मोबाईल, इंटरनेट–ईमेल, सोशल नेटवर्किंग साईट्स एवं ऑनलाईन बैंकिंग के उपयोग में बरती जाने वाली सावधानियाँ

साईबर स्पेस सूचनाओं का एक राजमार्ग है जो कि मुख्यतः 2 भागों से बना होता हैः–

1. **टेलीफोन नेटवर्क**
   (अ). लैंडलाईन फोन
   (ब). मोबाईल फोन
   (स). सैटेलाईट फोन

2. **कम्प्यूटर नेटवर्क**
   (अ). लॉकल एरिया नेटवर्क
   (ब). वाईड एरिया नेटवर्क
   (स). इन्टरनेट वर्ल्डवाइड नेटवर्कः इन्टरनेट सोसायटी ISOC द्वारा नियमित

सड़क पर वाहन चलाते समय आप हेलमेट, सीट बैल्ट, लेन ड्राईविंग, गति अवरोधक इत्यादि का उपयोग करते हुए अपनी सुरक्षा करते है, उसी प्रकार जब आप सूचनाओं के राजमार्ग पर होते है तो आपको कई सुरक्षा युक्तियों की पालना करनी होती है। वाहन चलाने के मामले में सर्वप्रथम आपको उस वाहन को चलाना सीखना होता है जिसे आप चलाना चाहते है, परंतु साईबर स्पेस के मामले में सीखने की प्रक्रिया या तो बहुत अनौपचारिक होती है या पूरी तरह से उपेक्षित होती है। यूजर्स की यही उपेक्षा साईबर स्पेस में सक्रिय अपराधियों के फलने–फूलने में सहायक होती है।

सम्मोहन विद्या (Hypnotism) पीड़ित को किसी भी भौतिक या साईबर वर्ल्ड से संबंधित धोखाधड़ी की ओर आकर्षित करने का सबसे महत्वपूर्ण कारक है, जिसे मानव की लालची प्रवृति से और अधिक बल मिलता है।

साईबर अपराध के क्षेत्र में किये गये अध्ययन यह दर्शाते हैं कि इस प्रकार के अपराधों के मुख्यतः 4 कारण हैः

- **किसी से छेड़खानी करने / क्षति पहुँचाने / अस्त–व्यस्त करने के लिए**
  - सामान्यतः राष्ट्रविरोधियों द्वारा ऐसा किया जाता है
- **किसी के चरित्र / प्रतिष्ठा को क्षति पहुँचाने के लिए**
  - ऐसा प्रायः लड़कियों, कम्पनियों या बैंको के उच्च प्रबन्धकों के साथ होता है
- **पेशेवर प्रतिद्वंद्वियों को क्षति पहुँचाने के लिए**
  - कोर्पोरेट कम्पनियों, व्यक्तिगत मामलों में
- **धन प्राप्त करने के लिये**
  - एटीएम / क्रेडिट कार्ड, ऑनलाईन बैंकिंग, नाईजीरियन फ्रॉड / प्लेसमेंट / टावर / फोन कॉल्स / एसएमएस, नवीनतम विवाह संबंधी, आईईडी जैसे शोध पत्र।

आईटी एक्ट 2001 एवं संशोधन एक्ट 2009ः भारत में साईबर अपराधों पर नियंत्रण हेतु विस्तृत कानून

