केवल जागरूकता के लिए

JUDICIAL ACADEMY

LEARNING
ENDURING JUSTICE

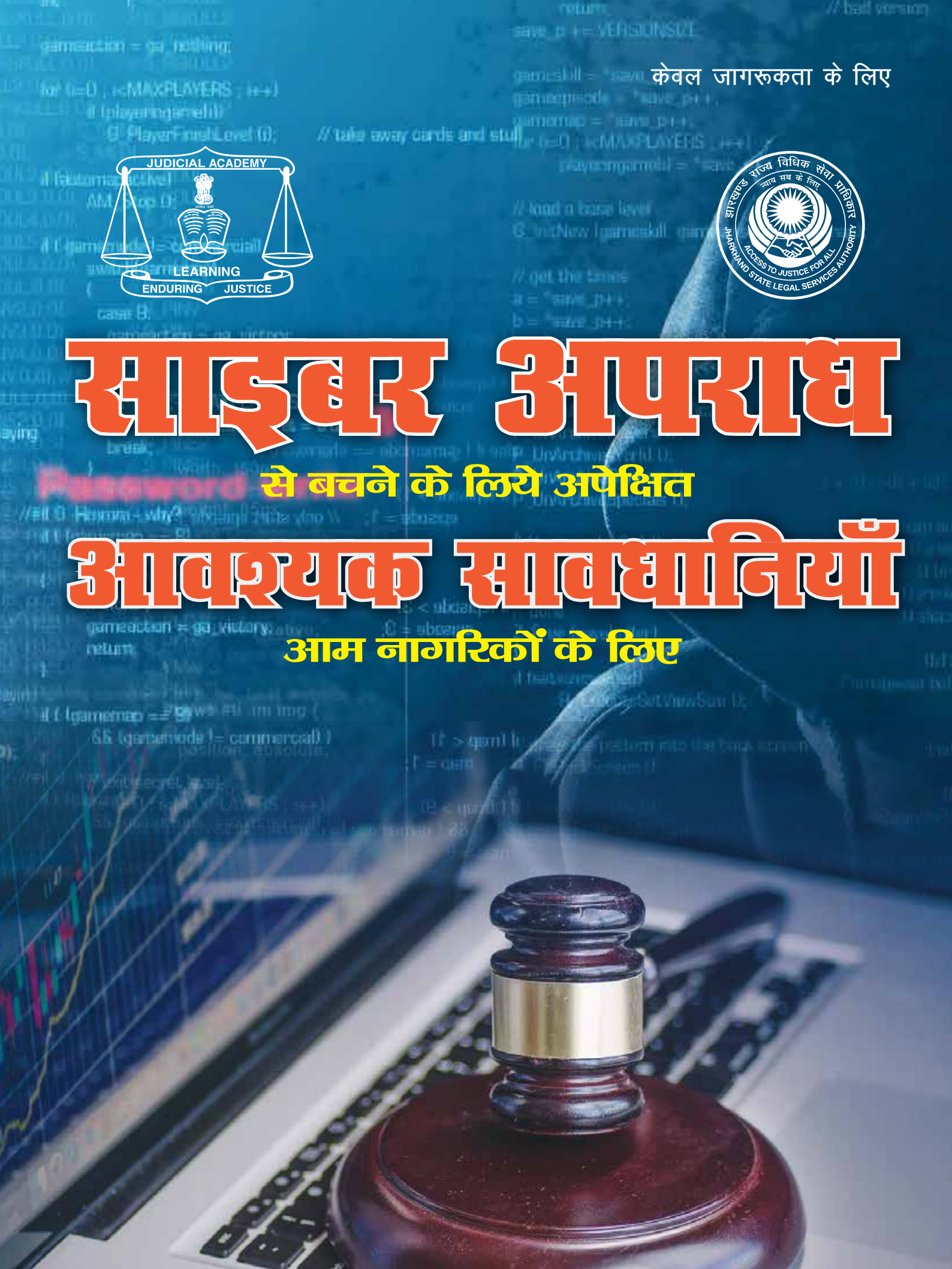
झारखण्ड राज्य विधिक सेवा प्राधिकार
न्याय सब के लिए
ACCESS TO JUSTICE FOR ALL
JHARKHAND STATE LEGAL SERVICES AUTHORITY

