राजस्थान राज्य विधिक सेवा प्राधिकरण

हर क्लिक में सतर्कता हर कदम पर सुरक्षा

साइबर सुरक्षा संकल्प

रियलिटी से वर्चुअल तक

एक लाइक और सब गायब

साइबर फ्रॉड के शिकार हुए हैं ?
जानिए कैसे वापस पाएं अपना पैसा

You lock your Computer screen

You know how to recognise phishing

You use strong passwords

You report suspicious situations

YOU ARE THE BEST DEFENCE AGAINST DIGITAL THREATS!

INSIDE

"The Booklet is published under the esteemed patronage and gracious blessings of our revered dignitaries"

Hon'ble Mr. Justice Surya Kant
The Chief Justice of India
Patron-in-Chief, NALSA

Hon'ble Mr. Justice Vikram Nath
Judge, Supreme Court of India
Executive Chairman, NALSA

Hon'ble Mr. Justice J.K. Maheshwari
Judge, Supreme Court of India
Chairman, SCLSC

Hon'ble Mr. Justice Sanjeev Prakash Sharma
The Acting Chief Justice, Rajasthan High Court
& Executive Chairman, RSLSA

Hon'ble Dr. Justice Pushpendra Singh Bhati
Judge, Rajasthan High Court
Chairman, RHCLSC, Jodhpur

Hon'ble Mr. Justice Inderjeet Singh
Judge, Rajasthan High Court
Chairman, RHCLSC, Jaipur

Justice Vikram Nath
Judge, Supreme Court of India
& Executive Chairman, NALSA

संदेश

डिजिटल युग में प्रौद्योगिकी ने हमारे दैनिक जीवन को अनेक रूपों में सहज और सुलभ बनाया है। इसके साथ ही, साइबर धोखाधड़ी, पहचान की चोरी, फ़िशिंग, वित्तीय अपराधों तथा ऑनलाइन दुरुपयोग जैसी चुनौतियाँ भी निरंतर सामने आ रही हैं। साइबर अपराधों की प्रकृति और विस्तार को समझना तथा उनसे बचाव के उपायों के प्रति सजग रहना वर्तमान समय की आवश्यकता है।

यह पुस्तिका साइबर अपराधों से संबंधित विषयों को सरल, सुव्यवस्थित और व्यावहारिक रूप में प्रस्तुत करती है। इसमें साइबर अपराधों के विभिन्न स्वरूपों, उनके कार्य करने के तरीकों तथा उनसे होने वाले संभावित दुष्प्रभावों का स्पष्ट विवरण दिया गया है। तथ्यात्मक जानकारी और उदाहरणों के माध्यम से यह प्रकाशन पाठकों को साइबर जोखिमों के प्रति जागरूक करने में सहायक सिद्ध होता है।

पुस्तिका का विशेष महत्व इस तथ्य में निहित है कि यह डिजिटल जागरूकता, सतर्कता और व्यक्तिगत उत्तरदायित्व पर बल देती है। यह सही रूप में इंगित करती है कि अनेक साइबर घटनाएँ सामान्य असावधानी के कारण घटित होती हैं और सजग तथा जिम्मेदार डिजिटल व्यवहार द्वारा इन्हें काफी हद तक रोका जा सकता है। व्यक्तिगत एवं वित्तीय जानकारी की सुरक्षा तथा संदिग्ध गतिविधियों के प्रति त्वरित प्रतिक्रिया संबंधी मार्गदर्शन उपयोगी एवं व्यवहारिक है।

इस प्रकाशन में साइबर अपराध से संबंधित विधिक प्रावधानों, उपलब्ध उपायों तथा संस्थागत प्रक्रियाओं का संक्षिप्त परिचय भी दिया गया है, जिससे नागरिकों को विधिक सहायता प्राप्त करने की दिशा में आवश्यक जानकारी मिलती है।

इस उपयोगी पहल के लिए मैं राजस्थान राज्य विधिक सेवा प्राधिकरण के प्रयासों की सराहना करता हूँ। मुझे विश्वास है कि यह पुस्तिका नागरिकों, विद्यार्थियों और विभिन्न वर्गों के पाठकों के लिए एक सहायक संदर्भ सामग्री सिद्ध होगी तथा साइबर सुरक्षा के प्रति जागरूकता बढ़ाने में सकारात्मक भूमिका निभाएगी।

Vikram Nath

Justice Sanjeev Prakash Sharma
The Acting Chief Justice
Rajasthan High Court
&
Executive Chairman, RSLSA

संदेश

डिजिटल क्रांति ने आधुनिक समाज को गहन रूप से परिवर्तित करते हुए सूचना, सेवाओं तथा अवसरों तक पहुँच का अभूतपूर्व विस्तार किया है। किन्तु इन सुविधाओं के साथ–साथ डिजिटल परिवेश में ऐसे साइबर अपराधों की चिंताजनक वृद्धि भी परिलक्षित हो रही है, जो आर्थिक सुरक्षा, व्यक्तिगत गोपनीयता तथा सामाजिक कल्याण को प्रभावित करते हैं। साइबर धोखाधड़ी, पहचान की चोरी, फ़िशिंग तथा ऑनलाइन शोषण जैसी गतिविधियाँ गंभीर चुनौतियों के रूप में उभरी हैं, जो जागरूकता तथा उत्तरदायी डिजिटल आचरण की अनिवार्यता को रेखांकित करती हैं।

यह पुस्तिका नागरिकों को साइबर अपराध की वास्तविकताओं से स्पष्ट, सुव्यवस्थित एवं सुगम रूप में परिचित कराने का एक समयोचित और सराहनीय प्रयास है। इसमें साइबर अपराधों के विभिन्न प्रकारों, अपराधियों द्वारा अपनाई जाने वाली सामान्य विधियों तथा व्यक्तियों को प्रभावित करने वाली डिजिटल धोखाधड़ी की बढ़ती घटनाओं का सरल एवं संतुलित विवेचन किया गया है। व्यावहारिक उदाहरणों और आवश्यक सावधानियों के माध्यम से यह प्रकाशन पाठकों को डिजिटल माध्यमों का सुरक्षित तथा विवेकपूर्ण उपयोग करने हेतु आवश्यक जानकारी प्रदान करता है।

इस पुस्तिका की एक महत्वपूर्ण विशेषता जागरूकता के माध्यम से रोकथाम पर दिया गया विशेष बल है। इसमें प्रतिपादित किया गया है कि तकनीकी सुरक्षा उपाय तब तक पर्याप्त सिद्ध नहीं हो सकते, जब तक उनके साथ उपयोगकर्ता का सतर्क और जागरूक व्यवहार न जुड़ा हो। व्यक्तिगत जानकारी की सुरक्षा, डिजिटल संचार का सत्यापन तथा संदिग्ध गतिविधियों पर त्वरित प्रतिक्रिया जैसी सरल किन्तु अत्यंत आवश्यक सावधानियों पर बल देकर यह पुस्तिका इस सिद्धांत को सुदृढ़ करती है कि साइबर सुरक्षा का प्रारंभ व्यक्तिगत जिम्मेदारी से होता है।

न्याय तक पहुँच के दृष्टिकोण से यह प्रकाशन एक महत्वपूर्ण जनोपयोगी कार्य भी करता है, क्योंकि यह पाठकों को साइबर अपराधों से संबंधित विधिक प्रावधानों, पीड़ितों को उपलब्ध उपायों तथा शिकायत एवं निवारण की संस्थागत व्यवस्थाओं से अवगत कराता है। ऐसी जानकारी नागरिकों को समय पर सहायता प्राप्त करने में सक्षम बनाती है तथा विधिक संस्थाओं के प्रति विश्वास को सुदृढ़ करती है।

राजस्थान राज्य विधिक सेवा प्राधिकरण के कार्यकारी अध्यक्ष के रूप में मेरा मत है कि विधिक जागरूकता प्रभावी न्याय–प्रणाली की आधारशिला है। यह पुस्तिका डिजिटल युग में जन–विधिक शिक्षा एवं नागरिक सशक्तिकरण के प्रति राजस्थान राज्य विधिक सेवा प्राधिकरण की सतत प्रतिबद्धता को प्रतिबिंबित करती है। मुझे विश्वास है कि यह सामान्य जन, विद्यार्थियों तथा अन्य हितधारकों के लिए एक उपयोगी संदर्भ सिद्ध होगी तथा एक सुरक्षित, जागरूक और उत्तरदायी डिजिटल समाज के निर्माण में सार्थक योगदान देगी।

Sanjeev Prakash Sharma

Shri Hari Om Attri
Member Secretary
Rajasthan State Legal Service Authority

संदेश

वर्तमान समय में डिजिटल प्रौद्योगिकी का व्यापक विस्तार जीवन के प्रत्येक क्षेत्र को प्रभावित कर रहा है। ऑनलाइन प्लेटफ़ॉर्म ने संचार, वित्तीय लेन–देन तथा सेवाओं तक पहुँच को सरल एवं त्वरित बनाया है, किन्तु इसके साथ नागरिकों के समक्ष विविध प्रकार के साइबर खतरों की आशंका भी बढ़ी है। ऑनलाइन धोखाधड़ी, डेटा के दुरुपयोग, पहचान की चोरी तथा डिजिटल छल–कपट की घटनाओं में निरंतर वृद्धि हो रही है, जिससे साइबर जागरूकता सुचित एवं जिम्मेदार नागरिकता का अनिवार्य अंग बन गई है।

यह पुस्तिका जनसामान्य को इन चुनौतियों के प्रति सजग करने हेतु एक व्यवहारिक एवं जानकारीपरक मार्गदर्शिका के रूप में तैयार की गई है। इसमें साइबर अपराध की प्रकृति, उसके विकसित होते स्वरूप तथा अपराधियों द्वारा डिजिटल कमजोरियों के दुरुपयोग की सामान्य विधियों का सरल एवं क्रमबद्ध विवरण प्रस्तुत है। तथ्यात्मक जानकारी और स्पष्ट व्याख्या के माध्यम से यह प्रकाशन पाठकों को डिजिटल माध्यमों से जुड़े जोखिमों को समझने तथा सुरक्षित ऑनलाइन आचरण अपनाने के लिए प्रेरित करता है।

इस पुस्तिका का प्रमुख उद्देश्य निवारक जागरूकता को प्रोत्साहित करना है। इसमें रेखांकित किया गया है कि सामान्य सावधानी, व्यक्तिगत एवं वित्तीय जानकारी के सतर्क उपयोग तथा ऑनलाइन संचार के समायोचित सत्यापन से अनेक साइबर घटनाओं से बचा जा सकता है। प्रस्तुत मार्गदर्शन नागरिकों को चेतावनी, संकेतों की पहचान करने, साइबर खतरों पर उचित प्रतिक्रिया देने तथा संभावित हानि से स्वयं को सुरक्षित रखने में सहायक होगा।

यह प्रकाशन माननीय न्यायाधिपति श्री संजीव प्रकाश शर्मा, कार्यवाहक मुख्य न्यायाधीश, राजस्थान उच्च न्यायालय एवं कार्यकारी अध्यक्ष, राजस्थान राज्य विधिक सेवा प्राधिकरण के मार्गदर्शन में तैयार किया गया है, जिनकी विधिक जागरूकता एवं नागरिक सशक्तिकरण की दृष्टि इस पहल में प्रेरक रही है।

उल्लेखनीय है कि इस पुस्तिका का प्रारंभिक रूप श्री पवन कुमार जीनवाल, सचिव, जिला विधिक सेवा प्राधिकरण, जयपुर द्वारा एक लघु जानकारीपरक साहित्य के रूप में जयपुर जिले के लिए आरंभ किया गया था। उनके इस सराहनीय प्रयास ने एक महत्त्वपूर्ण आधार प्रदान किया। विषय की व्यापक प्रासंगिकता एवं सामाजिक उपयोगिता को दृष्टिगत रखते हुए राजस्थान राज्य विधिक सेवा प्राधिकरण ने इसे अधिक महत्व का विषय मानते हुए संपूर्ण राजस्थान में प्रकाशन हेतु विकसित एवं विस्तारित करने का निर्णय लिया।

साइबर अपराध जैसे जटिल एवं तकनीकी विषय को सामान्य जन के लिए सरल, रोचक एवं बोधगम्य रूप में प्रस्तुत करना एक चुनौतीपूर्ण कार्य था। इस दिशा में सामग्री के परिष्कार एवं संरचनात्मक परिमार्जन में श्री हेमंत सिंह बघेला ने, संयुक्त सचिव, राजस्थान राज्य विधिक सेवा प्राधिकरण के रूप में, महत्वपूर्ण योगदान प्रदान किया, जिसके लिए मैं उनके प्रति हार्दिक कृतज्ञता व्यक्त करता हूँ।

अंततः इस पुस्तिका का अंतिम संयोजन एवं रूपांकन श्री पवन कुमार जीनवाल, सचिव, जिला विधिक सेवा प्राधिकरण जयपुर तथा सुश्री रश्मि नवल, उप सचिव, राजस्थान राज्य विधिक सेवा प्राधिकरण के संयुक्त प्रयासों से संपन्न हुआ, जिसके फलस्वरूप यह प्रकाशन अपने वर्तमान सुव्यवस्थित, सुसंगठित एवं प्रभावी स्वरूप में प्रस्तुत हो सका है।

राजस्थान राज्य विधिक सेवा प्राधिकरण के सदस्य सचिव के रूप में मैं इस प्रकाशन को विधिक साक्षरता के प्रसार तथा न्याय तक प्रभावी पहुँच सुनिश्चित करने के दायित्व का एक महत्त्वपूर्ण विस्तार मानता हूँ। मुझे विश्वास है कि यह पुस्तिका जनसामान्य के लिए एक उपयोगी संदर्भ सिद्ध होगी और एक अधिक सुरक्षित, जागरूक तथा डिजिटल रूप से उत्तरदायी समाज के निर्माण में सहायक बनेगी।

Hari Om Attri

रियलिटी से वर्चुअल तक

साइबर अपराध की दुनिया

वर्तमान डिजिटल युग में तकनीक का विकास तेजी से हो रहा है। इंटरनेट, मोबाइल और कंप्यूटर जैसी सुविधाओं ने जीवन को आसान बना दिया है, लेकिन इसके साथ ही साइबर अपराधों की संख्या भी बढ़ रही है। भारत में साइबर अपराधों के बढ़ते आंकड़े चिंता का विषय बन चुके हैं। इसका कारण यह है कि भारत के साइबर अपराध हॉट स्पॉट जामताड़ा और मेवात जैसे क्षेत्र अब राष्ट्रीय सीमाओं को पार कर चुके हैं।

केंद्रीय गृह मंत्रालय के प्रभाग भारतीय साइबर अपराध समन्वय केंद्र द्वारा किए गए विश्लेषण में यह पाया गया कि भारतीयों पर होने वाले साइबर अपराधों में लगभग 45 प्रतिशत साइबर अपराध दक्षिण एशियाई देशों, मुख्य रूप से म्यांमार, कंबोडिया और लाओस से संचालित हो रहे हैं। इसका यह अर्थ नहीं कि भारत में साइबर अपराध का खतरा नगण्य हो गया है। आंकड़ों के अनुसार, ट्रेडिंग स्कैम, फिशिंग और फर्जी रोमांस जैसी संदिग्ध गतिविधियों के खिलाफ दर्ज शिकायतों की संख्या 2019 में 26,049 से बढ़कर अप्रेल 2024 तक 7.4 लाख हो गई है।

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल पर वर्ष 2024 में छः लाख से अधिक शिकायतें दर्ज की गईं, जिसमें ठगी की कुल रकम लगभग 1,800 करोड़ रुपये आंकी गई है। आईआईटी कानपुर से जुड़े एक एनजीओ द्वारा किए गए अध्ययन के अनुसार 2020 से 2023 के बीच हुए 77 प्रतिशत साइबर अपराध वित्तीय धोखाधड़ी से संबंधित थे।

राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (NCRB) के अनुसार, वर्ष 2016 में साइबर अपराध के 12,317 मामले दर्ज हुए थे, जो वर्ष 2021 में बढ़कर 52,975 हो गए। वर्ष 2024 के पहले नौ महीनों में साइबर धोखाधड़ी से भारत को 11,333 करोड़ रुपये का नुकसान हुआ। खासतौर पर, स्टॉक ट्रेडिंग घोटालों से 4,636 करोड़ रुपये, निवेश घोटालों से 3,216 करोड़ रुपये और डिजिटल गिरफ्तारी धोखाधड़ी से 1,616 करोड़ रुपये का नुकसान हुआ है।

साइबर अपराध क्या होते हैं?

