.

✕ Don'ts:

- **Protect Information:** Never store sensitive data or share OTPs with strangers via calls or texts.
- **Use Strong PINs:** Avoid easily guessable PINs for your accounts.
- **Report SIM Loss:** Notify your network provider immediately if your SIM card is lost.
- **Monitor Activity:** Watch for unusual mobile activity or extended loss of network access and act promptly.
- **Secure Credentials:** Never share identity details linked to your SIM card.

Money Mules

Money Mules are individuals, knowingly or unknowingly, used to launder illegally obtained funds. Scammers persuade them to receive and transfer stolen money in exchange for commissions. These funds are moved across multiple accounts to obscure the fraudster's identity. Involvement in such activities, whether intentional or not, is illegal and carries severe legal consequences.

✓ Dos:

- **Scrutinise Job Offers:** Be cautious of unsolicited jobs involving money transfers. Research the company's or individual's legitimacy.
- **Guard Financial Information:** Never share bank account details or personal information with unknown parties.
- **Report Suspicious Activity:** Contact authorities if you suspect a money mule scheme.

× Don'ts:

- **Don't Share Accounts:** Never let others use your account to receive or transfer funds.
- **Refuse Commissions:** Reject offers to handle unauthorised money for a fee.
- **Know the Risks:** Transferring illegitimate funds can lead to serious legal action.

Juice Jacking

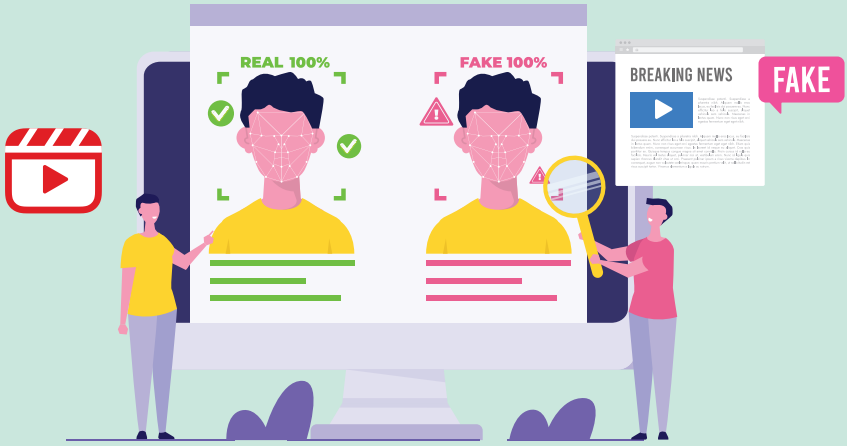
Juice Jacking is a cybersecurity risk associated with compromised public USB charging stations. Hackers can exploit USB ports that charge and transfer data, using them to install malware or steal sensitive information. While no confirmed cases exist, staying vigilant is essential.

✓ Dos:

- **Carry Your Charger:** Use your own charger and cable to avoid potentially tampered public ports.
- **Verify Prompts:** Be cautious of "trust this device" prompts and accept only from trusted sources.
- **Opt for AC Outlets:** Choose standard electrical outlets whenever possible.

✕ Don'ts:

- **Avoid Public Ports:** Do not use unknown or public USB ports or cables.



Deepfake Cybercrime

Cybercriminals use advanced AI to create fake videos or audio clips by manipulating real footage or recordings. These fake media are then spread through social media, messaging apps, and emails, often targeting public figures, celebrities, or people in authority. The goal is to deceive viewers, manipulate opinions, or spread false information. Criminals may use social engineering techniques to make the deepfake seem real, putting individuals and organisations at risk.

✓ Dos:

- **Stay Informed:** Learn about deepfake technology and its risks.
- **Verify Content:** Always check the authenticity of media before sharing or believing it.
- **Use Trusted Sources:** Rely on reputable platforms for news and updates.
- **Report Suspicious Content:** Alert authorities or platforms if you find potential deepfakes.