मोबाईल सुरक्षा सलाहः

1. अपना फोन सदैव अपने पास रखें।
2. किसी अनजान व्यक्ति को अपना फोन उधार न दें।
3. अधिकतर फोन में फोन को लॉक करने के लिये कोड की सुविधा होती है। यदि आपके पास कोड नहीं है तो आप फोन को अनलॉक नहीं कर सकते, इसलिये यदि कोई आपके फोन को चुराता है तो वह उसे उपयोग नहीं कर सकेगा।
4. यदि आपके फोन में ब्लूटूथ है और इसे उपयोग में नहीं ले रहे है तो ब्लूटूथ को स्विच ऑफ रखें।
5. अपने स्मार्टफोन में वाई–फाई को बन्द रखें एवं पब्लिक वाई–फाई हॉटस्पॉट का उपयोग न करें।
6. यदि एन्ड्रॉयड, ब्लैकबेरी, एप्पल आईफोन जैसे स्मार्टफोन का उपयोग कर रहे हैं तो सोशल नेटवर्किंग साईटस एवं कैमरा सैटिंग्स में जीपीएस को डिसेबल रखें, GEO TAGGING को भी डिसेबल रखें क्योंकि इससे आपकी लोकेशन को पब्लिक डोमेन पर शेयर करने का खतरा रहता है।
7. अनाधिकृत एप्प डाउनलोड ना करें।
8. मिस्ड कॉल के रूप में अनजाने नम्बरों से, विशेषतः 4,7,11 एवं 13 अंको वाले नंबरों से आने वाले कॉल्स को रिप्लाई ना करें ना ही इन नंबरों पर कॉल बैक करे। यदि आप कॉल बैक करते हैं तो आपको उच्च दरों पर कॉल चार्ज लग सकता है। यह प्रीमियम नंबर कॉलिंग धोखाधड़ी कहलाता है।
9. प्राईज या अवार्ड जीतने के ऑफर देने वाले आकर्षक या प्रलोभित करने वाले एसएमएस का रिप्लाई ना करें।
10. जब भी अपने हैंडसेट को रिपेयरिंग के लिये दें, तो पहले अपने मैमोरी कार्ड, सिमकार्ड एवं बैटरी को निकाल लें साथ ही अपनी व्यक्तिगत सूचनाओं को फोन मैमोरी से मैमोरी कार्ड में स्थानांतरित कर लें।
11. बच्चों को अपने व्यक्तिगत नंबर पब्लिक प्लेसेज पर किसी को नहीं देने चाहिए ऐसी स्थिति में सदैव अपने परिजनों के नंबर देवें।
12. अपने व्यक्तिगत/अंतरंग फोटोग्राफ अपने मोबाईल में स्टोर ना रखें क्योंकि यदि फोन चुरा लिया जाता है या कहीं गिर जाता है तो इनका दुरूपयोग किया जा सकता है।

स्मार्ट सर्फिंगः

1. सदैव वास्तविक ऑपरेटिंग सिस्टम, नियमित रूप से इंटरनेट से अद्यतन एंटीवायरस/इंटरनेट सुरक्षा सॉफ्टवेयर का उपयोग करें।
2. ब्राउजर को ऑटोमैटिक इंस्टाल होने वाले टूलबार्स से मुक्त रखें।
3. अपने ब्राउजर एवं इंस्टेंट मैसेन्जर्स जैसे याहू, गूगल, स्काईप इत्यादि पर अपने पासवर्ड सेव ना करें।
4. अपने ब्राउजर की टेंपरेरी कैशे, कुकीज को नियमित रूप से क्लीयर करें।
5. ब्राउजिंग करते समय पॉप अप्स या विज्ञापनों से शॉर्टकट्स एवं टूलबार्स को इंस्टाल ना करें।

6. अविश्वसनीय साईट्स से नकली/ चुराये हुए (पायरेटेड) चीजें (जैसे म्यूजिक वीडियोज, फ्री सॉफ्टवेयर्स) डाउनलोड ना करें।
7. सदैव मूल साईट (पेरेंट साईट) पर उपलब्ध सॉफ्टवेयर्स ही डाउनलोड करें।
8. आकर्षक/ प्रलोभित करने वाले संदेहास्पद लिंक्स/ हाइपरलिंक्स पर क्लिक ना करें।