साइबर अपराध ऐसी गैरकानूनी गतिविधियों को कहते हैं, जो इंटरनेट, कंप्यूटर या मोबाइल के माध्यम से की जाती हैं। इन अपराधों का उद्देश्य व्यक्तिगत जानकारी चुराना, वित्तीय नुकसान पहुंचाना, या किसी व्यक्ति या संस्था को मानसिक और सामाजिक रूप से प्रभावित करना होता है।

साइबर अपराध के मुख्य प्रकार

1. हैकिंग– किसी व्यक्ति या संस्था के कंप्यूटर सिस्टम में बिना अनुमति प्रवेश करके डेटा चोरी या नुकसान पहुंचाना।
2. फिशिंग– नकली वेबसाइट या ईमेल के माध्यम से संवेदनशील जानकारी चुराना, जैसे बैंक खातों की डिटेल्स।
3. आइडेंटिटी थेफ्ट– किसी अन्य व्यक्ति की पहचान का दुरुपयोग करके वित्तीय या अन्य गैरकानूनी गतिविधिया करना।
4. मैलवेयर और रैनसमवेयर अटैक– हानिकारक सॉफ्टवेयर का उपयोग कर कंप्यूटर सिस्टम को नुकसान पहुंचाना या डेटा चोरी करना।
5. साइबर बुलिंग– इंटरनेट के माध्यम से किसी को धमकाना, मानसिक प्रताड़ना देना या उसे परेशान करना।
6. फर्जी वेबसाइट– नकली वेबसाइटों या ई–कॉमर्स प्लेटफॉर्म के जरिए लोगों को

क्या आप जानते है ?

भारतीय साइबर अपराध समन्वय केंद्र द्वारा किए गए विश्लेषण में यह पाया गया कि भारतीयों पर होने वाले साइबर अपराधों में लगभग 45 प्रतिशत साइबर अपराध दक्षिण एशियाई देशों, मुख्य रूप से म्यांमार, कंबोडिया और लाओस से संचालित हो रहे हैं।

धोखा देना और आर्थिक नुकसान पहुंचाना।

7. **रैंसमवेयर अटैक**– दुर्भावनापूर्ण सॉफ्टवेयर का उपयोग कर किसी व्यक्ति या संस्था के डेटा को लॉक कर देना और फिरौती की मांग करना।
8. **डार्क वेब गतिविधियां**– अवैध व्यापार और गैरकानूनी गतिविधियों के लिए डार्क वेब का उपयोग करना।

90 प्रतिशत साइबर हमले मानवीय लापरवाही के कारण होते हैं। इसलिए, आज के समय में साइबर सुरक्षा जागरूकता सभी के लिए बेहद महत्वपूर्ण है। तकनीक का उपयोग करते समय सतर्कता बरतना आवश्यक है ताकि साइबर खतरों से बचा जा सके। सुरक्षित डिजिटल भविष्य के लिए सतर्कता और जागरूकता अनिवार्य है। ■■

UNEXPECTED EMAIL?

Proceed with caution- it could be Malicious !

Never open email links or unexpected attachments. Check with security to verify the safety of suspect emails.

CYBER FRAUDS

सी.वी.वी./ ओ.टी.पी. शेयरिंग

व्हाट्सएप मैसेज, फोन या अन्य सोशल मीडिया के माध्यम से कभी भी किसी को ए.टी.एम. नंबर, सी.वी.वी. नंबर, ओ.टी.पी. इत्यादि गोपनीय जानकारी साझा न करें।

साइबर अपराधी बैंक व भारतीय रिजर्व बैंक अधिकारी बन कर लोगों को फोन करते हैं और उनसे कहते हैं कि उनका एटीएम कार्ड ब्लॉक हो गया है या उनका के.वाई.सी. अपडेट नहीं है या उनका आधार बैंक खाते से जुड़ा नहीं है और इसलिए उनका खाता ब्लॉक किया जाएगा। फिर आधार को बैंक खाते से जोड़ने, के.वाई.सी. अपडेट कराने, या नया ए.टी.एम. कार्ड शुरू करने के बहाने उनसे उनके खाते से जुड़े गोपनीय जानकारी जैसे ए.टी.एम. नंबर, सी.वी.वी. नंबर, ओ.टी.पी. इत्यादि जानकारी प्राप्त कर लेते हैं। जैसे ही ये जानकारी साईबर अपराधियों को मिलती है वे संबंधित व्यक्ति के खाते से पैसे निकाल लेते हैं।▪▪

ओ.एल.एक्स./ई-कॉमर्स प्लेटफार्म्स

एम.पिन. या यू.पी.आई. पिन की जरूरत सिर्फ पैसों के भुगतान के लिए होती है,न कि प्राप्ति के लिए।

साइबर अपराधी ई–कॉमर्स वेबसाइट जैसे–ओ.एल.एक्स., क्विकर, फेसबुक इत्यादि का प्रयोग वस्तुओं का आकर्षक मूल्य रख फर्जी विज्ञापन के माध्यम से साइबर ठगी करते हैं। जब भी कोई व्यक्ति इनकी खरीददारी हेतु उनसे संपर्क करता है तो वे पैकेजिंग चार्ज, रजिस्ट्रेशन चार्ज, ट्रांसपोटेशन चार्ज, टैक्स इत्यादि के बहाने अग्रिम राशि की मांग करते हैं। व्यक्ति इसे वास्तविक विज्ञापन समझ अग्रिम पैसों की भुगतान कर देते हैं। इस साइबर ठगी में वे मालिक को अग्रिम राशि का भुगतान करने हेतु केडिट लिंक/क्यूआर कोड भेजने के बजाय डेबिट लिंक/क्यूआर कोड भेजते हैं एवं इसे स्कैन या क्लिक करने के पश्चात् पीड़ित के खाते से पैसे की निकासी हो जाती है। ▪▪

यू.पी.आई. फिशिंग

कभी भी कस्टमर केयर अधिकारी का नंबर गूगल सर्च पर न प्राप्त करें। एयरलाइंस/ई–कॉमर्स कंपनी की आधिकारिक वेबसाइट का ही इस्तेमाल करें।

साइबर अपराधी बैंकिंग या अन्य ई–कॉमर्स की समस्या को सुलझाने के बहाने पीड़ित के बैंक के साथ पंजीकृत मोबाइल नंबर से अल्फान्यूमेरिक लिंक को किसी खास नंबर (अलग–अलग बैंक पर निर्भर) पर फॉरवर्ड करवा लेते हैं और एक बार लिंक फॉरवर्ड होने के पश्चात् सिम बाईंडिग को दरकिनार कर पीड़ित के खाते से संबंधित यू.पी.आई. वॉलेट अपने मोबाइल में इंस्टॉल कर लेते हैं। इस प्रकार पीड़ित के मोबाइल नंबर से जुड़े खातों तक पहुंच बना पैसे की अवैध निकासी कर लेते हैं। ▪▪

रिक्वेस्ट मनी क्यूआर कोड/लिंक से गुगल पे/फोनपे/पे.टी.एम. फर्जीवाड़ा

किसी भी अज्ञात श्रोत से प्राप्त किसी भी प्रकार के लिंक या क्यूआर कोड पर क्लिक/स्कैन न करें। पैसे की प्राप्ति करने हेतु कभी भी एम. पिन या यू.पी.आई. पिन दर्ज करने की आवश्यकता नहीं होती है।

साइबर अपराधी द्वारा व्यक्ति को पैसा प्राप्त करने हेतु लिंक क्लिक कर या क्यूआर कोड स्कैन कर पैसा अपने खाते में लेने की बात करते हैं परंतु जैसे ही व्यक्ति के द्वारा इसे स्कैन या क्लिक किया जाता है पैसा व्यक्ति के खाता से निकासी हो जाती है, क्योंकि यह पैसा प्राप्ति का क्यूआर कोड/लिंक होता है। ▪▪

कैटफिशिंग

अपने प्रोफाइल की प्राइवेसी सेंटिग्स के माध्यम से " My friends only" का चयन कर अनजान लोगों को अपने प्रोफाइल तक पहुंचने से रोकें।

साइबर अपराधी, एक धनी विदेशी व्यक्ति बनकर पीड़ित से सोशल मीडिया प्लेटफॉर्म यथा फेसबुक, इंस्टाग्राम व्हाट्सएप इत्यादि के माध्यम से दोस्ती करते हैं। वह सामान्यतः पारिवारिक समस्याएं, अकेलापन इत्यादि झूठी भावनात्मक कहानियां पीड़ित के साथ साझा करते हैं और पीड़ित उनकी झूठी भावनात्मक कहानियों को सच मान लेता है। काफी गहन मित्रता के पश्चात् वे मंहगे गिफ्ट भेजने की झूठी कहानियां गढ़ गिफ्ट के फोटो पीड़ित को भेजता है। उसके कुछ दिन पश्चात् वह कहता है कि संबंधित गिफ्ट एयरपोर्ट पर कस्टम अधिकारी द्वारा जप्त कर लिया गया है एवं गिफ्ट को छुड़ाने हेतु पैसों की मांग करता है। पीड़ित व्यक्ति उस फर्जी कस्टम अधिकारी जो कि उसी साइबर अपराधी गैंग का सदस्य होता है, को पैसे हस्तांतरित कर देता है। ▪▪

गुगल डॉक्स ऐप

किसी से जानकारी प्राप्त करने हेतु ऑनलाइन फॉर्म गूगल डॉक्स इत्यादि का व्यापक रूप से उपयोग किया जाता है। साइबर अपराधी द्वारा इन एप्लीकेशन का दुरूपयोग कर पीड़ित से बैंकिग लेन–देन से संबंधित गोपनीय जानकारी जैसेः ए.टी.एम. नंबर, यू.पी. आई. पिन, पासवर्ड इत्यादि दर्ज करवा लिय जाता है। जैसे ही पीड़ित फॉर्म में बैंक से संबंधित गोपनीय जानकारी भरता है, यह गोपनीय जानकारी साइबर जालसाज द्वारा प्राप्त कर ली जाती है और इसके माध्यम से पीड़ित के खाते से पैसों की अवैध निकासी कर ली जाती है। ■■

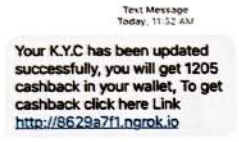
बैंक कभी भी ऑनलाइन फॉर्म भरने को नहीं कहता है। ऑनलाइन फॉर्म में बैंकिंग विवरणी कभी भी साझा न करें।

मोबाइल एप्लीकेशन

मोबाईल एप्लीकेशन निजी जानकारी चुराने, मोबाईल कंट्रोल को साइबर अपराधी तक पहुँचाने व अन्य साइबर अटैक कराने में महत्वपूर्ण भूमिका निभाते हैं। लोग सामान्यतः सुरक्षात्मक चेतावनी को अनदेखा करते हुए विभिन्न अज्ञात श्रोतों से मोबाईल एप्लीकेशन डाउनलोड करते हैं। ये एप्लीकेशन वायरस से संक्रमित हो सकते हैं एवं आपकी गोपनीय जानकारी अन्य बाहरी श्रोतों में ट्रांसफर कर सकते हैं जिसके माध्यम से कोई अन्य व्यक्ति आपके पासवर्ड, वित्तीय जानकारी आदि को नियंत्रित कर सकता है। मोबाईल एप्लीकेशन इंस्टाल करते समय अनावश्यक चीजों की अनुमति मांगी जाती है, और लोग बिना सोचे समझें अनुमति प्रदान कर देते हैं। जिसके पश्चात् उनकी निजी एवं अन्य गोपनीय जानकारी संबंधित एप्प तक पहुँच जाती है।

एप इंस्टाल करते समय उसके द्वारा माँगी गई अनुमति को स्वीकार करते समय सावधान रहें, जैसे सामान्य दस्तावेज स्कैन करने वाले एप को आपकी लोकेशन अथवा कॉल लॉग की आवश्यकता नहीं पड़ती।

फर्जी कैशबैक ऑफर्स



साइबर अपराधी पीड़ित को फोनपे/गूगल पे इत्यादि पर कैशबैक का झूठा लालच देते हैं एवं कैशबैक की प्राप्ति हेतु लिंक को क्लिक कर/क्यूआर कोड को स्कैन कर राशि को अपने खाते में जमा करने के लिए कहते हैं। जैसे ही पीड़ित लिंक को क्लिक करने के पश्चात् यू.पी.आई. या एम.पिन अंकित करता है उनके खाते में पैसा जमा होने के बजाए पैसे की उनके खाते से निकासी हो जाती है। ■■