साइबर अपराध

Password से बचने के लिये अपेक्षित

आवश्यक सावधानियाँ

आम नागरिकों के लिए



साइबर अपराध से बचने के लिये अपेक्षित आवश्यक सावधानियाँ आम नागरिकों के लिए

भारत इंटरनेट इस्तेमाल करने वाला विश्व का तीसरा देश है। आज हम अपने मोबाइल एवं कम्प्यूटर के माध्यम से बैंकिंग के काम, खरीदारी एवं अन्य दैनिक कार्य करते हैं। इन्टरनेट, मोबाइल एवं कम्प्यूटर का इस्तेमाल आजकल ज्यादा होने के कारण साइबर अपराध में वृद्धि हो रही है, जिससे बचने के लिए कुछ सर्तकता आवश्यक है।

1. सुरक्षित इंटरनेट बैंकिंग कार्यप्रणाली

व्यवहार जो अपेक्षित नहीं हैं :

- अज्ञात स्रोत से फाइल का डाउनलोड।
- पॉप-अप विंडो द्वारा ड्राइवर आदि का डाउनलोड।
- किसी भी वेबसाइट को बिना पूर्ण जानकारी के अपने कम्प्यूटर पर सॉफ्टवेयर इनस्टॉल करने की अनुमति।
- किसी भी अनजान फेसबुक लिंक/संदेश लिंक पर क्लिक।

RBI Circular

आर० बी० आई० के पत्र संख्या RBI/2017-18/15 DBR. No. Leg. BC. 78/09.07.005/2017-18 दिनांक 6/7/2017 के आलोक में यदि उपभोक्ता की गलती नहीं हो तो बैंक से अवैध निकासी की गई राशि बैंक वापस देगा।

व्यवहार जो अपेक्षित है :

- अपनी निजी जानकारी एवं पासवर्ड को सुरक्षित रखें, डेबिट कार्ड, क्रेडिट कार्ड का नम्बर किसी को न बताएँ।
- फायरवॉल तकनीक, प्रॉक्सी सर्वर एवं सुरक्षित राउटर कॉन्फिग्रेशन करे।

2. सुरक्षित ईमेल कार्यप्रणाली

व्यवहार जो अपेक्षित नहीं हैं :

- ईमेल पर आए संलग्न वस्तु को खोलने के समय आवश्यक सावधानी बरतें अनापेक्षित अकारण अज्ञात ईमेल बिना पुष्टि के नहीं खोलें नहीं जवाब दें।

- अज्ञात ईमेल में दिए गए अज्ञात लिंक जैसे जोक्स, वीडियो पर क्लिक ना करे अपना PIN/OTP/पासवर्ड किसी को न बतायें।

व्यवहार जो अपेक्षित है :

- पासवर्ड मजबूत बनायें अर्थात पासवर्ड में कैरेक्टर, न्यूमेरिक एवं विशेष कैरेक्टर का समावेश करें तथा पासवर्ड किसी से भी शेयर न करें। पासवर्ड 8 से 10 अंकों का मजबूत होता है।
- पासवर्ड के कुछ अक्षर छोटे तथा कुछ अक्षर बड़े होने चाहिए।
- प्रत्येक यूजर का अलग कम्प्यूटर होना चाहिए।
- यूजर्स को स्क्रीन लॉक विकल्प का सदैव प्रयोग करना चाहिए।
- लॉग ऑन लॉग ऑफ दिए गए मेनू से करना चाहिए।
- संवेदनशील आंकड़ों, जानकारियों को फाइल या हार्ड डिस्क ड्राइव को इनक्रिप्ट करने पर गंभीरता से विचार करना चाहिए।
- सुरक्षा हेतु सिस्टम पर सिक्योरिटी इनेबल लॉगिंग को इनेबल रखें।
- कार्य/दिन की समाप्ति पर कम्प्यूटर सिस्टम को शट डाउन करें।

3. ए.टी.एम. का सुरक्षित प्रयोग

व्यवहार जो अपेक्षित नहीं है :

