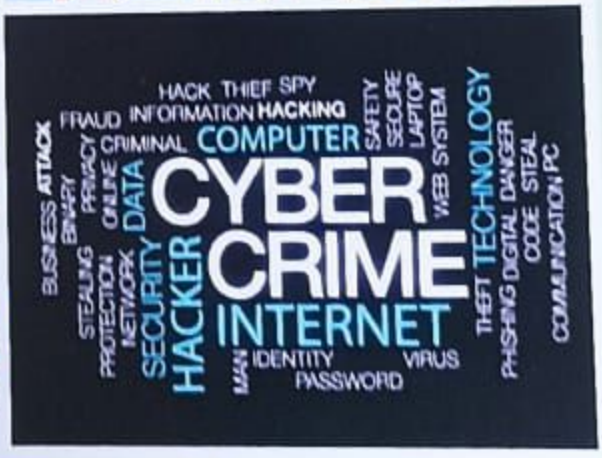
Cyber Safety Awareness Hand Book



Cyber Police Station
New Delhi District

AMRUTHA GUGULOTH, IPS
Deputy Commissioner of Police
New Delhi District

WHAT ARE CYBER CRIMES?

Cybercrimes are offences that may be committed against individuals, companies or institutions by using computers, internet or mobile technology.

Cyber criminals want to get unauthorized access to our sensitive information .In majority of cases, the cyber criminals would advent an attack with a clear cut objective, for that they use some of the most effective methods.

Some common ways used by cyber criminals are:

- **Email Spoofing:** Sending out e-mails to you that look like genuine and from a trusted e-mail ID but actually, they're not.

- **Malicious Files Applications:** Sending you malicious applications and files through direct messaging, emails or websites etc. in order to get access to smart phone and personal data.

- **Identity Theft:** Deliberate use of someone's identity to financial advantage or to obtain credit and other benefits the other person's name/ for counterparts disadvantage or loss.

- **Social Engineering:** Social Engineering is a technique used by cybercriminals to gain your confidence to get information from you. Depending on what you like to do most, a cybercriminal may try to interact with you to mine for information and/or commit some harm to you. Suppose you like to play an online game, an impersonator behaves like another child and invites you to talk to him and share information.

- **Cyber Bullying:** A form of harassment or bullying inflicted through the use of electronic or communication devices such as computer, mobile phone, laptop, etc.

- **Job Frauds:** Fraudulent representation or a deceptive activity on the part of an employee or a prospective employee toward an employer.

- **Banking Frauds:** Fraudulently obtaining money from depositors by posing as a bank or other financial institution's agents.

CYBER BULLYING

Cyber bullying means using internet or mobile technology to intentionally harass or bully someone by sending rude, mean or hartful messages, comments and images/videos. A cyber bully can use text messages, emails, social media platforms, web pages, chat rooms etc.

E-MAIL FRAUD

There are many ways a cybercriminal can use an email to trigger an attack on your system or collect your important information. You may have heard about phishing, vishing, etc.

Online Transaction Fraud

Online transaction fraud means illegally withdrawing or transferring money from your account to another account by a cyber criminal. Online transaction frauds can happen when your login credentials or bank account details or credit card details are stolen by a cyber criminal.

OLX Fraud

OLX is a leading platform to buy and sell goods and services. In this type of fraud, the fraudster usually poses as an army/ paramilitary officer, contacts a person selling products on websites like OLX and Quikr,

App/QR Code Fraud

Fraudsters impersonating as bank agents, ask persons to downlod app namely Quick support, Anydesk or teamViewer. These apps share your screen with fraudsters and all your data/details comprised. Similarly always scan QR Codes with precaution.

Safeguards for your social networking profiles

Social networking sites such as Facebook,Twitter, Instagram, Snapchat, etc., are extensively used by all of us. We love sharing an update or a selfie or pictures with our friends and relatives. We love receiving likes and comments on our posts/pictures and updates. While social networking sites have helped us in connecting with our friends and relatives easily, there are serious cyber threats that can impact us if we are not careful.

How it works?

Cyber criminals and cyber bullies can use social networking platforms to harm us.

- Cyber criminal can create your fake account on social media and use it to share negative things and inappropriate content to harm your image or for other illegal purposes. This is a very real threat and can impact anyone. It is easy to create a social media account using any email id. These days our pictures, email id, date of birth and other details are easily available online. Cyber criminals can use these details to create our fake account.