सिम कार्ड स्वैपिंग

यह एक प्रकार से व्यक्ति की पहचान की चोरी (Identity theft) है जहां साइबर अपराधी टेलीकॉम सेवा प्रदाता के माध्यम से आपके पंजीकृत मोबाइल नंबर के लिए जारी किए गए पुराने सिम कार्ड के जगह नए सिम कार्ड को प्राप्त कर लेते हैं। नए सिम कार्ड की मदद से साइबर अपराधी पीड़ित के बैंक खाते से वित्तीय लेनदेन के लिए आवश्यक ओ.टी.पी. और अन्य गोपनीय जानकारी प्राप्त कर लेते हैं। ■■

फर्जी सोशल मीडिया अकाउंट

फेसबुक, मेसेंजर आदि से जब भी कोई पैसे की मांग करें तो इसकी जांच संबंधित व्यक्ति से मिलकर या निजी मोबाईल फोन पर कॉल करने के पश्चात् ही पैसों का हस्तांतरण करें।

साइबर अपराधी प्रचलित सोशल मीडिया जैसे फेसबुक/इंस्टाग्राम अकाउंट को लक्षित करते हैं। वे किसी अकाउंट से मिलता–जुलता फेक अकाउंट बना उनके दोस्तों या रिश्तेदारों से किसी मेडिकल इमरजेंसी इत्यादि का बहाना बनाकर पीड़ित के दोस्तों से पैसे की मांग करते है। पीड़ित का दोस्त उसे अपना वास्तविक दोस्त समझ कर पैसा ट्रांसफर कर देता है। जब तक पीड़ित को इसका एहसास होता है तब तक कई लोग पैसा ट्रांसफर कर फर्जीवाड़ा का शिकार बन चुके होते हैं। किसी व्यक्ति का फेसबुक अकाउंट हैक कर भी इसी तरह का साइबर अपराध किया जाता है। ■■

स्क्रीन शेयरिंग ऐप्स

बैंक/ई–कॉमर्स कंपनी कभी भी किसी तृतीय पक्ष का स्क्रीन शेयरिंग ऐप डाउनलोड करने के लिए नहीं कहता है।

साइबर अपराधी पीड़ित को बैंकिंग कार्यो में मदद करने या कंपनी की पॉलिसी का बहाना बना पीड़ित को मोबाइल में स्क्रीन शेयरिंग ऐपलिकेशन जैसे एनीडेस्क/क्विकसपोर्ट डाउनलोड व इंस्टॉल करवाकर पीड़ित के मोबाइल तक अपनी पहुंच बना पीड़ित के बैंक से संबंधित गोपनीय जानकारी जैसे सी.वी.वी नंबर, ओ.टी.पी. इत्यादि प्राप्त कर लेते हैं तथा उसके पश्चात् पीड़ित के खाते से पैसों की अवैध निकासी शुरू कर देते हैं। ■■

साइबर स्टॉकिंग

सोशल मीडिया प्लेटफार्म पर निजी जानकारी, फोटो, वीडियो इत्यादि साझा करते समय सावधान रहें। इन जानकारियों तक सिर्फ विश्वसनीय लोगों की ही पहुँच हो।

साइबर स्टॉकिंग ऑनलाईन स्टॉकिंग है, जिसके अंतर्गत इंटरनेट व अन्य इलेक्ट्रानिक साधन का प्रयोग कर किसी व्यक्ति या ग्रुप को लगातार प्रताड़ित या डराया जाता है, गलत आरोप लगाना, आपत्तिजनक टिप्पणियां करना व किसी की ऑनलाइन गतिविधि पर लगातार नजर बनाए रखना साइबर स्टॉकिंग की शैली में आता है। साइबर अपराधी ई–मेल, मैसेज, फोन कॉल इत्यादि के माध्यम से पीड़ित का पीछा करते है। साइबर स्टॉकिंग यौन उत्पीडन, अनुचित संपर्क या आपकी व आपके परिवार की गतिविधियों की ओर अवांछित ध्यान/आकर्षण इत्यादि के रूप में हो सकता है। ■■

ए.टी.एम./डेबिट कार्ड क्लोनिंग

प्रत्येक ए.टी.एम. व डेबिट कार्ड में एक मैगनेटिक स्ट्रीप होता है, जिसमें कार्ड से संबंधित महत्वपूर्ण गोपनीय जानकारी होती है। साइबर अपराधी द्वारा स्कीमिंग डिवाइस के माध्यम से इस गोपनीय जानकारी को कार्ड से संग्रह कर लिया जाता है तथा किसी खाली कार्ड पर कॉपी कर असली ए.टी.एम. कार्ड का क्लोन बना लिया जाता है। पीड़ित के द्वारा ए.टी.एम. पिन अंकित करते समय पिन होल, स्पाई कैमरा, ए.टी.एम. की–पैड के ऊपर ओवरले डिवाइस इत्यादि का प्रयोग कर साइबर अपराधी पीड़ित के ए.टी.एम. कार्ड का पिन प्राप्त कर खाते से अवैध निकासी करते हैं। ■■

ए.टी.एम. पिन हमेशा स्वंय अंकित करे एवं यह सुनिश्चित करें कि कोई इसे देख नहीं सके
ए.टी.एम. कार्ड इत्यादि से पैसे निकासी करते समय अपने अगल–बगल या पीछे किसी को खड़ा न होने दें।
ए.टी.एम. पिन को हमेशा बदलते रहें एवं ऐसा पिन न रखें जो आसानी से अनुमान लगाया जा सके।
यह सुनिश्चित कर लें कि बैंकिंग लेनदेन से संबंधित विवरणी मैसेज के माध्यम से भी प्राप्त हो।

एडिटेड गुगल कस्टमर केयर नंबर

साइबर अपराधी गूगल पेज पर बैंक/एयरलाइन इत्यादि के कस्टमर केयर नंबर को इस प्रकार से संपादित कर देते हैं कि जब भी कोई गूगल पर संबंधित बैंक/एयरलाइन इत्यादि के कस्टमर केयर नंबर को सर्च करें तो साइबर अपराधी द्वारा संपादित नंबर ही ऊपर में दिखे। पीड़ित वास्तविक कस्टमर केयर नंबर के स्थान पर साइबर अपराधी द्वारा संपादित नंबर पर कॉल कर देते है एवं उसके पश्चात् अपने निर्देशानुसार वह उनसे पैसे ठग लेते हैं। ■■

बैंक या एयरलाइन कस्टमर केयर का नंबर संबंधित बैंक या एयरलाइन के अधिकारिक वेबसाइट से ही प्राप्त करें न कि गूगल सर्च के माध्यम से। गूगल सर्च हमेशा सत्यापित जानकारी नहीं देता है।

रैन्समवेयर हमला

रैन्समवेयर एक प्रकार का हानिकारक सॉफ्टवेयर है, जिसको "चलाने" (RUN) पर कम्प्यूटर या डिवाइस की कार्यशैली बाधित हो जाती है एवं इसके पश्चात स्क्रीन पर एक मैसेज प्रकट होने लगता है, जिसके माध्यम से संबधित कम्प्यूटर या डिवाइस की कार्यशैली को वापस शुरू कराने हेतु पैसों का भुगतान करने के लिए कहा जाता है। अन्य शब्दों में यह एक प्रकार की ऑनलाइन फिरौती है। रैन्समवेयर मुख्यतः फिशिंग ई–मेल या अनजाने में किसी संक्रमित वेबसाईट के इस्तेमाल से फैलता है। ■■

लॉटरी /नाइजेरियन फर्जीवाड़ा

इस प्रकार के अपराध मे साइबर अपराधी ई–मेल या मैसेज भेज पीड़ित को यह सूचित करते है कि उसने लॉटरी या लाखों रुपये जीते है एवं पीड़ित को सिर्फ यह चयन करना होता है कि वह पैसों को कैसे लेना पंसद करेगा। पीड़ित व्यक्ति से सकारात्मक जवाब प्राप्त होने पर पैसे या लॉटरी प्राप्त करने हेतु वह उन्हे रजिस्ट्रेशन, शिपमेंट चार्ज, जी.एस.टी. इत्यादि बारी–बारी से माँगते हैं तथा पीड़ित लगातार पैसे साईबर ठग को देते चला जाता है, जब तक कि उसे इस ठगी का एहसास नहीं हो जाता। शुरूआत में इस तरह के साइबर अपराध नाईजीरिया से होते थे, अतः इसे नाइजेरियन फर्जीवाड़ा भी कहते है। ■■

ऑनलाइन नौकरी

हमेशा आधिकारिक रूप से पंजीकृत वेबसाईट पर ही अपना आवेदन समर्पित करे। नौकरी प्राप्त करने हेतु किसी भी प्रकार का अग्रिम भुगतान ना करें।

साइबर अपराधी फर्जी वेबसाइटों, समाचार पत्रों जैसे विभिन्न प्लेटफार्मों का उपयोग करके फर्जी नौकरी का विज्ञापन देते हैं। पीड़ित नौकरी की तलाश में इन फर्जी जॉब ऑफर्स को देखता है और साइबर अपराधी से संपर्क करता है। साइबर अपराधियों से संपर्क करने पर, पीड़ित को नौकरी पाने के लिए पंजीकरण शुल्क या अग्रिम भुगतान (जो वे वापसी योग्य होने का दावा करते हैं) करने के लिए कहा जाता है। पीड़ित पैसा हस्तांतरित करता है और नौकरी पाने के लिए जालसाज के दिशा–निर्देशों का पालन करता है और साइबर अपराध का शिकार हो जाता है। कुछ मामलों में, फर्जी वेबसाइट के माध्यम से नकली भुगतान चैनल का प्रयोग कर गोपनीय वित्तीय जानकारी प्राप्त की जाती है। ■■

सोशल मीडिया पर साईबर बुलिंग

डिजिटल तकनीक के माध्यम से सोशल मीडिया इत्यादि ऑनलाइन प्लेटफार्म पर धमकी देने को साइबर बूलिंग कहा जाता है। यह विभिन्न सोशल मीडिया प्लेटफार्म, गेमिंग प्लेटफार्म इत्यादि के माध्यम से किया जाता है। इसका उद्देश्य पीड़ित को डराना, धमकाना या बदनाम करना होता है, जैसे–किसी व्यक्ति के बारे में झुठी कहानी या रूपांतरित फोटो पोस्ट कर धमकी देना, किसी अन्य व्यक्ति की पहचान चोरी कर गलत मेसेज भेज उस व्यक्ति को बदनाम करना। ■■

किसी भी जानकारी या फोटो इत्यादि को ऑनलाइन अपलोड करते समय अत्यंत सावधानी बरतें तथा यह ध्यान रखें कि यह हमेशा के लिए ऑनलाइन प्लेटफार्म पर उपल्बध रहेगा और भविष्य में इसका दुरूपयोग किया जा सकता है।

ज्यूस जैकिंग

चार्ज करते समय अपने फोन का डेटा ट्रांसफर को ऑफ करके रखें। सार्वजनिक स्थानों पर चार्ज करने से पहले अपने डिवाइस को स्विच ऑफ कर दें।

ज्यूस जैकिंग एक तरह का साइबर फ्रॉड है जिसमें यू.एस.बी. चार्जिंग पोर्ट, जो पोर्ट वास्तव में डेटा कनेक्शन और चार्जिंग दोनों के लिए उपयोग किया जाता है, का उपयोग करके स्मार्ट फोन, टैबलेट या अन्य कंप्यूटर उपकरणों से डेटा कॉपी किया जाता है। पीड़ित यह सोचता है कि यह केवल चार्जिंग पोर्ट है। ■■

फर्जी सोशल मीडिया प्रोफाइल के जरिए उत्पीड़न

सोशल मीडिया साइटस में अपनी प्रोफाइल की ''प्राइवेसी सेटिंग्स'' में " My Friends Only " सेटिंग का चयन कर अनजान लोगों को अपने प्रोफाइल तक पहुँच से रोकें।

साइबर अपराधी सोशल मीडिया से पीड़ित का फोटो प्राप्त कर उसे रूपांतरित कर देते हैं तथा विभिन्न सोशल मीडिया प्लेटफॉर्म पर उसे अपलोड कर देते हैं। उसके पश्चात् वे रूपांतरित फोटो को विभिन्न सोशल मीडिया से हटाने हेतु पीड़ित से पैसों की मांग करते हैं। पीड़ित उनके जाल में फंसके पैसा हस्तांतरित कर देता है। ■■

कम्प्यूटर अथवा डिवाइस हैकिंग

हैकिंग किसी कम्प्यूटर/ डिवाईस तक अवैध तरीके से पहुँच बनाने की प्रक्रिया है। साइबर अपराधी विभिन्न तरीको जैसे–फिशिंग लिंक, मालवेयर इत्यादि के माध्यम से पीड़ित के कम्प्यूटर/ डिवाईस तक पहुँच बनाने के लिए हैकिंग का उपयोग करते है। हैकिंग के माध्यम से किसी व्यक्ति के कम्प्यूटर/ डिवाइस में उपस्थित महत्वपूर्ण दस्तावेज, फोटो इत्यादि चुराया जा सकता है या इनसे छेड़छाड़ किया जा सकता है। ■■