- कभी भी अपना ए.टी.एम. कार्ड एवं पिन किसी को भी न दें, कभी भी अपना पिन पर्स या बटुए में न रखें, यदि बैंक के अधिकारी भी आपसे कार्ड नम्बर या पिन मांगे तो न दें।
- कार्ड या कार्ड के पीछे पिन नंबर न लिखें।

- किसी को भी अपना पासवर्ड/पिन न देखने दें।
- जन्मदिन या मोबाइल नंबर आदि को पासवर्ड या पिन के रूप में न बनायें, इससे आसानी से अनुमान लगाया जा सकता है।
- अपने कार्ड को सदैव अपने पास सुरक्षित रखें, कार्ड को कहीं भी कभी भी न छोड़ें।
- ए.टी.एम. पिन के सम्बन्ध में प्राप्त किसी ईमेल का जवाब न दें, इसे फिशिंग प्रयास कहा जाता है।
- टेलीफोन पर ए.टी.एम. कार्ड या पिन या ओ.टी.पी./सी.वी.वी आदि की जानकारी किसी को न दें।
- ए.टी.एम. का उपयोग करते समय किसी अनजान व्यक्ति या सुरक्षा गार्ड से सहायता स्वीकार न करें बल्कि तुरंत बैंक को फोन करें।

व्यवहार जो अपेक्षित है :

- जहाँ पर गार्ड की तैनाती हो उस ए.टी.एम. का प्रयोग सदैव सुरक्षित होता है।
- आप जिस ए.टी.एम. का इस्तेमाल हमेशा करते आ रहें हों, कोशिश करें कि उसी ए.टी.एम. का इस्तेमाल किया जाये, जो कि सुरक्षा के दृष्टिकोण से उचित होगा।
- अपने पिन (व्यक्तिगत पहचान संख्या) को याद रखें तथा अन्य सभी भौतिक प्रमाणों को नष्ट कर दें।
- ए.टी.एम. लेनदेन का एस.एम.एस. की सुविधा प्राप्त करने लिये बैंक में अपना वर्तमान/सही मोबाइल नंबर अवश्य पंजीकृत करावें ताकि हर लेन देन की सूचना मिल सके।
- खाते में यदि कोई अनाधिकृत कार्ड का लेन देन हो तो बैंक को तुरंत सूचित करें, यह आपके कार्ड से की जा रही धोखाधड़ी को रोकने में मदद करेगा।
- यदि आपको किसी ए.टी.एम. क्षेत्र में संदिग्ध व्यक्ति दिखाई दे तो ऐसे ए.टी.एम. से कोई लेन देन न करें।
- ए.टी.एम. में लेन देन के समय अनजान लोगों से अनावश्यक बातचीत न करें तथा संदिग्ध गतिविधियों से सावधान रहें।
- ए.टी.एम. में लेन देन शुरू करने के पश्चात् कोई संदेह या समस्या उत्पन्न होती है तो लेन देन को तुरंत निरस्त करने का बटन दबायें।
- पिन दर्ज करते समय पूर्ण सावधानी रखें ताकि कोई आपका पिन न देख सके।

- ए.टी.म. छोड़ने के पहले नगदी एवं कार्ड लेना न भूलें, यह सुनिश्चित करें की कार्ड से भुगतान करते समय कार्ड को आपके सामने स्वाइप किया जाये।
- यदि आपका ए.टी.एम. कार्ड गुम गया हो या चोरी हो गया हो तो उसे तुरंत ब्लॉक करा लें, इसके लिए आप टोल फ्री नंबर पर कॉल करें या फिर अपने बैंक की शाखा को सूचित करें।
- यदि आपके कार्ड की अवधि समाप्त हो गई हो तो उसे इस प्रकार नष्ट किया जाना चाहिए कि कार्ड की चुम्बकीय पट्टी नष्ट हो जाये।
- ए.टी.एम. से जुड़ी कोई डिवाइस या पट्टी आदि दिखाई दे तो तुरंत बैंक को सूचित करें।