- Online frauds can be triggered through links shared on social networking sites. Cyber criminals share a post with a malicious link or a malware. If you click on the link, your computer or mobile can be infected or compromised.

Let's discuss how you can protect yourself and your social media accounts. Don't forget to share these suggestions with your family and friends.

- First important step is to safeguard your own social networking account so that it is not hacked or compromised. For this you must use a complex password and change it periodically.

Do you know that most of the social media sites and email service providers give you an option of two factor authentication to login in to your account? You can go to settings and activate two factor authentication. This means you will need to type your password and One Time Password (OTP) received on your mobile to login to your account. It is a good safety feature and should be used for all your accounts.

- Never share password of you social media accounts with anyone. Sharing password may compromise your account.
- Whatever you post on social networking sites can be visible to everyone unless you restrict the access of your posts to your friends/followers. You must change the privacy settings of your social media account and ensure that your updates/posts, etc. are visible to your friends/followers only.
- Never install unwanted software and apps from unknown sources. Never click on links or files received from unknown person on social media. This may be an attempt to infect your computer with a malware.

- Fake news or Hoax messages spread like wildfire on social media. Before forwarding or sharing any message on social media or messaging app, check it on other sources also to confirm its authenticity.
- If you are accessing social media accounts on your mobile phone,remember to keep a strong password to access your phone.
- If your social media account is hacked/compromised, send an alert email or message to all your contacts. Immediately ask your social media service provider to temporarily block your account. Try to retrieve your password and change your password immediately.
- If you notice that your fake account has been created, you can immediately inform social media service provider so that the account can be blocked. If someone is bullying you, posting inappropriate comments or images or creating your fake account to damage your image, inform your parents or elders immediately so that they can support and guide you. With support from your parents, you can also register a complaint at your nearest police station.

Hope you enjoyed reading this handbook. These suggestions should help you in protecting yourself from cybercrimes. As you know cybercriminals frequently devise new ways to cheat people. It is important to remain up to date with new threats and ways to protect ourselves.

Few suggestions from us:-

- Read more about cybersecurity, emerging new threats and ways to safeguard against cybercrimes.
- Be a good cyber citizen. Use precautions yourself and educate your friends and family about cyber security

Law For Cyber Crime

The Information Technology Act 2000, Deals With Cyber Crime In India.

Section	Type of Offence	Punishment
66	Computer Related Offences	3 Years + 5 Lac Fine
66 C	Identity Theft	3 Years + 1 Lac Fine
66 D	Cheating By Personation	3 Years + 1 Lac Fine
66 E	Violation Of Privacy	3 Years + 2 Lac Fine
67	Publishing/transmitting Obscence Material	3 Years + 5 Lac Fine
66 A	Publishing/transmitting Sexually Explicit Material	5 Years + 10 Lac Fine
66 B	Child Pornography	5 Years + 10 Lac Fine

For any cyber threat/complai

1930

www.cybercrime.gov.in

साइबर सेल नई दिल्ली जिला दिल्ली पुलिस

कृपया ध्यान दें, साइबर अपराध की जानकारी ही बचाव है, जिससे बचाव हेतु निम्न जानकारी का होना अतिआवश्यक है:-

- **गूगल सर्च पर आंख बन्द कर भरोसा ना करे।**
- **बहुत सारे साईबर अपराधी गूगल/फेसबुक/वॉट्सएप/इंस्टाग्राम पर अपने मोबाइल No. डाल रखे है। कृपया इनके झांसे मे ना आये।**
- **आक्सीजन सिलेंडर, रेमडेसिविर इन्जेक्शन या अन्य दवाओं के लिये गूगल सर्च पर भरोसा करके किसी के खाते में पैसे नही डाले।**
- **हमेशा कैश ऑन डेलीवरी पर भरोसा करें।**
- **स्मार्ट साईबर स्पेस यूजर बने और इस मुश्किल घड़ी में साईबर फ्रॉड से बचे।**
- *www.cybercrime.gov.in* **पर साईबर आपराध को रिपोर्ट करें।**

Cyber Crime Helpline Number 155260 OR Report here, 01123469900

नई दिल्ली जिला, दिल्ली पुलिस साईबर सेल के तरफ से जनहित मे जारी।

जागरूक रहें, सतर्क रहें

स्वंय जागरूक बनें, औरों को भी करें

जागरूकता ही बचाव है

लालच बुरी बला है ....