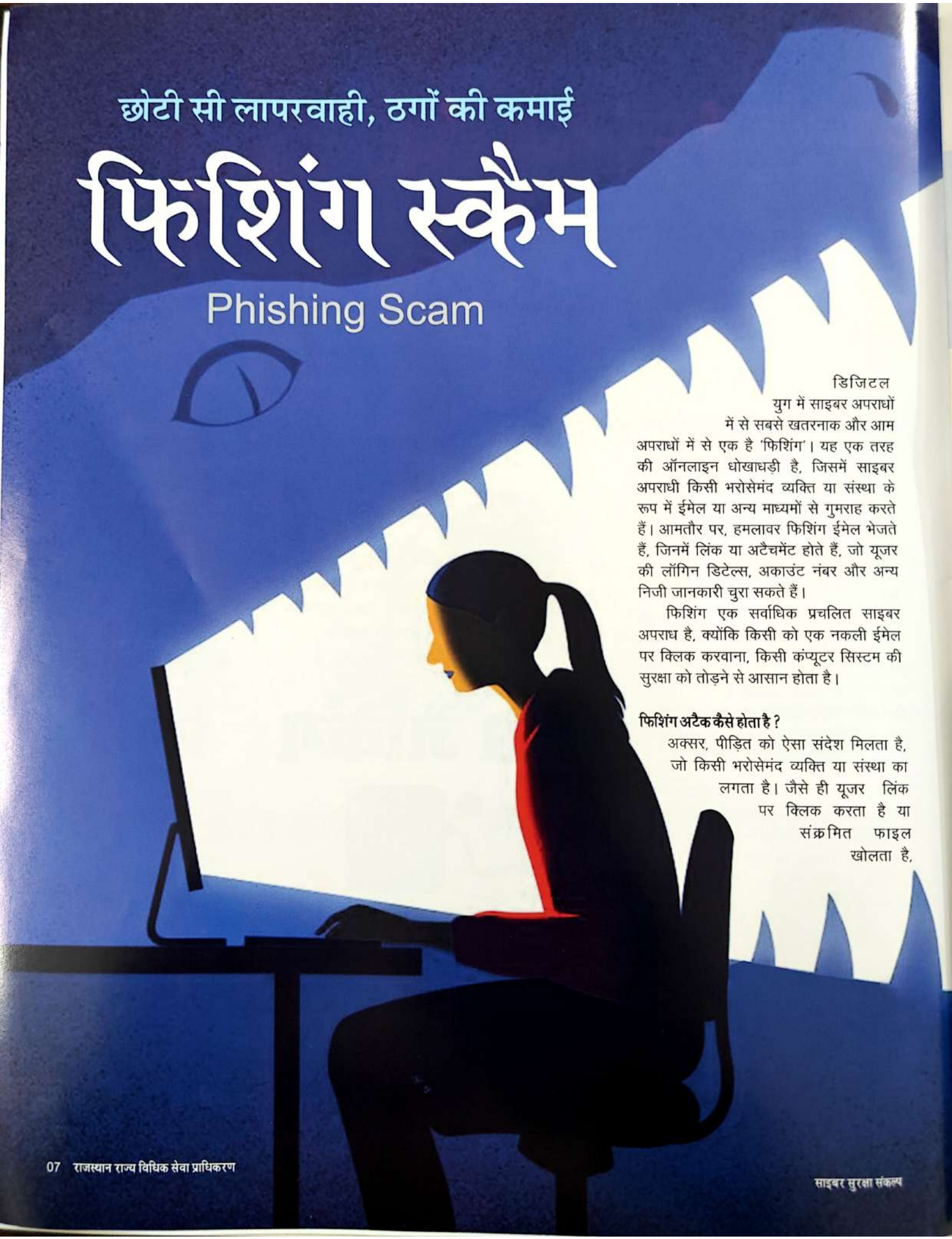
सेक्सटोर्शन

साइबर अपराधी द्वारा किसी महिला का फर्जी फेसबुक अकाउंट बनाकर पीड़ित के साथ वीडियो चैट कर उसपर अश्लील कार्य करने हेतु राजी कर लेता है। उसके पश्चात् इस वीडियो चैट का स्क्रिन शॉट रिकॉर्ड कर लेता है फिर पीड़ित को यह रिकॉड किया गया विडियो या स्क्रीन शॉट को विभिन्न सोशल मीडिया प्लैटफॉर्म पर वायरल करने की धमकी देकर पीड़ित से पैसे का माँग करता है ■■

छोटी सी लापरवाही, ठगों की कमाई

फिशिंग स्कैम

Phishing Scam



डिजिटल युग में साइबर अपराधों में से सबसे खतरनाक और आम अपराधों में से एक है 'फिशिंग'। यह एक तरह की ऑनलाइन धोखाधड़ी है, जिसमें साइबर अपराधी किसी भरोसेमंद व्यक्ति या संस्था के रूप में ईमेल या अन्य माध्यमों से गुमराह करते हैं। आमतौर पर, हमलावर फिशिंग ईमेल भेजते हैं, जिनमें लिंक या अटैचमेंट होते हैं, जो यूजर की लॉगिन डिटेल्स, अकाउंट नंबर और अन्य निजी जानकारी चुरा सकते हैं।

फिशिंग एक सर्वाधिक प्रचलित साइबर अपराध है, क्योंकि किसी को एक नकली ईमेल पर क्लिक करवाना, किसी कंप्यूटर सिस्टम की सुरक्षा को तोड़ने से आसान होता है।

फिशिंग अटैक कैसे होता है ?

अक्सर, पीड़ित को ऐसा संदेश मिलता है, जो किसी भरोसेमंद व्यक्ति या संस्था का लगता है। जैसे ही यूजर लिंक पर क्लिक करता है या संक्रमित फाइल खोलता है,

उसका सिस्टम हैक हो सकता है या उसे नकली वेबसाइट पर भेज दिया जाता है। इन नकली वेबसाइटों का उद्देश्य पीड़ित से उसकी निजी जानकारी, जैसे पासवर्ड, बैंक अकाउंट डिटेल या क्रेडिट कार्ड नंबर लेना होता है।

हालांकि, कई फिशिंग ईमेल गलत वाक्य रचना और वर्तनी की गलतियों के कारण नकली लगते हैं, लेकिन अब साइबर अपराधी आर्टिफिशियल इंटेलिजेंस AI और चैटबॉट्स का उपयोग कर असली दिखने वाले फिशिंग हमले कर रहे हैं।

कुछ फिशिंग हमले फोन कॉल के जरिए भी किए जाते हैं, जहां हमलावर खुद को किसी अधिकारी या कंपनी कर्मचारी के रूप में पेश कर पीड़ित से उसकी निजी जानकारी निकलवाने की कोशिश करता है। अब AI की मदद से हमलावर किसी मैनेजर या अन्य उच्च पदस्थ अधिकारी की आवाज की नकल कर सकते हैं, जिससे धोखाधड़ी की संभावना और बढ़ जाती है।

फिशिंग ईमेल को कैसे पहचाने ?

फिशिंग ईमेल असली ईमेल की तरह दिखते हैं और इनमें कंपनियों के लोगो और अन्य पहचान चिन्ह हो सकते हैं। हालांकि, कुछ संकेत होते हैं जिनसे फिशिंग ईमेल को पहचान सकते हैं–

- ईमेल में अजीब URL या गलत स्पेलिंग वाले लिंक होते हैं।
- प्रेषक का ईमेल पता किसी सार्वजनिक सेवा जैसे Gmail, Yahoo से होता है, न कि किसी कंपनी के आधिकारिक डोमेन से।
- संदेश में डराने या जल्दी कोई कार्रवाई करने का दबाव डाला जाता है।
- ईमेल में पासवर्ड या बैंक डिटेल जैसी व्यक्तिगत जानकारी मांगी जाती है।
- ईमेल में व्याकरण और लेखन संबंधी गलतियां हो सकती हैं।

फिशिंग के प्रकार

साइबर अपराधी समय के साथ नए और अधिक खतरनाक फिशिंग अटैक के तरीके अपनाते जा रहे हैं।

स्पीयर फिशिंग (Spear Phishing) – यह किसी विशेष व्यक्ति या कंपनी को निशाना बनाने वाला फिशिंग हमला होता है। इसमें हमलावर पीड़ित की निजी जानकारी इकट्ठा करके उसे असली दिखने वाले ईमेल भेजता है।

व्हेलिंग (Whaling Attack) – यह स्पीयर फिशिंग का एक विशेष प्रकार है, जिसमें बड़े अधिकारियों को निशाना बनाया जाता है। अपराधी ऐसा ईमेल भेजते हैं, जो किसी कंपनी के सीईओ या मैनेजर के नाम से भेजा गया लगता है और जिसमें बड़ी धनराशि के भुगतान की मांग होती है।

फार्मिंग (Pharming) – इसमें असली वेबसाइट का नकली संस्करण तैयार किया जाता है और यूजर को वहां लॉगिन करने के लिए प्रेरित किया जाता है। जब यूजर अपनी जानकारी डालता है, तो वह हमलावर तक पहुंच जाती है।

क्लोन फिशिंग (Clone Phishing) – इसमें असली ईमेल का एक क्लोन बनाया जाता है और उसमें छेड़छाड़ करके हानिकारक लिंक जोड़े जाते हैं। चूंकि यह ईमेल पहले के असली मेल की तरह दिखता है, इसलिए यूजर आसानी से इसमें क्लिक कर सकता है।

ईविल ट्विन अटैक (Evil Twin Attack) – इसमें हैकर एक नकली Wi-Fi नेटवर्क बनाते हैं, जो असली नेटवर्क की तरह दिखता है। जब यूजर इसमें कनेक्ट होता है, तो उसका सारा डेटा चोरी हो सकता है।

वॉयस फिशिंग (Phishing)–यह फोन कॉल के जरिए किया जाने वाला फिशिंग हमला होता है, जिसमें हमलावर खुद को बैंक अधिकारी या अन्य भरोसेमंद व्यक्ति बताकर जानकारी हासिल करने की कोशिश करता है।

एसएमएस फिशिंग (Phishing) – यह मोबाइल मैसेजिंग के जरिए किया जाता है, जिसमें हमलावर फर्जी लिंक भेजते हैं और यूजर से संवेदनशील जानकारी मांगते हैं।

कैलेंडर फिशिंग (Calendar Phishing) – इसमें नकली कैलेंडर इनवाइट भेजे जाते हैं, जिनमें हानिकारक लिंक होते हैं।

पेज हाईजैकिंग (Page Hijacking) – इसमें किसी असली वेबसाइट को हैक करके यूजर को नकली पेज पर रीडायरेक्ट किया जाता है, जहां से उसकी जानकारी चोरी की जाती है।

वर्ष 2023 में, कैलिफोर्निया स्थित क्लाउड सुरक्षा कंपनी Zscaler द्वारा किए गए अध्ययन के अनुसार भारत में 79 मिलियन से अधिक फिशिंग हमले दर्ज किए गए। फिशिंग धोखाधड़ी के शिकार होने वाले देशों में संयुक्त राज्य अमेरिका पहले स्थान पर है, उसके बाद यूनाइटेड किंगडम और तीसरे स्थान पर भारत है।

बचाव ही उपाय

एंटीवायरस सॉफ्टवेयर– यह मालवेयर और वायरस को पहचानकर उन्हें रोक सकता है।

डेस्कटॉप और नेटवर्क फायरवॉल– यह अनधिकृत एक्सेस को रोकने में मदद करता है।

एंटी–स्पाइवेयर सॉफ्टवेयर– यह जासूसी सॉफ्टवेयर को पहचानकर सिस्टम से हटा सकता है।

वेब ब्राउजर में एंटी–फिशिंग टूलबार– यह खतरनाक वेबसाइटों को ब्लॉक करता है।

गेटवे ईमेल फिल्टर– यह संदेहास्पद ईमेल को पहचानने में मदद करता है।

वेब सुरक्षा गेटवे– यह ऑनलाइन गतिविधियों की निगरानी करता है।

स्पैम फिल्टर– यह अवांछित ईमेल को रोकता है।

फिशिंग फिल्टर– माइक्रोसॉफ्ट और अन्य कंपनियों द्वारा दिए गए सुरक्षा टूल फिशिंग को रोकने में मदद कर सकते हैं।

इसके अलावा, ईमेल ऑथेंटिकेशन तकनीक का उपयोग करना जरूरी है ताकि आने वाले ईमेल की वैधता की पुष्टि की जा सके।

फिशिंग से बचने के उपाय

1. **संदिग्ध लिंक से बचें**– किसी भी ईमेल, संदेश या वेबसाइट में आने वाले लिंक पर क्लिक करने से पहले सावधान रहें। सुनिश्चित करें कि वह लिंक आधिकारिक वेबसाइट से मेल खाता हो। नकली वेबसाइटों का URL अक्सर थोड़ा भिन्न होता है, जिससे वह असली वेबसाइट से अलग नजर आता है।
2. **ईमेल और संदेशों को सही से जांचें**–किसी भी संदिग्ध ईमेल या संदेश में दिए गए सुझावों का पालन न करें। अक्सर, धोखेबाज आधिकारिक संस्थाओं की तरह ईमेल भेजते हैं, लेकिन इनमें कुछ गलतियां होती हैं, जैसे कि नाम का गलत लिखना या संदिग्ध लिंक।
3. **पब्लिक Wi-Fi से बचें**– पब्लिक Wi-Fi नेटवर्क का उपयोग करते समय व्यक्तिगत जानकारी साझा करने से बचें। इन नेटवर्कों पर आपके डेटा को हैक किया जा सकता है। हमेशा सुरक्षित नेटवर्क का ही उपयोग करें।
4. **एंटीवायरस और सिक्योरिटी सॉफ्टवेयर का इस्तेमाल करें**– अपने कंप्यूटर और स्मार्टफोन में एंटीवायरस सॉफ्टवेयर और सिक्योरिटी अपडेट को हमेशा सक्रिय रखें। इससे वायरस और अन्य प्रकार के मालवेयर से सुरक्षा मिलती है।
5. **बैक्टी से बचें**– किसी भी बैंक से संबंधित संवेदनशील जानकारी जैसे पासवर्ड या OTP को साझा करने से पहले सुनिश्चित करें कि वह कॉल या संदेश असली है। बैंक आमतौर पर ईमेल या कॉल के माध्यम से संवेदनशील जानकारी की मांग नहीं करते।
6. **2–फैक्टर ऑथेंटिकेशन का इस्तेमाल करें**– अपने ऑनलाइन खातों में सुरक्षा बढ़ाने के लिए 2–फैक्टर ऑथेंटिकेशन का उपयोग करें। इससे आपका खाता अधिक सुरक्षित रहेगा, क्योंकि इसमें पासवर्ड के साथ–साथ एक अतिरिक्त सुरक्षा कदम शामिल होता है।

फिशिंग एक खतरनाक साइबर धोखाधड़ी है। सही सावधानियों और जागरूकता के माध्यम से इस प्रकार की धोखाधड़ी से बचा जा सकता है। साइबर धोखाधड़ी से बचने के लिए हमेशा सतर्क रहें और इंटरनेट पर व्यक्तिगत जानकारी साझा करते समय अत्यधिक सावधानी बरतें।

फिशिंग तकनीकें

फिशिंग हमले सिर्फ ईमेल भेजकर किसी व्यक्ति के उस पर क्लिक करने की उम्मीद करने तक सीमित नहीं होते। अपराधी कई अलग–अलग तकनीकों का इस्तेमाल करके लोगों को फंसाने की कोशिश करते हैं।