4. खरीदारी के उपरांत यदि भुगतान कार्ड के माध्यम से किया जाये

व्यवहार जो अपेक्षित नहीं है :

- पॉइंट ऑफ सेल राशि इंटर करने हेतु दुकानदार से न कहे अपितु राशि इंटर करें
- पिन नंबर दुकानदार को न बताएँ।

व्यवहार जो अपेक्षित है :

- कार्ड से भुगतान करते समय कार्ड को आपके सामने स्वाइप किया जाये।
- मोबाइल नंबर बैंक खाते के साथ लिंक रखें एवं एस.एम.एस. के अलर्ट की सुविधा रखें ताकि लेन देन के तुरंत बाद आपके मोबाइल पर प्राप्त सन्देश से लेन देन की पुष्टि हो जाये।
- पिन दर्ज करते समय पूर्ण सावधानी रखें ताकि कोई आपना पिन न देख सके।
- यदि आपको अहसास हो की कोई अन्य व्यक्ति आपके पिन पर नजर रखे हुए है तो एक हाथ से पिन पैनल को कवर कर लें तथा दूसरे हाथ से पिन को प्रविष्ट करें संभव हो की थोड़ी झिझक हो पर सुरक्षा के दृष्टिकोण से यह आवश्यक है।

5. ई–व्यवसाय

ई-व्यवसाय इंटरनेट के माध्यम से किया जाता है, इसमें खरीद-बिक्री के अलावा और भी सेवाएँ विद्यमान रहती हैं, जैसे ए.टी.एम. कार्ड का

उपयोग आई.आर.सी.टी.सी. टिकट्स की बुकिंग, मोबाइल रिचार्ज, बिजली बिल का भुगतान, वस्तु एवं अन्य सेवाएँ ऑनलाइन कर सकते हैं।

व्यवहार जो अपेक्षित नहीं है :

- कार्ड नंबर एवं इसके पीछे अंकित सी.वी.वी. किसी भी व्यक्ति से शेयर न करें।
- किसी भी व्यक्ति द्वारा किए गए लुभावने कॉल या ईमेल संदेशों से बचें तथा अन्य व्यक्तिगत जानकारी साझा नहीं करें।
- किसी वेबसाइट की सुरक्षा की जांच किये बगैर इंटरनेट पर कोई संवेदनशील सूचना न दें।
- यदि ईमेल की वैद्यानिकता पर अविश्वास हो तो सीधे कंपनी से संपर्क कर पुष्टि करने का प्रयास करें।

व्यवहार जो अपेक्षित है :

- ई-वॉलेट या प्लास्टिक मनी का प्रयोग करें।
- अपने खाते का स्टेटमेंट नियमित रूप से जांच करें, बैंक खाता नंबर, कार्ड, पिन डिटेल को गोपनीय रखें।
- पासवर्ड को नियमित अंतराल में परिवर्तित करते रहें।
- अपने मोबाइल या कम्प्यूटर में एंटी वायरस और एंटी मालवेयर का प्रयोग करें।
- ऑनलाइन शॉपिंग पर फाइनल प्रिंट को सावधानी से पढ़ें।
- शॉपिंग पूर्व सुपुर्दगी, प्रभारो, ऑर्डर निरस्त करने के नियम एवं सामान लौटाने की नीतियों की समुचित जानकारी अवश्य प्राप्त करें।