नई दिल्ली जिला, दिल्ली पुलिस

जिला कंट्रोल रूम नं.: 011-23362229, 23348494

ईमेल : dcp-newdelhi-dl@nic.in / acpcybercell.ndd@delhipolice.gov.in

ट्विटर : @DCPNewDelhi

दिल्ली पुलिस

दिल्ली पुलिस

सायबर अपराध से बचाव हेतु जागरूकता अभियान

- फोन कॉल/SMS या अन्य किसी माध्यम से OTP या UPI, MPIN, ATM PIN किसी के साथ शेयर न करे।
- KYC के लिए SMS पर ध्यान ने दें, और न ही SMS में दिए गए मोबाइल न. पर कॉल करे।
- SMS या WhatsApp पर आये किसी भी लिंक या Google form (जिस पर किसी भी कंपनी, बैंक, ई-वॉलेट आदि का नाम हो सकता है) में कोई भी अपनी निजी जानकारी जैसे- UPI, MPIN, ATM PIN बैंक, में पंजीकृत मोबाइल न., कार्ड न. रूपये (रूपये 01,02,05,10 या 20 रूपये जैसी छोटी रकम हो सकती है) आदि दर्ज न करें। छोटे amount का झांसा/लालच देकर आपकी निजी जानकारी चुरा लेना मकसद होता है।
- किसी के भी कहने पर रिमोट एक्सेस ऐप जैसे- Quick support, Any desk, team, team viewer, Aindroid आदि न तो प्ले store/App Store या लिंक के माध्यम से डाउनलोड करे और ना ही उसका पिन व ID किसी को शेयर करे।
- फोन या ने किसी माध्यम से प्राप्त SMS को अज्ञात व्यक्ति के द्वारा बतलाये गए न. पर Forward न करे।
- ATM मशीन से काश निकासी/जमा करते समय किसी की सहायता न ले, साथ ही अपने कार्ड के पीछे वाली सफेद पट्टी पर अपना नाम अवश्य लिखे, ताकि कार्ड बदले जाने पर तुरंत पहचान कर सके।
- बिना गार्ड वाले ATM मशीन को इस्तेमाल करने से बचे, पिन को हाथ से छुपाकर डाले।
- ATM कार्ड का पिन हमेशा समय-समय पर चेंज करते रहे।
- फोन, ईमेल SMS, WhatsApp या न्यूज पेपर के माध्यम से प्राप्त नौकारी, लौटरी, पालिसी बौनस, सस्ता लोन आदि पर भरोसा न करे, साथी ही बताये गए Paytm या अन्य किसी वालेट में या किसी बैंक खाते में रूपयों का स्थान्तरण या कैश जमा न करे।
- OLX या अन्य जगह पर खरीदारी या सामान बेचते समय QU Code या Request Money का इस्तेमाल न करे।
- WhatsApp आदि के माध्यम से भेजे गए QR Code या Request Money को स्कैन न करे।
- रूपये प्राप्त करने हेतु किसी भी लिंक पर क्लिक नहीं करना होता है और न ही Pay के बटन को दबायें।
- फर्जी NEFT/RTGS पर भरोसा न करे, भुगतान प्राप्त होने पर ही सामान की डिलेवरी करे।
- Google पर सर्च किये Customer Care नंबर का इस्तेमाल न करे, धोखा हो सकता है।
- किसी भी समस्या के होने पर बैंक, ई-वालेट या अन्य सम्बन्धित की असली वेबसाइट पर ही जाकर कस्टमर केयर नंबर या इमेल आदि का इस्तेमाल करे।
- Facebook/Instagram/Twitter, E-mail, WhatsApp, Telegram आदि किसी भी सोशल साइट्स/ऐप के माध्यम से की गई बात/चैट या धन कि मांग पर भरोसा न करे, फोन करके या मिलकर या अन्य किसी माध्यम से कन्फर्म अवश्य करे।
- अनजान नंबर से WhatsApp पर आई विडियो कॉल पर अपना आपतिजनक विडियो शेयर ना करे। आपके साथ ब्लेक मैलिंग हो सकती है।

जागरूकता ही बचाव है, जागरूक रहे और सुरक्षित रहे

नई दिल्ली जिला, दिल्ली पुलिस

जिला कंट्रोल रूम नं.: 011-23362229, 23348494

ईमेल : dcp-newdelhi-dl@nic.in / acpcybercell.ndd@delhipolice.gov.in

ट्विटर : @DCPNewDelhi