URL स्पूफिंग– इसमें हमलावर जावास्क्रिप्ट (JavaScript) का उपयोग करके ब्राउजर के एड्रेस बार में असली वेबसाइट की नकली तस्वीर डालते हैं। जब यूजर लिंक पर माउस ले जाता है, तो सही URL दिख सकता है, लेकिन जावास्क्रिप्ट का उपयोग करके इसे बदला भी जा सकता है।

लिंक मैनिपुलेशन – इसे URL छिपाने की तकनीक भी कहा जाता है। इसमें हमलावर नकली लिंक बनाते हैं, जो देखने में किसी असली वेबसाइट का पता लगता है, लेकिन असल में यह किसी खतरनाक वेबसाइट की ओर ले जाता है।

लिंक शॉर्टनिंग– इसमें हमलावर Bitly जैसी लिंक–शॉर्टनिंग सेवाओं का उपयोग करके लिंक की असली मंजिल छिपा देते हैं। इस तरह यूजर को यह पता नहीं चल पाता कि लिंक किसी असली वेबसाइट पर जा रहा है या फिर किसी धोखाधड़ी वाले पेज पर।

होमोग्राफ स्पूफिंग– इस तकनीक में हमलावर असली वेबसाइट जैसा दिखने वाला URL बनाते हैं, लेकिन उसमें थोड़ा सा बदलाव कर देते हैं। जैसे, "bank.com" की जगह "bank-com" लिखा जा सकता है, जो देखने में असली वेबसाइट जैसा ही लगेगा।

ग्राफिकल रेंडरिंग– कुछ सुरक्षा सॉफ्टवेयर ईमेल में लिखे गए शब्दों को स्कैन कर फिशिंग हमलों का पता लगाते हैं। लेकिन अगर हमलावर ईमेल का पूरा या कुछ हिस्सा एक इमेज के रूप में भेजते हैं, तो यह सुरक्षा जांच को पार कर सकता है।

गुप्त रीडायरेक्ट (Covert Redirect)– इसमें यूजर को किसी भरोसेमंद वेबसाइट पर जाने के लिए कहा जाता है, लेकिन असल में उसे पहले एक नकली वेबसाइट पर ले जाया जाता है, जहां उसकी लॉगिन जानकारी मांगी जाती है। उसके बाद ही यूजर को असली वेबसाइट पर भेजा जाता है।

चैटबॉट का उपयोग –अब हमलावर AI आधारित चैटबॉट्स का उपयोग करके फिशिंग ईमेल को और अधिक वास्तविक दिखाने लगे हैं। इससे वर्तनी और व्याकरण की गलतियां कम होती हैं और ईमेल असली लगने लगता है।

AI वॉयस जनरेटर– हमलावर किसी व्यक्ति की आवाज की नकल करने के लिए AI टूल्स का उपयोग कर सकते हैं। वे किसी मैनेजर या परिवार के सदस्य की आवाज निकालकर फोन पर बात करते हैं, जिससे पीड़ित को लगता है कि असली व्यक्ति ही बात कर रहा है।

BE A SUSPICIOUS OF EVERYTHING

Cyber criminals make the internet A dangerous place. Be street-smart. Keep a critical eye out and avoid Unsafe activities.

एक लाइक और सब गायब

सोशल मीडिया साइबर ठगी

यदि सोशल मीडिया प्रोफाइल पर शेयर की गई नीजी तस्वीरें, स्थान की जानकारी और व्यक्तिगत विचार तक किसी अजनबी को अनचाहा एक्सेस मिल जाता है, तो यह गोपनीय जानकारी चुराने, बदनाम करने या यहां तक कि शारीरिक/आर्थिक नुकसान पहुंचाने का कारण बन सकता है।

आज के समय में सोशल मीडिया हमारी जिंदगी का अहम हिस्सा बन गया है। यह संचार, जानकारी साझा करने और जीवन की घटनाओं को दूसरों तक पहुचाने का एक नया माध्यम बन चुका है। हम अपने दिन–प्रतिदिन के अनुभव, पारिवारिक तस्वीरें, लोकेशन अपडेट और विचार सोशल मीडिया पर साझा करते हैं।

हालांकि, यह सुविधा कभी–कभी खतरा भी बन सकती है। यदि कोई अनजान व्यक्ति हमारे सोशल मीडिया प्रोफाइल तक पहुंच जाता है, तो वह हमारी निजी जानकारी का गलत इस्तेमाल कर सकता है। इससे जानकारी की चोरी, बदनामी, पहचान की चोरी या कभी–कभी शारीरिक/यौन शोषण और लूटपाट जैसी घटनाए भी हो सकती हैं। इसलिए, सोशल मीडिया का सुरक्षित और सही तरीके से उपयोग करना बहुत जरूरी है।

सोशल मीडिया धोखाधड़ी के प्रकार

1. सहानुभूति धोखाधड़ी (Sympathy Fraud)–

धोखेबाज सोशल मीडिया पर दोस्ती करता है और लगातार बातचीत कर भरोसा जीतता है। बाद में, वह पैसे ऐंठने या अन्य नुकसान पहुचाने का प्रयास करता है।

सावधानियां

- अपनी फ्रेड लिस्ट हाइड रखें। किसी अनजान व्यक्ति की फ्रेंड रिक्वेस्ट स्वीकार करने से बचें।
- सोशल मीडिया पर व्यक्तिगत जानकारी साझा न करें। अपनी पोस्ट को केवल फ्रेड्स के देखने तक ही सीमित रखें।
- बिना पुष्टि किए किसी को पैसे न भेजें।

2. रोमांस धोखाधड़ी (Romance Fraud)–

धोखेबाज पहले दोस्ती करता है और फिर धीरे–धीरे प्यार और भावनात्मक लगाव बढ़ाता है। बाद में वह भावनात्मक, आर्थिक या शारीरिक रूप से शोषण करता है।

सावधानियां

- अनजान लोगों से दोस्ती करने से बचें।
- निजी तस्वीरें और वीडियो ऑनलाइन साझा न करें।
- ब्लैकमेलिंग होने पर तुरंत पुलिस को सूचित करें।

3. साइबर स्टॉकिंग (Cyber Stalking)–

यह अपराध तब होता है जब कोई व्यक्ति इंटरनेट के माध्यम से किसी को डराने या परेशान करने के लिए ईमेल, मैसेज या सोशल मीडिया का इस्तेमाल करता है। स्टॉकर गुमनाम रहकर धमकी भरे संदेश भेजता है और पीड़ित की गतिविधियों पर नजर रखता है।

सावधानियां

- अपनी सोशल मीडिया प्रोफाइल को निजी (Private) रखें।
- अपनी लोकेशन या यात्रा की जानकारी सार्वजनिक न करें।
- यदि कोई लगातार पीछा कर रहा है, तो तुरंत पुलिस में शिकायत दर्ज कराएं।

4. साइबर बुलिंग (Cyber Bullying)–

यह ऑनलाइन ठगी सोशल मीडिया, मैसेज, फोरम या गेमिंग ऐप्स के जरिए होती है।

इसमें किसी व्यक्ति को बदनाम करने या अपमानित करने के लिए झूठी और आपत्तिजनक बातें फैलाई जाती हैं।

सावधान रहें! अगर आपके बच्चे के व्यवहार में बदलाव दिखे

- वह अचानक आक्रामक हो जाए या दोस्तों/परिवार से बात करना बंद कर दे।
- डिजिटल डिवाइस का उपयोग करना बंद कर दे या डर महसूस करे।
- साइबर बुलिंग अपराध है, यह बच्चों को समझाए।
- सुरक्षित इंटरनेट इस्तेमाल पर परिवार और दोस्तों से चर्चा करें।
- अपने बच्चों की ऑनलाइन गतिविधियों पर नजर रखें और पैरेंटल कंट्रोल चालू करें।
- यदि किसी मित्र को साइबर बुलिंग का शिकार होते देखें, तो तुरंत माता–पिता या शिक्षकों को सूचित करें।
- आपत्तिजनक मैसेज डिलीट न करें, क्योंकि यह पुलिस अनुसंधान में मदद कर सकते हैं।

■■

साइबर अपराध की रिपोर्ट कैसे और कहाँ करें?

- **स्पष्ट स्क्रीन शॉट लें, सबूत सुरक्षित रखें।**
- **घटना का संक्षिप्त विवरण लिखें।**
- **नजदीकी पुलिस स्टेशन या साइबर सेल में जाएं।**
- **ऑनलाइन शिकायत दर्ज करने के लिए राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल पर जाएं।**
- **हेल्पलाइन नंबर 1930 पर कॉल करें।**

कहीं कोई आपके साथ न कर दे

OTP धोखाधडी

आजकल एक ही क्लिक में खाना ऑर्डर करना, चाय पीते हुए बिल भरना, या अमेजन से अपनी पसंदीदा ड्रेस खरीदना बहुत आसान हो गया है। ऑनलाइन लेन–देन ने हमारी जिंदगी को पहले से ज्यादा सुविधाजनक बना दिया है।

लेकिन इस सुविधा के साथ खतरे भी जुड़े हुए हैं। ओटीपी (वन टाइम पासवर्ड) ऑनलाइन सुरक्षा की एक महत्वपूर्ण परत है, लेकिन ठगों ने इसे धोखाधड़ी के लिए इस्तेमाल करने के नए तरीके ढूंढ लिए हैं।

ओटीपी धोखाधड़ी क्या है ?

ओटीपी एक विशेष कोड होता है, जो हमारे मोबाइल नंबर या ईमेल पर भेजा जाता है ताकि किसी भी ऑनलाइन लेन–देन को सत्यापित किया जा सके। यह कोड ऑनलाइन लेन–देन को सुरक्षित बनाने के लिए इस्तेमाल किया जाता है। लेकिन ठग इस सुरक्षा प्रणाली का गलत फायदा उठाते हैं और लोगों को ओटीपी बताने के लिए धोखा देते हैं और ओटीपी प्राप्त कर लोगों के बैंक खाते से पैसे निकाल लेते हैं।

कैसे होती है ओटीपी धोखाधड़ी ?

- साइबर अपराधी किसी व्यक्ति की व्यक्तिगत जानकारी जैसे बैंकिंग डिटेल्स या मोबाइल नंबर प्राप्त कर लेते हैं।
- वे बैंक, ई–कॉमर्स साइट, कूरियर कंपनी या किसी अन्य सेवा प्रदाता का कर्मचारी बनकर फोन करते हैं।
- वे बहुत विश्वसनीय तरीके से बात करके ओटीपी मांगते हैं।
- जैसे ही वे ओटीपी प्राप्त कर लेते हैं, वे बैंक खाते से पैसे निकाल लेते हैं या अन्य धोखाधड़ी वाले लेन–देन कर लेते हैं।

कैसे करते हैं धोखेबाज धोखाधड़ी ?

1. नकली बैंक कॉल–

ठग बैंक अधिकारी बनकर फोन करते हैं और खाते में संदिग्ध गतिविधि बताकर डराते हैं कि यदि आपने ओटीपी साझा नहीं किया, तो आपका पैसा सुरक्षित नहीं रहेगा।

2. फर्जी इनाम का झांसा–

कॉल या मैसेज करके इनाम, लॉटरी, या विशेष ऑफर जीतने के लिए बताकर इनाम पाने के लिए वे ओटीपी मांगते हैं।

3. गलती से भेजा गया ओटीपी

ठग कॉल करके कहते हैं कि उन्होंने गलती से आपके नंबर पर ओटीपी भेज दिया है। वे अनुरोध करते हैं कि आप वह ओटीपी उन्हें बता दें।

4. फ्री लोन या क्रेडिट कार्ड लिमिट बढ़ाने का लालच

ठग बिना ब्याज के लोन या टैक्स रिफंड मिलने के लिए ओटीपी साझा करने को कहते है।

5. कॉल मर्जिंग

एक ठग कॉल कर किसी जानकार का नाम लेकर कॉल मर्ज करने के लिए कहते हैं जैसे ही कॉल मर्ज होता है उसी समय बैंक का ओटीपी कॉल आता है और ठग इसे सुनकर खाते से पैसे निकाल लेता है।

6. बिजली या अन्य बिल भुगतान के नाम पर ठगी

फर्जी संदेश भेजकर कहा जाता है कि यदि आप तुरंत बिल जमा नहीं करेंगे तो बिजली कनेक्शन काट दिया जाएगा। घबराकर लोग दिए गए नंबर पर कॉल करते हैं और ठग उन्हें ओटीपी साझा करने के लिए मजबूर कर देते हैं।

7. ऑनलाइन नौकरी का झांसा

ठग ऑनलाइन नौकरी के नाम पर पहले जॉइनिंग शुल्क या अन्य प्रक्रिया के लिए ओटीपी वेरिफिकेशन मांगते हैं। जैसे ही आप ओटीपी साझा करते हैं, आपके खाते से पैसे निकल जाते हैं।

8. कॉल मर्जिंग (Call merging)

इसमें ठग किसी व्यक्ति को कॉल करके किसी अन्य व्यक्ति या बैंक के अधिकारी की नकली कॉल को मर्ज करवा देता है। इससे ऐसा प्रतीत होता है कि दोनों एक ही कॉल पर हैं, लेकिन यह एक धोखाधड़ी का तरीका होता है।

8. कॉल फॉरवर्डिंग (Call Forwarding)

किसी नंबर पर आने वाली कॉल को किसी अन्य नंबर पर डायवर्ट कर देना। ठग इस तकनीक का उपयोग OTP फ्रॉड में करते हैं ताकि बैंक या अन्य सेवाओं से आने वाले कॉल सीधे उनके पास पहुंचें, न कि असली ग्राहक के पास।

कैसे पहचानें कि यह धोखाधड़ी है ?