6. मोबाइल बैंकिंग

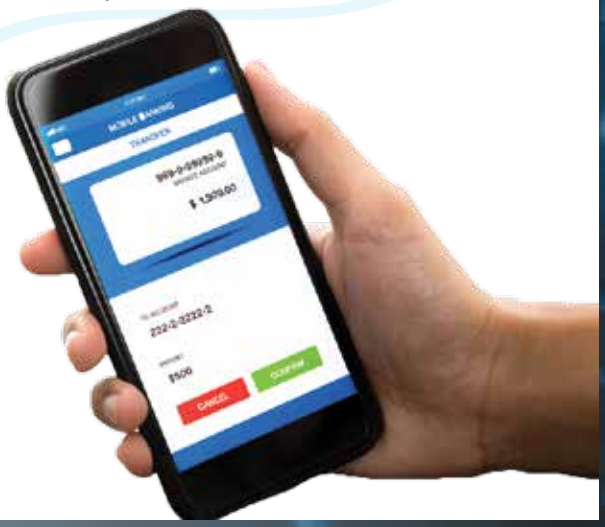
डिजिटल इंडिया अभियान से प्रभवित होकर आम आदमी ''नगद रहित अर्थव्यवस्था'' की ओर अग्रसर हुआ। ऐसे में मोबाइल बैंकिंग एक बेहतर और सुरक्षित विकल्प के तौर पर उभरा इसके जरिये बैंकिंग सुविधा ग्राहकों के जेब तक पहुँच गई। कोई भी सामान खरीदने से लेकर बड़े-बड़े भुगतान एवं फंड ट्रांसफर करने के लिए बैंक जाने की जरूरत नहीं पड़ी। मोबाइल बैंकिंग सुविधा 24 घंटे घर पर ही मौजूद रहती है।

व्यवहार जो अपेक्षित नहीं है :

- अपना यूजर आई.डी., बैंक खातों की जानकारी और पासवर्ड से संबंधित जानकारी अपने मोबाइल फोन में न रखें, किसी गलत हाथों में मोबाइल जाने से आपको नुकसान हो सकता है।
- अगर कहीं आपके मोबाइल में नेटवर्क नहीं मिल रहा हो तो लालच में फ्री वाई-फाई या हॉट स्पॉट से मोबाइल बैंकिंग का उपयोग नहीं करे ऐसा करते हैं तो डाटा चोरी की संभावना बनी रहती है।
- अपने बैंक अकाउंट या मोबाइल बैंकिंग से गुप्त व्यक्तिगत डाटा को मैसेज के जरिये भेजने की गलती न करें।
- साइबर चोर फोन पर बात करने के दौरान भी आपके फोन से डाटा ट्रांसफर कर सकते हैं इसलिए अनजान कॉल आने पर बातचीत में सावधानी बरतें।

व्यवहार जो अपेक्षित है :

- मोबाइल बैंकिंग से संबंधित एप का डाउनलोड सदैव बैंक के प्रामाणिक वेबसाइट अथवा गूगल प्ले स्टोर से करने का चुनाव सर्वथा श्रेष्ठ होता है।
- सुरक्षित मोबाइल बैंकिंग के इस्तेमाल के लिए स्क्रीन लॉक का प्रयोग करें।
- अपने पिन की जानकारी सदैव गोपनीय रखें।
- एंटी वायरस सॉफ्टवेयर का प्रयोग करें तथा उसे अपडेट रखें ताकि मालवेयर आदि वायरस से मोबाइल को सुरक्षित रखा जा सके।



- मोबाइल बैंकिंग से संबंधित कार्य उपरांत तुरंत लॉग आउट करें।
- यदि आप अपने मोबाइल फोन का उपयोग मोबाइल बैंकिंग के लिए करते हैं तो फोन को लॉक रखें तथा एप को भी पासवर्ड से सुरक्षित रखें।

नोट : साइबर अपराध घटित होने की स्थिति में निकटतम थाने में FIR करें तथा साथ हीं पीड़ित धारा 43A IT Act के प्रावधानों के अंतर्गत सक्षम पदाधिकारी (सचिव, सूचना प्रौद्योगिकी विभाग, झारखण्ड सरकार) के समक्ष क्षतिपूर्ति हेतु आवेदन दे सकते हैं।

❑❑❑

न्यायिक अकादमी झारखण्ड
धुर्वा डैम के समीप, धुर्वा, राँची-834004,
फोन : 0651-2902833, 2902831,
फैक्स : 0651-2902834, 2902831
ईमेल : judicialacademyjharkhand@yahoo.co.in,
वेबसाइट : www.jajharkhand.in

झारखण्ड राज्य विधिक सेवा प्राधिकार
न्याय सदन, ए.जी. ऑफिस के समीप, डोरण्डा, रांची
फोन : 0651-2481520
फैक्स : 0651-2482397
ईमेल : jhalsaranchi@gmail.com
वेबसाइट : www.jhalsa.org