ईमेल सुरक्षाः

1. अपने पासवर्ड को 8 कैरेक्टर्स से अधिक का रखें साथ ही स्पेशल कैरेक्टर्स एवं एल्फान्यूमेरिक अक्षरों एवं बड़े व छोटे अक्षरों का पासवर्ड में समावेश करें।
2. अपने सभी अकाउण्टस के लिये एक ही पासवर्ड का उपयोग ना करें।
3. सुरक्षा प्रश्न, मोबाईल एसएमएस अलर्ट, सैकण्डरी ईमेल एड्रेस इत्यादि को चालू (इनेबल) रखें।
4. पब्लिक नेटवर्क/वाईफाई पर सदैव HTTPS के साथ साईट में लॉगिन करें।
5. सार्वजनिक स्थानों पर फ्री वाईफाई एक्सेस का उपयोग ना करें।
6. स्पैम/जंक ईमेल्स पर क्लिक ना करें।
7. अपने ईमेल पासवर्ड किसी के साथ शेयर ना करें।
8. जब किसी ईमेल को एक से अधिक लोगों को अग्रेषित (फॉरवर्ड) करना हो तो ईमेल एड्रेसेज लिखने के लिये BCC ऑप्शन का उपयोग करें।
9. यदि आप अपना ईमेल अकाउंट एक्सेस नहीं कर पा रहे हैं तो तुरंत मेल सेवा प्रदाता को रिपोर्ट करें, वे आपको फॉरगोट पासवर्ड विकल्प/अकाउंट हैकिंग के बारे में जानकारी देंगें।

सोशल नेटवर्क/चैटिंगः

1. अपनी व्यक्तिगत/ सम्पर्क संबंधी जानकारी सोशल नेटवर्किंग साईट्स पर ना डालें।
2. पब्लिक डोमेन में सोशल मीडिया पर अपनी या अपने परिवार के फोटोग्राफ ना डालें।
3. किसी भी सेवा को उपयोग में लेने से पहले प्राईवेसी सैटिंग्स/सुरक्षा सैटिंग्स का बुद्धिमतापूर्ण उपयोग करें।
4. किसी भी अनजान/अस्पष्ट मित्र के साथ अपने फोटोग्राफ या वैबकैम को शेयर ना करें।
5. यदि आप किसी प्रकार की साईबर स्टाकिंग (आपकी ऑनलाईन गतिविधियों का किसी के द्वारा अनाधिकृत रूप से ट्रेक करना) के शिकार होते हैं तो तुरंत साईट के सेवा प्रदाता या नजदीकी साईबर सैल (पुलिस थाना) पर संपर्क करें।
6. सोशल मीडिया पर कभी अपनी लोकेशन अपडेट ना करें।
7. किसी अनजान को अपनी मित्र लिस्ट में ना जोड़ें। अपने प्राईवेसी ऑप्शंस को FRIENDS ONLY के लिए सिक्योर्ड रखें अनजान मित्रों को तुरंत अपनी प्रोफाईल से ब्लॉक करें।
8. सोशल मीडिया पर दिखने वाले संदेहास्पद पोस्ट एवं विज्ञापनों पर क्लिक ना करें। आपके अकाउंट में बहुत सारे गलत सूचना सहित भ्रामक एवं आकर्षक स्पैम लिंक्स दिख सकते हैं उन पर क्लिक ना करें एवं इनको तुरंत स्पैम के रूप में रिपोर्ट करें। उदाहरणार्थः
    - अपने मोबाईल को मुफ्त में रिचार्ज करें.....
    - देखें किसने आपकी प्रोफाईल को विजिट किया.....

- आपको एक विडियो में टैग किया गया है..... विडियो देखें.....
- आपका अकाउंट स्लो है अपने यूजर आईडी एवं पासवर्ड से इसे वेरिफाई करें।

फेसबुक सुरक्षा हेतु सलाहः

- अपनी मित्र लिस्ट में उन्हीं को जोड़ें जिन्हें आप जानते हैं।
- अच्छा एवं मजबूत पासवर्ड बनाएं एवं इसे केवल फेसबुक के लिए ही उपयोग करें।
- अपने पासवर्ड किसी के साथ शेयर ना करें।
- नियमित रूप से पासवर्ड बदलें।
- प्रत्येक सेशन (Session) में केवल एक बार फेसबुक लॉगिन करें। यदि फेसबुक की तरह दिखने वाली कोई साईट दूसरी बार लॉगिन करने के लिये मैसेज देती है तो उस लिंक को छोड़ें एवं सीधे ब्राउजर की एड्रेस बार में www.facebook.com टाइप करें।
- यदि किसी अन्य व्यक्ति का कम्प्यूटर उपयोग में ले रहे हैं तो वन टाईम पासवर्ड (OTP) का उपयोग करें एवं उपयोग के बाद फेसबुक को लॉगआउट कर देवें।
- किसी भी व्यक्ति की बेहूदा पोस्ट से बचें चाहे वह किसी मित्र द्वारा ही क्यों ना पोस्ट की गई हो। यदि आपको लगता है कि यह आपके मित्र द्वारा पोस्ट नहीं की गई है तो इस पर क्लिक ना करें। हैकर्स आपके मित्र के अकाउंट को हैक कर उनके अकाउंट पर लिंक्स भेज सकते हैं।