खुद से पूछें

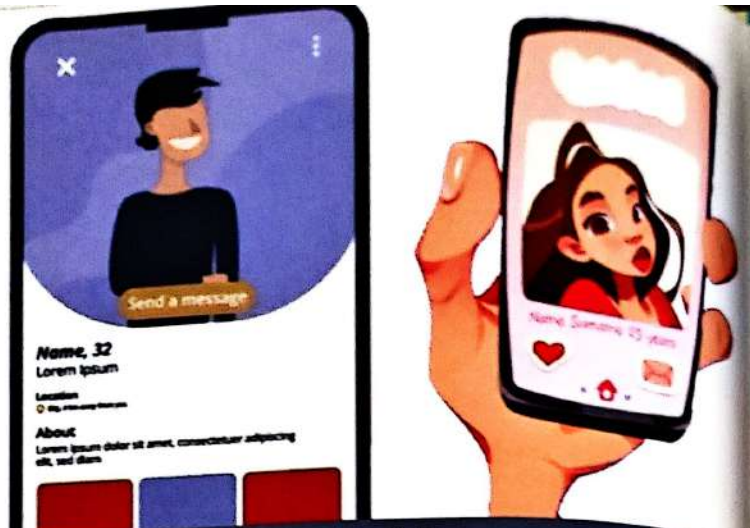
- क्या मैंने खुद कोई ऐसा लेन–देन किया था?
- क्या यह संदेश किसी विश्वसनीय स्रोत से आया है?
- क्या संदेश में जल्दी करने या दबाव बनाने की कोशिश की जा रही है?
- मैसेज और कॉल को ध्यान से पढ़ें / समझें।
- क्या इसमें गलत वर्तनी या अजीब भाषा का इस्तेमाल किया गया है?
- क्या संदेश में कोई संदेहजनक लिंक है?

कैसे बचें ओटीपी धोखाधड़ी से ?

- किसी भी थर्ड–पार्टी के ऐप को डाउनलोड करने से पहले सतर्क रहें।
- स्क्रीन शेयरिंग ऐप को किसी अजनबी के कहने पर इंस्टॉल न करें।
- किसी भी धोखाधड़ी की स्थिति में तुरंत अपने बैंक से संपर्क करें और अपनी कार्ड या खाता ब्लॉक करवाएं।
- साइबर अपराध की शिकायत www.cybercrime.gov.in पर करें या 1930 हेल्पलाइन नंबर पर कॉल करें।

ओटीपी फ्रॉड से बचाव के उपाय

- किसी के साथ भी ओटीपी साझा न करें।
- अज्ञात नंबरों से सतर्क रहें और बैंक से सीधे संपर्क करें।
- संदिग्ध लिंक पर क्लिक न करें, केवल आधिकारिक वेबसाइट का उपयोग करें।
- बैंकिंग ऐप्स में मजबूत पासवर्ड और 2–फैक्टर ऑथेंटिकेशन का इस्तेमाल करें।
- सोशल मीडिया पर बैंकिंग डिटेल्स साझा करने से बचें।
- पब्लिक वाई–फाई पर ऑनलाइन बैंकिंग न करें।
- किसी भी अनजान नंबर से कॉल फॉरवर्डिंग न करें।
- कोई भी वित्तीय निर्णय लेने से पहले संबंधित संस्था से पुष्टि करें।



क्या आप ऑनलाइन जीवनसाथी की तलाश कर रहे हैं?

सूचना प्रौद्योगिकी अधिनियम, 2000 (IT Act 2000) के तहत ऑनलाइन विवाह साइटें मध्यस्थ (Intermediary) मानी जाती हैं और इन प्लेटफॉर्म पर होने वाली धोखाधड़ी के लिए ये भी जिम्मेदार होती हैं। लेकिन, इन साइटों पर सख्त KYC (Know Your Customer) प्रक्रिया लागू नहीं होती, जिससे फर्जी प्रोफाइल आसानी से बन जाते हैं।

भारत में अधिकतर शादियाँ माता–पिता द्वारा तय की जाती हैं, लंकिन अब ऑनलाइन विवाह साइटों ने तेजी से अपनी जगह बना ली है। पारंपरिक विवाह प्रक्रिया को एक नया रूप मिला, जब इंटरनेट के माध्यम से जीवनसाथी खोजने की सुविधा शुरू हुई।

हालांकि, इन प्लेटफॉर्म्स के बढ़ते उपयोग के साथ–साथ साइबर अपराधों का खतरा भी बढ़ रहा है। साइबर अपराधी नकली प्रोफाइल बनाकर लोगों को धोखा देने का प्रयास करते हैं। इसलिए, ऑनलाइन जीवनसाथी की तलाश करते समय सतर्क रहना अत्यंत आवश्यक है।

ऑनलाइन विवाह धोखाधड़ी कैसे होती है?

1. फर्जी प्रोफाइल बनाना – धोखेबाज आकर्षक विवरण के साथ फर्जी प्रोफाइल बनाते हैं। अक्सर वे खुद को विदेश में कार्यरत दिखाते हैं, जिससे वास्तविक मुलाकात मुश्किल हो जाती है।

2. शिकार की तलाश – ऐसे प्रोफाइल मुख्यतः विधवा, तलाकशुदा या उम्रदराज महिलाओं को निशाना बनाते हैं। साथ ही, आर्थिक रूप से संपन्न लोगों को भी फँसाने की कोशिश करते हैं।

3. व्यक्तिगत बातचीत शुरू करना – फोन नंबर और ईमेल शेयर करके विश्वास जीता जाता है। एक बार भरोसा जम जाने पर, वे ऑनलाइन विवाह साइट से प्रोफाइल हटा देते हैं और सिर्फ फोन या ईमेल पर संपर्क रखते हैं।

4. पैसे की माँग– जब भरोसा पूरी तरह बन जाता है, तो धोखेबाज महंगे गिफ्ट की कस्टम क्लियरेंस, विदेशी मुद्रा रूपांतरण शुल्क, हीरे–गहनों की सरकारी मंजूरी, या पारिवारिक आपात स्थिति जैसे बहानों से पैसे माँगते हैं।

5. गायब हो जाना– पैसे मिलने के बाद, धोखेबाज पीड़ित से संपर्क तोड़ लेते हैं, जिससे उन्हें ढूँढना मुश्किल हो जाता है।

सुरक्षित ऑनलाइन विवाह के लिए महत्वपूर्ण सावधानियाँ

1. सही विवाह साइट का चुनाव करें

- गूगल पर अच्छी तरह से खोजें और उपयोगकर्ताओं की समीक्षाएँ पढ़ें।
- सत्यापित प्रोफाइल वाले प्लेटफॉर्म को प्राथमिकता दें।
- वेबसाइट की विश्वसनीयता जाँचें और पंजीकरण से पहले उसकी नीतियों को समझें।

2. प्रोफाइल की गहराई से जाँच करें

- नाम, पता, शिक्षा, नौकरी और पारिवारिक पृष्ठभूमि की पुष्टि करें।
- सोशल मीडिया प्रोफाइल देखें, अगर कोई जानकारी नहीं मिले, तो सतर्क रहें।

3. अलग ईमेल आईडी का उपयोग करें

- शादी की वेबसाइट पर रजिस्टर करने के लिए एक अलग ईमेल आईडी बनाएं। हमेशा ईमेल के जरिए बातचीत करें और शुरुआत में अपना व्यक्तिगत डेटा जैसे फोटो, फोन नंबर, घर का पता आदि साझा न करें।

4. जल्दबाजी न करें

- शादी जिंदगी का अहम फैसला है, इसे धीरे–धीरे आगे बढ़ाएँ।
- अगर कोई जल्दी शादी के लिए दबाव बना रहा है, तो सावधान रहें।
- कभी भी व्यक्तिगत या संवेदनशील तस्वीरें साझा न करें।

5. पैसों की लेन–देन से बचें

- किसी भी परिस्थिति में पैसे या संपत्ति देने से पहले पूरी तरह जाँच–पड़ताल करें।
- अगर कोई व्यक्ति बार–बार पैसों की माँग करता है, तो तुरंत वेबसाइट पर रिपोर्ट करें।

6. व्यक्तिगत रूप से मिलें

- ऑनलाइन बातचीत के बाद यदि आपको भरोसा हो, तो सार्वजनिक स्थान पर मिलें।
- परिवार के किसी सदस्य या करीबी दोस्त को साथ लेकर जाएँ।

7. एनआरआई (NRI) प्रोफाइल से सतर्क रहें

- एनआरआई प्रोफाइल पर शादी का फैसला करने से पहले उससे व्यक्तिगत रूप से मिलें। उनके विदेश में रहने और काम करने से जुड़े दस्तावेजों की जांच करें। ■■

धोखाधड़ी के संकेत (Red Flag)

- वीडियो कॉल या सामने मिलने से बचता हो।
- जल्दी प्यार जताने लगे।
- छोटे या बड़े अमाउंट के पैसे ट्रांसफर की माँग करे।
- सोशल मीडिया पर बहुत कम जानकारी हो।
- परिवार या कार्यस्थल की जानकारी देने से बचे।
- एक ही प्रोफाइल से कई बार संपर्क करे और बार–बार नंबर बदले।

ऑनलाइन मैट्रिमोनियल फ्रॉड के मामले

मामला 1 –

एक 40 साल की महिला को एक शख्स ने भारतीय मूल का यूके निवासी बताया और मैट्रिमोनियल साइट पर रिक्वेस्ट भेजी। शादी का प्रस्ताव देकर उसने महिला का विश्वास जीत लिया और कहा कि वह मुंबई मिलने आ रहा है।

इसके बाद महिला को फोन आया कि वह दिल्ली एयरपोर्ट पर फंस गया है। फिर एक महिला, जो खुद को कस्टम अधिकारी बता रही थी, ने कॉल पर बताया कि उसे ज्यादा अमेरिकी डॉलर लाने के कारण रोका गया है और उसकी जमानत के लिए पैसे देने होंगे। महिला ने कुल 74 लाख रुपये दे दिए। पैसे मिलते ही उस व्यक्ति ने संपर्क बंद कर दिया, तब जाकर महिला को एहसास हुआ कि उसके साथ धोखा हुआ है। मामले में FIR दर्ज कर की गई है।

मामला 2 –

एक महिला ने मैट्रिमोनियल साइट पर अपनी फर्जी प्रोफाइल बनाई। 31 वर्षीय शिकायतकर्ता ने उस महिला की प्रोफाइल देखकर बातचीत करने लगे। जब शिकायतकर्ता ने मिलने की इच्छा जताई, तो महिला ने बहाने बनाकर मिलने से मना कर दिया।

बाद में, महिला ने अपने जन्मदिन पर मिलने की बात कही और शिकायतकर्ता से आईफोन खरीदने को कहा। लेकिन फिर उसने मिलने से इनकार कर दिया और कहा कि उसके पिता अस्पताल में भर्ती हैं।

महिला ने इलाज के नाम पर कई बार में कुल 23. 44 लाख रुपये ले लिए, जिसमें आईफोन की कीमत भी शामिल थी। जब शिकायतकर्ता ने उसे मिलने के लिए मजबूर किया, तो महिला ने अंततः उससे मुलाकात की। लेकिन तब उसे एहसास हुआ कि महिला की असली शक्ल उसकी प्रोफाइल फोटो से बिल्कुल अलग थी। पूछताछ करने पर महिला ने कबूल किया कि उसने किसी अमीर व्यक्ति को फंसाने के लिए फर्जी तस्वीरें अपलोड की थीं ताकि वह उसके पिता के इलाज का खर्च उठा सके।

सावधान रहें!

जीवनसाथी ढूंढना आसान नहीं होता। इसमें समय लग सकता है, लेकिन सिर्फ इसलिए किसी जाल में न फंसें कि चीजें आपकी उम्मीद के मुताबिक नहीं हो रही हैं। ऑनलाइन प्यार और खुशहाल जीवनसाथी पाने के लिए सबसे जरूरी है सतर्क रहना।

साइबर सुरक्षा संकल्प

Not every Prince charming Is after your hea₹t

Be smart and be vigilant

Indian Costums never calls or send SMS. All communications from Indian Costums contains **Document Identification Number (DIN)** which is a unique number and can be verified at **www.cbic.gov.in**

IN CASE OF THESE EVENTS CONTACT YOUR LOCAL POLICE

Identity Theft

पहचान की चोरी

डिजिटल युग की गंभीर चुनौती

अपने बैंक खातों, क्रेडिट कार्ड स्टेटमेंट्स और क्रेडिट रिपोर्ट की नियमित रूप से जांच करें। डिजिटल लेन–देन, अकाउंट रजिस्ट्रेशन और ऑनलाइन खरीदारी के बढ़ते चलन के कारण साइबर सुरक्षा जोखिम भी बढ़ गए हैं। इसलिए सतर्क रहना ही सबसे बड़ा बचाव है।

जब कोई व्यक्ति बिना अनुमति के किसी अन्य व्यक्ति की व्यक्तिगत जानकारी चुरा लेता है और उसका गलत इस्तेमाल करता है, तो इसे पहचान की चोरी (Identity Theft) कहा जाता है। यह जानकारी नाम, फोन नंबर, पता, बैंक खाता नंबर, आधार नंबर या क्रेडिट / डेबिट कार्ड नंबर आदि हो सकती है।

पहचान की चोरी के प्रकार

वित्तीय पहचान की चोरी (Financial Identity Theft- इसमें अपराधी वित्तीय खाते की जानकारी, जैसे क्रेडिट कार्ड या बैंक खाते के नंबर, चुरा लेते हैं। वे आमतौर पर ऑनलाइन धोखा देकर या असुरक्षित स्थानों और डेटाबेस से विवरण चुराकर इस जानकारी तक पहुंचते हैं।

चिकित्सा पहचान की चोरी (Medical Identity Theft)– इस प्रकार की चोरी में अपराधी किसी अन्य व्यक्ति की स्वास्थ्य बीमा जानकारी का दुरुपयोग करके चिकित्सा सेवाएं प्राप्त करते हैं। यह अपराध न केवल वित्तीय नुकसान पहुंचाता है, बल्कि पीड़ित के चिकित्सा रिकॉर्ड में गलत प्रविष्टियाँ जोड़कर गंभीर स्वास्थ्य जोखिम भी पैदा कर सकता है।

सामाजिक सुरक्षा पहचान की चोरी (Social Security Identity Theft)– इस प्रकार की चोरी में अपराधी किसी व्यक्ति के सामाजिक सुरक्षा नंबर का उपयोग करके नए क्रेडिट खाते खोलते हैं, जिससे पीड़ित के क्रेडिट स्कोर पर नकारात्मक प्रभाव पड़ सकता है।

बाल पहचान की चोरी (Child Identity Theft)– इसमें अपराधी किसी बच्चे की जानकारी का उपयोग करके विभिन्न प्रकार की धोखाधड़ी को अंजाम देते हैं।

कृत्रिम पहचान की चोरी (Synthetic Identity Theft)– इसमें अपराधी असली और नकली जानकारी को मिलाकर एक पूरी तरह से नई पहचान तैयार करते हैं।

कर संबंधी पहचान की चोरी (Tax related Identity Theft)– जब कोई व्यक्ति चोरी की गई व्यक्तिगत जानकारी का उपयोग करके कर रिटर्न दाखिल करता है और गलत तरीके से कर वापसी का दावा करता है, तो इसे कर–संबंधी पहचान की चोरी कहा जाता है।