× Don'ts:

- **Don't Share Unverified Media:** Avoid spreading content without checking its truthfulness.
- **Don't Trust Suspicious Sources:** Stay away from unreliable sources that may share deepfakes.
- **Don't Trust Blindly:** Be cautious of content that seems exaggerated or emotional.
- **Don't Ignore Privacy:** Review privacy settings and limit the personal info you share online

Remote Access Fraud

Remote Access Fraud occurs when cybercriminals impersonate trusted entities. They trick individuals into granting unauthorized access to their devices through screen-sharing apps. Once granted access, they can steal sensitive data, take control of accounts, and carry out fraudulent transactions.

✓ Dos:

- **Trust Carefully:** Never grant remote access to anyone you don't know and trust.
- **Verify Identity:** Confirm the caller's identity directly on your own (not through the numbers they provide).
- **Avoid Unknown Software:** Don't download software at someone's request unless you're certain.
- **Be Cautious:** Remain wary of unsolicited calls, messages, or emails.
- **Enhance Security:** Use strong passwords and enable multi-factor authentication.

× Don'ts:

- **Download Safely:** Only install screen-sharing apps from official sources and when required only.
- **Secure Payment Apps:** Log out of all payment-related apps before downloading any screen-sharing software.
- **Remove After Use:** Uninstall the screen-sharing app once the task is complete.
- **Protect Your Data:** Never share personal or financial information remotely and avoid entering credentials while someone has screen access.

Unsafe Browsing

Unsafe browsing means accessing harmful or untrustworthy websites. downloading dangerous files, or sharing sensitive information on unreliable platforms. This can subject users to risks such as malware. phishing, identity theft (impersonation), and data breaches.

✓ Dos:

- **Use Secure Browsers:** Always browse with updated, secure browsers and ensure sites use HTTPS.
- **Install Antivirus:** Protect your device with trusted antivirus software.
- **Verify URLs:** Check website links before entering sensitive information.
- **Enable Firewalls:** Use firewalls for an added layer of security.

× Don'ts:

- **Avoid Clicking Unknown Links:** Stay away from unverified or suspicious links.
- **Be Cautious on Public Wi-Fi:** Don't use unsecured public Wi-Fi without protection.
- **Don't Save Passwords on Public Devices:** Avoid storing login credentials on shared or public computers.
- **Skip Unsafe Sites:** Don't Ignore browser warnings and avoid visiting flagged or unsecured websites.

Ransomware

Ransomware is a type of malicious software that locks a victim's files, making them inaccessible. Attackers then demand a ransom payment in exchange for key to unlock the file. Ransomware can spread through phishing emails, malicious software downloads, and security flaws. It poses a severe threat to individuals and organizations, causing significant data loss and financial damage.

✓ Dos:

- **Back Up Data:** Regularly back up your data to prevent loss.
- **Use Content Scanning:** Implement timely content scanning and filtering to identify harmful files.
- **Update Systems:** Keep your systems and software up to date to fix security flaws.
- **Employee Training:** Train employees to recognize and avoid phishing attempts and other malicious activities.

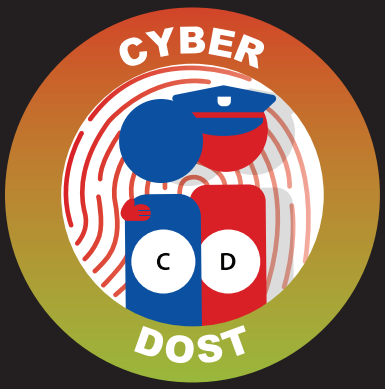
× Don'ts:

- **Avoid Paying Ransom:** Do not pay the ransom, as it does not guarantee the return of data and encourages further attacks.
- **Protect Personal Information:** Do not provide personal information to unfamiliar sources.
- **Contain the Attack:** Do not let the attack spread. Isolate affected systems immediately.
- **Avoid Running Backups During Attack:** Do not run backups during an attack, as they may also become locked.

STOP.

THINK.

TAKE ACTION.



Report such cybercrimes on www.cybercrime.gov.in

or

1930

Keep yourself updated with latest cybercrimes by following **CyberDost** on