ई–फ्रॉड को रोकनाः

1. ऑनलाईन शॉपिंग/ बैंकिंग सुविधा का इंटरनेट पर उपयोग करते समय संवेदनशील सूचना दर्ज करते समय सदैव वर्चुअल कीबोर्ड (VIRTUAL KEYBOARD) का उपयोग करें।
2. ऑनलाईन शॉपिंग/ बैंकिंग सुविधा का इंटरनेट पर उपयोग करते समय वास्तविक ऑपरेटिंग सिस्टम एवं एंटीवायरस सहित कम्प्यूटर का उपयोग करें।
3. ऑनलाईन शॉपिंग/ बैंकिंग सुविधा का इंटरनेट पर उपयोग सार्वजनिक नेटवर्क एवं सार्वजनिक स्थानों पर ना करें।
4. अपने नेट बैंकिंग पासवर्ड किसी के साथ शेयर ना करें।
5. अपने नेट बैंकिंग पासवर्ड/ क्रेडिट कार्ड की डिटेल फोन, एसएमएस या ईमेल पर शेयर ना करें।
6. खरीददारी के लिये कार्ड का उपयोग करते समय कार्ड को अपनी आंखों के सामने स्वाईप करें।
7. अपने कार्ड के पीछे लिखे सीवीवी कोड (CVV Code) को मिटा देवें एवं इसे याद रखें।
8. अपने कार्ड को उपयोग में लेने से पहले इसे हस्ताक्षरित करें।
9. एटीएम काउंटर पर धोखाधड़ी से सावधान रहें
    - अपनी लेनदेन पर्ची को कचरा पात्र में ना फेंके।
    - सावधान रहें कि कोई आपके पीछे खड़ा आपको देख तो नहीं रहा।
    - मशीन के पूर्णतया लॉग ऑफ होने के बाद ही एटीएम काउंटर को छोड़ें।
    - एटीएम पर किसी प्रकार की अनापेक्षित सहायता ना लेवें।

10. सुरक्षा कारणों से आपके अकाउंट को वेरिफाई करवाने के लिये जाली ईमेल जो बैंक से भेजी गई प्रतीत होती है उन ईमेल्स पर क्लिक ना करें।
11. अवार्ड/लॉटरी/बिजनस अवसर/जॉब अवसर का ऑफर देने वाले आकर्षक एवं भ्रामक ईमेल जाली और धोखाधड़ी वाले होते हैं।
12. ऑनलाईन आयकर रिफंड का दावा करने वाले ईमेल्स जाली एवं धोखाधड़ी वाले होते हैं।
13. अवार्ड/लॉटरी/बिजनस अवसर/जॉब अवसर का ऑफर देने वाले आकर्षक एवं भ्रामक मोबाईल संदेश जाली और धोखाधड़ी वाले होते हैं।
14. ऑनलाईन शॉपिंग/ बैंकिंग का उपयोग करते समय जिस डोमेन (यूआरएल) पर आप काम कर रहे हैं उसे जाँच लेवें यह HTTPS एवं PADLOCK सहित होना चाहिए एवं यूआरएल सदैव उस मूल साईट (पेरेंट साईट) का होना चाहिए जिस पर आप काम करना चाहते हैं।
15. अपने कार्ड एवं बैंक अकाउंट पर एसएमएस अलर्ट सुविधा चालू करवायें जब भी आप अपना रजिस्टर्ड मोबाईल नम्बर बदलना चाहें तो संबंधित बैंक को लिखित में सूचित करें।
16. अपना वन टाईम पासवर्ड (OTP) किसी के साथ शेयर ना करें।

यदि आप किसी प्रकार की साईबर धोखाधड़ी का शिकार होते हैं तो शीघ्र अपने नजदीकी पुलिस स्टेशन या अधोलिखित पुलिस थाने में शिकायत दर्ज करवायें:

साईबर क्राईम पुलिस स्टेशन,
राजस्थान, जयपुर
टेलीफोन न0 0141–2309547, 2309548
ईमेल आईडी: ccps-raj@nic.in, ps.ccps.scrb@rajpolice.gov.in

Caution in the use of Mobile, Internet- email & Social Networking Sites and Online banking

Cyber Space spreads over Information Highway which in turn, is made up of 2 major components

1. **Telephone Network**
    a. Landline Phone
    b. Mobile Phone
    c. Satellite Phone
2. Computer Network
    a. LAN: Local Area Network
    b. WAN: Wide Area Network
    c. Internet Worldwide Network: Governed by INTERNET SOCIETY ISOC

While driving on a road, you protect yourself by using helmet, seat-belt, lane driving, following speed restrictions etc, similarly you need to follow apt safety measures when you are on the Information Highway. In case of the former, you first learn to drive whatever vehicle you intend to use, but in case of the latter, the process of learning is either very informal or completely bypassed. It helps criminals in cyber space to thrive on account of the user's ignorance.

Hypnotism is the most vital factor to lure a victim into any fraud net in physical as well as Cyber world. It is further facilitated by greed, a very pressing human factor.

The studies in the field of cybercrimes have revealed that broadly three are 4 reasons for committing such a crime:

- **To tease/ mischief/ disrupt**
    - Normal to anti-national
- **To harm the character/reputation**
    - Most common with girls, top management in companies/banks
- **To harm professional rivals**
    - Corporate companies, individuals
- **To gain money**
    - ATM/Credit card, Online banking, Nigerian fraud/placement/tower/phone calls/SMS, latest matrimony, research paper **like IED** with an element of surprise

IT ACT 2001 WITH AMENDMENTS IN 2009: DETAILED LAW TO HANDLE CYBERCRIMES IN INDIA

MOBILE SAFETY TIPS

1. Keep your phone with you at all times.
2. Don't lend your phone to someone you don't know or trust.
3. Most phones allow you to lock your phone with a code. If you don't have the code, you can't unlock it, so if anyone steals your phone he won't be able to use it.
4. If you have Bluetooth on your phone, keep this switched off when you are not using it.
5. Keep your WIFI Off- on a smartphone and also don't connect to PUBLIC WIFI-HOTSPOT in public places.
6. If using Smart phone like Android, blackberry, Apple IPHONE, keep GPS disabled with Social Networking Sites and in Camera Settings, keep GEO TAGGING DISABLED as it has a threat of sharing your location in public domain.
7. Don't download unauthenticated applicants from market.
8. Don't reply or call back on unidentified numbers specially 4, 7, 11 to 13 digit numbers even coming as missed call. When you call back, you may be charged on very high tariff. It is called Premium number calling fraud.

9. Don’t reply to SMS with luring or tempting offers of Prize Winning or award winning.
10. Whenever give your handset for repair or maintenance, always remove memory card, Sim card, battery and then give. Transfer all your personal information from phone memory to memory card before giving it.
11. Kids should always give their parents umber in public places, don’t share your personal number.
12. Don’t store personal/intimate pictures in your mobile phones because if stolen or dropped, they can be very vulnerable.

SMART SURFING

1. Always use genuine Operating System, Antivirus/Internet Security Software, regularly updated with Internet.
2. The Browser should be kept free from toolbars which get automatically installed on your browser.
3. Never save your passwords on your browsers and Instant Messengers like yahoo, Google, Skype etc.
4. Keep your browser’s temporary cache, cookies clear on regular basis.
5. While browsing, don’t install shortcuts and toolbars from pop ups and ads.
6. Don’t download pirated stuff from untrusted sites. (eg. Music videos, free Softwares).
7. Always install software’s available at the parent sites.
8. Don’t click on suspicious links/hyperlinks which are luring and tempting.