वृद्धजनों से धोखाधड़ी (Elder Fraud)– बुजुर्ग आमतौर पर अच्छे क्रेडिट स्कोर वाले होते हैं, इसलिए वे पहचान चोरों के आसान शिकार बनते हैं। उदाहरण के लिए, धोखेबाज मेडिकेयर प्रतिनिधि बनकर फोन पर संवेदनशील जानकारी प्राप्त करने की कोशिश कर सकते हैं।

सोशल मीडिया पहचान की चोरी (Social Media Identity Theft)–अपराधी सोशल मीडिया प्लेटफॉर्म पर कमजोर गोपनीयता सेटिंग्स का फायदा उठाकर या फर्जी सोशल मीडिया अकाउंट बनाकर किसी व्यक्ति की पहचान की नकल कर सकते हैं और इसका दुरुपयोग कर सकते हैं।

ऑनलाइन शॉपिंग धोखाधड़ी (Online Shopping Fraud)– साइबर अपराधी असुरक्षित ऑनलाइन शॉपिंग प्लेटफॉर्म में सेंध लगाकर ग्राहक की गोपनीय जानकारी, जैसे क्रेडिट कार्ड नंबर, चुरा सकते हैं।

चेतावनी संकेत

पहचान की चोरी कई तरह से हो सकती है, इसलिए इसके संकेत हमेशा साफ–साफ नजर नहीं आते। लेकिन कुछ सामान्य चेतावनी संकेत हैं, जो बताते हैं कि आपकी पहचान या संवेदनशील व्यक्तिगत जानकारी चोरी हो सकती है।

- अजनबी खर्चों के बिल या ऐसे खातों के लिए वसूली नोटिस मिलना, जिन्हें आपने कभी नहीं खोला।
- बिल या बैंक स्टेटमेंट्स का न आना।
- क्रेडिट रिपोर्ट में अनजान गतिविधियां दिखना, जैसे नए खाते खुलना या नए अनुरोध दर्ज होना।
- ऐसे क्रेडिट कार्ड या बैंक स्टेटमेंट मिलना, जिनके लिए आपने आवेदन ही नहीं किया।
- ऐसे मेडिकल बिल आना, जिनमें दिखाए गए इलाज आपने करवाए ही नहीं।
- बिना किसी कारण के क्रेडिट या लोन के लिए आवेदन अस्वीकार हो जाना।

अपने बैंक, क्रेडिट कार्ड कंपनी या क्रेडिट में कोई संदिग्ध गतिविधि नजर आती है, तो तुरंत इसकी रिपोर्ट करें।

- किसी ऐसे खाते के लिए कर्ज वसूली एजेंटों के कॉल आना, जिसे आपने कभी नहीं खोला।
- डाक (मेल) न मिलना या डाक का अचानक गायब हो जाना।

धोखाधडी होने पर क्या करें ?

अगर आप पहचान की चोरी का शिकार हो गए हैं, तो घबराएं नहीं, उचित तरीके से समस्या का समाधान करें।

1. धोखाधडी की रिपोर्ट करें– अगर आपके बैंक खाते या क्रेडिट कार्ड में कोई संदिग्ध गतिविधि दिख रही है, तो तुरंत अपने बैंक या क्रेडिट कार्ड कंपनी से संपर्क करें। यदि आवश्यक हो, तो शिकायत दर्ज कराएं। अपने क्रेडिट रिपोर्ट पर फ्रॉड अलर्ट लगवाएं।

2. संदिग्ध खातों को बंद करें– उन खातों को तुरंत बंद कर दें, जो आपकी जानकारी के बिना खोले गए हैं या जिनका दुरुपयोग किया गया है।

3. प्रासंगिक दस्तावेज एकत्र करें– अपने क्रेडिट रिपोर्ट की प्रतियां प्राप्त करें, गलतियों को ठीक करें, और इन दस्तावेजों को सुरक्षित रखें, क्योंकि बैंक और अन्य संस्थाएं इनकी मांग कर सकती हैं।

4. रिपोर्ट तैयार करें– यह रिपोर्ट आपको क्रेडिट कंपनियों, कर्ज वसूलने वाली एजेंसियों और अन्य व्यापारिक संस्थानों के साथ बातचीत में मदद करेगी।

5. पासवर्ड और पिन बदलें– सभी महत्वपूर्ण खातों के पासवर्ड और पिन को अपडेट करें, खासकर ईमेल, बैंकिंग और अन्य वित्तीय खातों के।

पहचान की चोरी से होने वाले नुकसान

धोखेबाज आपकी चुराई गई जानकारी का इस्तेमाल करके–

- ✓ आपके बैंक खाते तक पहुँच सकता है।
- ✓ लोन या क्रेडिट कार्ड के लिए आवेदन कर सकता है।
- ✓ आपके नाम पर टैक्स रिफंड क्लेम कर सकता है।
- ✓ ड्राइविंग लाइसेंस, पासपोर्ट या वीजा बनवा सकता है।
- ✓ बिजली, पानी, गैस जैसे नए कनेक्शन ले सकता है।
- ✓ आपके मेडिकल इंश्योरेंस पर इलाज करवा सकता है।
- ✓ सोशल मीडिया पर आपकी पहचान का गलत इस्तेमाल कर सकता है।

धोखाधडी से खुद को कैसे बचाएं ?

आज के डिजिटल युग में, जब लगभग हर काम ऑनलाइन होता है, तो अपनी व्यक्तिगत जानकारी की सुरक्षा करना बेहद जरूरी हो गया है।

पहचान की चोरी से बचने के उपाय

☑ **मजबूत पासवर्ड का उपयोग करें**– ऐसा पासवर्ड बनाएं जिसे अनुमान लगाना मुश्किल हो। इसमें अक्षर, संख्याएं और विशेष प्रतीकों का मिश्रण होना चाहिए।

☑ **व्यक्तिगत दस्तावेज नष्ट करें**– अपनी निजी जानकारी वाले दस्तावेज कूड़ेदान में फेंकने से पहले उन्हें काटकर या जलाकर नष्ट कर दें, ताकि कोई उनका दुरुपयोग न कर सके।

☑ **सार्वजनिक वाई–फाई से सावधान रहें**– सार्वजनिक वाई–फाई नेटवर्क का उपयोग करने से बचें, क्योंकि ये हैकर्स के लिए आपकी निजी जानकारी चुराने का आसान तरीका हो सकते हैं।

☑ **ऑनलाइन और फोन पर सतर्क रहें**– किसी को भी व्यक्तिगत जानकारी न दें, जब तक कि आप खुद संपर्क न करें और उस व्यक्ति या संस्था पर पूरा भरोसा न हो।

इसके अलावा, अपने बैंक खातों, क्रेडिट कार्ड स्टेटमेंट्स और क्रेडिट रिपोर्ट की नियमित रूप से जांच करें। डिजिटल लेन–देन, अकाउंट रजिस्ट्रेशन और ऑनलाइन खरीदारी के बढ़ते चलन के कारण साइबर सुरक्षा जोखिम भी बढ़ गए हैं। इसलिए सतर्क रहना ही सबसे बड़ा बचाव है।

DO YOU GIVE YOUR INFORMATION TO KNOWN PEOPLE

सुरेश एक कम ब्याज दर पर गैर–मान्यता प्राप्त लोन एजेंसी से होम लोन के लिए आवेदन करता है। वह अपने PAN कार्ड और आयकर रिटर्न (ITR) की फोटोकॉपी जमा कर देता है।

4 महीने बाद...बैंक से कॉल आता है– 'क्या आपने हमारे बैंक से ऑटो लोन लिया है?' सुरेश को पता चलता है कि उसके दस्तावेज का गलत इस्तेमाल करके 7 अलग–अलग बैंकों से लोन लिया गया है।

पुलिस जाँच में सामने आता है कि **धोखेबाज ने सुरेश की पहचान पत्रों की फोटोकॉपी पर फोटो, हस्ताक्षर, पता और मोबाइल नंबर बदलकर फर्जी आवेदन किए थे।**

सुरेश को पछतावा होता है कि उसने अपनी निजी जानकारी गलत जगह साझा कर दी।

BE CAREFUL

अपराधी ऑनलाइन बैंकिंग सिस्टम या मोबाइल एप्लिकेशन में सुरक्षा कमजोरियों का फायदा उठाकर साइबर अपराधी अनधिकृत पहुंच प्राप्त कर सकते हैं।

डिजिटल बैंक धोखाधड़ी

हाल के वर्षों में, डिजिटल बैंकिंग व्यक्तिगत और व्यावसायिक वित्तीय प्रबंधन का एक लोकप्रिय तरीका बन गया है। हालांकि, ऑनलाइन बैंकिंग की सुविधा के साथ–साथ डिजिटल बैंक धोखाधड़ी का खतरा भी बढ़ गया है। साइबर अपराधी डिजिटल बैंकिंग में कमजोरियों का फायदा उठाने के नए तरीके खोज रहे हैं। सतर्कता, सही जानकारी और सुरक्षित व्यवहार अपनाकर हम अपने वित्तीय लेन–देन को सुरक्षित बना सकते हैं। ।

डिजिटल बैंक धोखाधड़ी कैसे होती है ?

डिजिटल बैंक धोखाधड़ी तब होती है जब अपराधी विभिन्न तरीकों से किसी व्यक्ति की व्यक्तिगत या वित्तीय जानकारी तक अनधिकृत पहुंच प्राप्त कर लेते हैं।

1. फिशिंग अटैक (Phishing Attack)

यह सबसे आम तरीका है जिसमें धोखेबाज बैंक या वित्तीय संस्थान के नाम पर नकली ईमेल भेजते हैं और उपयोगकर्ताओं से उनकी संवेदनशील जानकारी जैसे लॉगिन क्रेडेंशियल्स मांगते हैं। ये ईमेल अक्सर आधिकारिक दिखते हैं और उपयोगकर्ताओं को किसी लिंक पर क्लिक करने के लिए प्रेरित करते हैं, जो उन्हें नकली वेबसाइट पर ले जाता है।

2. मैलवेयर अटैक (Malware Attack)

मैलवेयर एक प्रकार का हानिकारक सॉफ्टवेयर होता है जो कंप्यूटर या मोबाइल डिवाइस में प्रवेश कर सकता है। एक बार इंस्टॉल हो जाने पर, यह कीस्ट्रोक रिकॉर्ड कर सकता है, लॉगिन क्रेडेंशियल्स चुरा सकता है, और उपयोगकर्ता की जानकारी तक पहुंच प्राप्त कर सकता है।

3. सोशल इंजीनियरिंग (Social Engineering)

इसमें धोखेबाज लोगों को फोन कॉल, टेक्स्ट मैसेज या सोशल मीडिया के माध्यम से धोखा देकर उनकी गोपनीय जानकारी प्राप्त करने की कोशिश करते हैं।

4. ऑनलाइन बैंकिंग सिस्टम की खामियों का फायदा उठाना

अपराधी ऑनलाइन बैंकिंग सिस्टम या मोबाइल एप्लिकेशन में सुरक्षा कमजोरियों का फायदा उठाकर अनधिकृत पहुंच प्राप्त कर सकते हैं। वे सत्र अपहरण (Session Hijacking) या क्रॉस–साइट स्क्रिप्टिंग (Cross-Site Scripting) जैसी तकनीकों का उपयोग कर खातों से पैसे निकाल सकते हैं।

डिजिटल बैंक धोखाधड़ी के प्रकार

1. क्रेडिट कार्ड धोखाधड़ी (Credit Card Fraud)

इसमें अपराधी किसी व्यक्ति की क्रेडिट कार्ड जानकारी का उपयोग करके अनधिकृत लेनदेन करते हैं। यह चोरी हुए कार्ड डेटा, नकली कार्ड या ऑनलाइन खरीदारी के माध्यम से हो सकता है।

2. पहचान की चोरी (Identity Theft)

इसमें धोखेबाज किसी व्यक्ति की व्यक्तिगत जानकारी, जैसे आधार नंबर या जन्मतिथि, चुराकर उसका दुरुपयोग करते हैं। इससे वे नकली बैंक खाते खोल सकते हैं या ऋण प्राप्त कर सकते हैं।

3. फिशिंग अटैक (Phishing Attack)

यह धोखाधड़ी ईमेल, टेक्स्ट संदेश या नकली वेबसाइटों के माध्यम से की जाती है, जहां उपयोगकर्ताओं को उनकी वित्तीय जानकारी साझा करने के लिए प्रेरित किया जाता है।

4. खाता अधिग्रहण (Account Takeover)

इसमें अपराधी उपयोगकर्ता के बैंक खाते तक पहुंच प्राप्त कर लेते हैं और अवैध रूप से धन निकासी कर सकते हैं। वे ब्रूट फोर्स (Brute Force) हमलों या चोरी किए गए पासवर्ड का उपयोग करके लॉगिन क्रेडेंशियल्स प्राप्त करते हैं।

5. मोबाइल बैंकिंग धोखाधड़ी (Mobile Banking Fraud)

अपराधी मोबाइल बैंकिंग एप्लिकेशन के जरिए धोखाधड़ी करते हैं। वे नकली बैंकिंग ऐप्स, मैलवेयर से संक्रमित ऐप्स या सिम स्वैपिंग तकनीक का उपयोग करके उपयोगकर्ता के खाते तक पहुंच प्राप्त कर सकते हैं।

6. रैनसमवेयर अटैक (Ransomware Attack)

इसमें अपराधी मैलवेयर का उपयोग करके उपयोगकर्ता की फाइलों को एन्क्रिप्ट कर देते हैं और फिर फिरौती की मांग करते हैं।

सुरक्षित ऑनलाइन लेन-देन के लिए महत्वपूर्ण सुझाव

ऑनलाइन बैंकिंग और डिजिटल लेन–देन ने हमारे जीवन को आसान बना दिया है, लेकिन साइबर अपराधी भी लगातार नए तरीके खोज रहे हैं। सतर्कता, सही जानकारी और सुरक्षित व्यवहार अपनाकर हम अपने वित्तीय लेन–देन को सुरक्षित बना सकते हैं। याद रखें, सुरक्षा आपकी प्राथमिकता होनी चाहिए।