EMAIL SECURITY

1. Keep your passwords more than 8 characters with alphanumeric and special characters also using UPPER and Lower case. Eg. ArAvind@#35
2. Never keep same passwords for all your accounts.
3. Security Question, Mobile SMS Alert, Secondary Email Address should be enabled.
4. Always login the site on Public networks/WIFI with HTTPS.
5. Avoid using FREE WIFI Access at public places.
6. DON’T Click on SPAMS/Junk Mail.
7. Never share your email password with anyone.
8. Whenever you need to forward an email to more than one person use the BCC option to write addresses.
9. If you are unable to access your email account, immediately report it to the Mail Service Provide. They give you an option of forgot password/Account hacked etc.

Social Networks/Chats

1. Never post your personal/Contact information on the social networking sites.
2. Don’t publish your pictures/family pictures on the social media in public domain.
3. Use the Privacy settings/security settings of the site wisely before you start using the service.
4. DON’T FLIRT/Make anonymous friends or share your pictures/webcam with them.
5. In case your are Cyber Bullyed/Cyber stalked immediately report to the service provider of the site or the nearest Cyber Cell (Police Station)
6. Never update your whereabouts on the social media. Like your current location etc.
7. Don’t Add unknown friends to your account. Keep your privacy options secured for FRIENDS ONLY. Immediately block unknown friends from your profile.
8. Don’t click on suspicious posts and Ads appearing on social media. A lots of SPAM Links, luring and tempting with FALSE information can appear on your account. DON’T Click on them and immediately report it as SPAM. For Eg.
    a. GET YOUR MOBILE RECHARGED FREE…..
    b. SEE WHO VISITED YOUR PROFILE…..
    c. YOUR ARE TAGGED IN A VIDEO… WATCH THE VIDEO …
    d. ACCOUNT GETTING SLOW VERIFY YOUR ACCOUNT WITH YOUR USER ID AND PASSWORD …etc…

Tips for facebook Security

- Only Friend people you know.
- Create a good password and use it only for Facebook.
- Don't share your password.
- Change your password on a regular basis.
- Log into facebook only ONCE each session. If it looks like Facebook is asking you to log in a second time, skip the links and directly type www.facebook.com into your browser address bar.
- Use a one-time password (OTP) when using someone else's computer. Log out of Facebook after using someone else's computer.
- Beware of "goofy" post from anyone, even from Friends. If it looks like something your friend wouldn't post, don't click on it. Scammers might hack your Friend's accounts and send links their accounts.

PREVENT E-FRAUDS

1. While using online Shopping/banking facility on your Internet, always USE THE VIRTUAL KEYBOARD to enter sensitive details.
2. Whenever you use online Shopping/banking, do it from a PC which is secured with genuine OS and antivirus.
3. Don't use public networks and public places to do Online shopping/banking.
4. Don't share your banking passwords with anyone.
5. Never give your Banking Passwords/Credit Card Detail on phone, sms or Emails.
6. Whenever using your CARD for shopping, get it swiped in front of your eyes.
7. Erase the CVV Code from the back side of your card and remember by heart.
8. Always keep your card signed before you start using it.
9. At ATM Counters, be careful of cheats.
    - Don't leave your Transaction slip at the dustbin.
    - Just be careful of nobody standing behind you and watching you
    - Leave the ATM Counter when the machine is completely logged off.
    - Don't entertain unsolicited help at the ATM.
10. Lots of FAKE EMAILS posing them to be from the bank asking you to verify your account due to security reasons. DON'T CLICK ON SUCH EMAILS.
11. Emails with luring awards/Lottery/business Opportunity/JOB Opportunity asking you to deposit money to claim are all FAKE/FRAUD.
12. Emails claiming for online INCOME TAX REFUND are all fake/fraud.
13. SMS on mobile for awards/lottery/winning alerts are FAKE/FRAUD.
14. While doing Online Shopping/Banking always check the DOMAIN (URL) you are working on. It should have HTTPS and PADLOCK. The URL should be of the parent site you are working on.
15. ACTIVATE SMS ALERT Facility on all your Cards and Accounts. Whenever you change your registered Mobile Number, Do intimate to the concerned BANK in Writing.

16. **NEVER SHARE YOUR OTP ON ANY PRETEXT.**

If you fall prey to any fraud net, you must lodge a complaint with your police station or

Cyber Crime Police Station,
Rajasthan, Jaipur
Telephone no. 0141-2309547, 2309548