1. अपने बैंकिंग विवरण किसी से साझा न करें– कभी भी अपने नेट बैंकिंग पासवर्ड, वन टाइम पासवर्ड (OTP), एटीएम या फोन बैंकिंग पिन, CVV नंबर, कार्ड की समाप्ति तिथि आदि किसी के साथ साझा न करें, चाहे वह बैंक अधिकारी होने का दावा करे।

2. बैंक कभी पासवर्ड या OTP नहीं माँगता– कोई भी बैंक आपसे फोन या ईमेल पर पासवर्ड, OTP, पिन आदि नहीं माँगता। यदि कोई ऐसा करे, तो तुरंत अपने बैंक को इसकी सूचना दें।

3. मजबूत पासवर्ड बनाएं और समय–समय पर बदलें– अपने ऑनलाइन बैंकिंग अकाउंट का पासवर्ड मजबूत रखें और नियमित रूप से बदलें। पासवर्ड में छोटे–बड़े अक्षर, अंक और विशेष प्रतीक (जैसे /, रु, –) का उपयोग करें। जन्मतिथि या आसान पासवर्ड जैसे password / 123 न रखें।

4. सार्वजनिक या साझा कंप्यूटर पर ऑनलाइन बैंकिंग से बचें– साइबर कैफे या सार्वजनिक कंप्यूटर का उपयोग करते समय नेट बैंकिंग न करें। ये कंप्यूटर की–लॉगर सॉफ्टवेयर से संक्रमित हो सकते हैं, जो आपकी जानकारी चोरी कर सकते हैं।

5. हमेशा ब्राउजर डेटा साफ करें– नेट बैंकिंग या ऑनलाइन लेन–देन करने के बाद अपने ब्राउजर का इतिहास और कुकीज हटाना न भूलें।

6. सही बैंक वेबसाइट का उपयोग करें– हमेशा बैंक की आधिकारिक वेबसाइट का उपयोग करें और सुनिश्चित करें कि वेबसाइट के पते में "https://" हो और ब्राउजर में 'ताला' (Lock) आइकन दिखे।

7. अपने बैंक खाते की गतिविधियों पर नजर रखें– अपने बैंक खाते को नियमित रूप से लॉगिन करके जांचें कि कोई संदिग्ध लेन–देन तो नहीं हुआ है। यदि कोई गड़बड़ी मिले, तो तुरंत बैंक को सूचित करें।

8. संदिग्ध ईमेल और लिंक पर क्लिक न करें– यदि कोई ईमेल बैंक से आया हुआ लगे और उसमें लिंक पर क्लिक करने के लिए कहा जाए, तो सावधान रहें। यह फिशिंग (Phishing) हमला हो सकता है।

9. क्रेडिट/डेबिट कार्ड प्राप्त होने पर जाँच करें– जब भी नया कार्ड मिले, तो यह सुनिश्चित करें कि लिफाफा सील किया हुआ हो। अगर उसमें कोई छेड़छाड़ दिखे, तो तुरंत बैंक को सूचित करें।

10. ATM और POS (स्वाइप मशीन) पर सतर्कता बरतें– ATM पर पैसे निकालते समय आस–पास किसी अजनबी की गतिविधियों पर नजर रखें। किसी को भी अपना पिन देखने न दें और अपना लेन–देन पूरा करने के बाद ही ATM छोड़ें।

11. मोबाइल बैंकिंग के लिए फोन अपडेट रखें– यदि आप मोबाइल बैंकिंग का उपयोग करते हैं, तो अपने फोन का ऑपरेटिंग सिस्टम और एंटीवायरस सॉफ्टवेयर अपडेट रखें।

12. ई–वॉलेट का सुरक्षित उपयोग करें– हमेशा केवल आधिकारिक ऐप स्टोर (जैसे Google Play Store या Apple App Store) से ही ई–वॉलेट ऐप डाउनलोड करें। ईमेल, एसएमएस या सोशल मीडिया पर मिले लिंक से कोई भी ऐप इंस्टॉल न करें।

13. कार्ड की जानकारी सेव न करें– ई–वॉलेट या ऑनलाइन शॉपिंग वेबसाइटों पर अपने कार्ड की जानकारी सेव न करें। इससे डेटा चोरी का खतरा बढ़ सकता है।

14. अंतरराष्ट्रीय लेन–देन की सुविधा तभी चालू करें जब जरूरत हो– यदि आप विदेश यात्रा नहीं कर रहे हैं, तो अपने कार्ड पर अंतरराष्ट्रीय लेन–देन की सुविधा को बंद रखें।

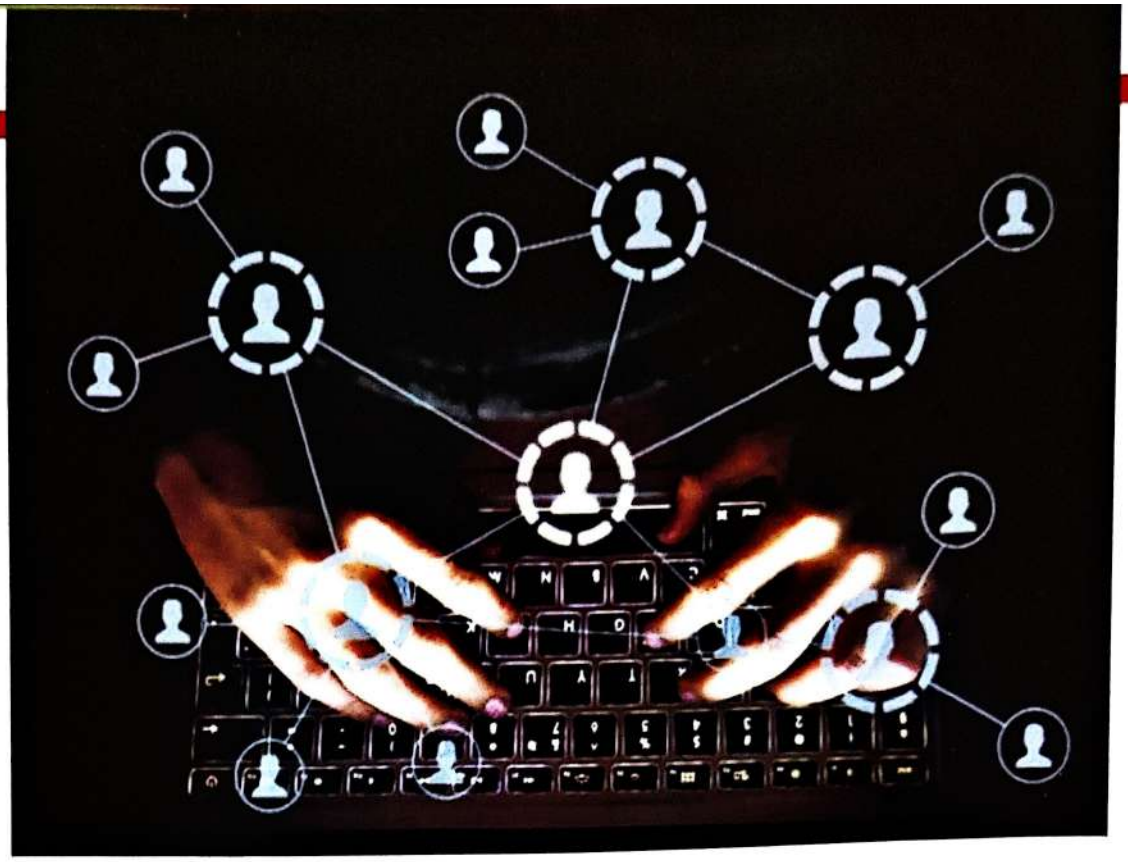
15. धोखाधड़ी वाले फोन कॉल से सावधान रहें– यदि कोई व्यक्ति आपके परिवार का सदस्य बनकर फोन करे और दुर्घटना या आपातकालीन स्थिति में पैसों की मांग करे, तो पहले अपने परिवार के व्यक्ति से सीधे संपर्क करें और सूचना की पुष्टि करें।

16. ऑनलाइन निवेश और पैसे कमाने वाले विज्ञापनों से बचे– यदि कोई विज्ञापन यह दावा करता है कि बिना मेहनत के पैसा कमाया जा सकता है, तो सतर्क रहें। यह एक ऑनलाइन धोखाधड़ी हो सकती है।

17. सिर्फ विश्वसनीय वेबसाइटों से खरीदारी करें– ऑनलाइन शॉपिंग करते समय केवल जानी–मानी वेबसाइटों से ही सामान खरीदें। किसी संदिग्ध वेबसाइट पर अपने बैंक की जानकारी दर्ज न करें।

18. ब्राउजर में ऑटो–फिल सुविधा का उपयोग न करें– ऑनलाइन फॉर्म भरते समय ब्राउजर की ऑटो–फिल सुविधा बंद रखें ताकि आपकी संवेदनशील जानकारी सुरक्षित रहे। ■■

साइबर सुरक्षा संकल्प



Pawan Jeenwal
Add District & Sessions Judge, Secretary, DLSA, Jaipur

वित्तीय धोखाधडी मामलों में बैंक द्वारा कस्टमर की गलती बताकर किसी भी प्रकार की कोई राशि कस्टमर को नही लौटाई जाती है। जबकि भारतीय रिजर्व बैंक के दिशानिर्देशों के अनुसार, यदि किसी साइबर अपराध के तहत वित्तीय धोखाधडी होती है और ग्राहक तीन दिनों के भीतर बैंक को सूचना दे देता है तो बैंक उसे संपूर्ण राशि लौटाने के लिए उत्तरदायी है।

साइबर फ्रॉड के शिकार हुए हैं?

कैसे पाएं अपना पैसा वापस

सागर ने लुई फिलिप्स नाम के ब्रांड का एक ब्लेजर (कोट) ऑनलाईन खरीदा। ब्लेजर के फिट नही आने पर उसे रिर्टन करने की ऑनलाईन रिक्वेस्ट लुई फिलिप्स पर भेज दी। अगले दिन एक व्यक्ति फोन कर स्वयं को लुई फिलिप्स का कस्टमर केयर एक्सीक्यूटिव बताकर रिर्टन अमाउंट प्राप्त करने के लिए उसे एक मोबाईल एप्प डाउनलोड करने के लिए कहता है। सागर उस एप्प को डाउनलोड कर लेता है और एप्प के डाउनलोड होने के बाद सागर के बैंक खाते से तीन बार में 95000 रूपये चले जाते है। तब सागर को अहसास होता है की उसके साथ साईबर अपराध हुआ है। सागर तुरंत ही इसकी सूचना अपने बैंक को देता है और नजदीकी थाने में एफ.आई.आर दर्ज करवाता है। इसी दौरान सागर को एक ई.मेल के जरिये संदेश प्राप्त होता है की लुई फिलिप्स की वेबसाईट को साईबर अपराधी ने हैक कर लिया है तथा लुई फिलिप्स के कस्टमर्स का डेटा लीक हो चुका है।

सागर के बैंक ने सागर को यह कहते हुए रूपए वापस देने से मना कर दिया की आपकी गलती की वजह से आपके बैंक खाते से रूपए गए है। इस में बैंक की कोई गलती नही है। इसलिए बैंक आपको कोई राशि नही लौटाएगा।

अधिकतर वित्तीय धोखाधडी मामलों में बैंक द्वारा कस्टमर की गलती बताकर किसी भी प्रकार की कोई राशि कस्टमर को नही लौटाई जाती है। जबकि भारतीय रिजर्व बैंक (RBI) के दिशानिर्देशों के अनुसार, यदि किसी साइबर अपराध के तहत वित्तीय धोखाधड़ी होती है और ग्राहक तीन दिनों के भीतर बैंक को सूचना दे देता है, तथा यदि गलती ग्राहक या बैंक की न होकर किसी

तीसरे पक्ष की होती है या या बैंक की और से अंशदायी लापरवाही (Contributory Negligence) तो बैंक उसे संपूर्ण राशि लौटाने के लिए उत्तरदायी है।

भारतीय रिजर्व बैंक (RBI) का परिपत्र (Circular)

6 जुलाई 2017 को RBI ने एक महत्वपूर्ण परिपत्र (RBI/2017-18/15 DBR-No-Leg-BC-78/09-07-005/2017-18) जारी किया था, जिसमें बैंकों को साइबर फ्रॉड के मामलों में ग्राहकों की सुरक्षा के लिए दिशा–निर्देश दिए गए हैं। इस परिपत्र के अनुसार–

1. ग्राहक की शून्य देयता–

ग्राहक को निम्नलिखित परिस्थितियों में शून्य देयता (Zero Liability) का लाभ मिलेगा–

- यदि बैंक की ओर से किसी प्रकार की धोखाधड़ी, लापरवाही या कमी हुई हो (चाहे ग्राहक द्वारा लेनदेन की सूचना दी गई हो या नहीं)।
- यदि गलती तीसरे पक्ष की हो। जहां न तो बैंक की और न ही ग्राहक की कोई कमी होती है, बल्कि प्रणाली के किसी अन्य भाग में गलती होती है,और ग्राहक बैंक को अनधिकृत लेनदेन की सूचना तीन कार्य दिवसों के भीतर दे दे।

2. ग्राहक की सीमित देयता (Limited Liability of a Customer)

ग्राहक निम्नलिखित परिस्थितियों में अनधिकृत लेनदेन से होने वाले नुकसान के लिए उत्तरदायी होगा–

- यदि ग्राहक की लापरवाही के कारण नुकसान होता है, जैसे कि उसने अपने भुगतान प्रमाण–पत्र (पेमेंट क्रेडेंशियल) साझा कर दिए हैं, तो ग्राहक को पूरी हानि वहन करनी होगी जब तक कि वह बैंक को अनधिकृत लेनदेन की सूचना नहीं देता। ग्राहक द्वारा रिपोर्ट करने के बाद होने वाले किसी भी नुकसान की भरपाई बैंक करेगा।
- यदि अनधिकृत इलेक्ट्रॉनिक बैंकिंग लेनदेन की जिम्मेदारी न तो बैंक की है और न ही ग्राहक की, बल्कि यह प्रणाली के किसी अन्य भाग में होती है, और ग्राहक बैंक से प्राप्त सूचना के चार से सात कार्य दिवसों के भीतर बैंक को सूचित करने में देरी करता है, तो ग्राहक की प्रति लेनदेन देयता सीमित होगी।

3. ग्राहक की देयता का सारांश

खाता प्रकार	अधिकतम देयता (₹)
• बीएसबीडी खाते	5,000
• अन्य सभी बचत खाते	10,000
• प्री–पेड भुगतान साधन और गिफ्ट कार्ड	10,000
• एमएसएमई के चालू/कैश क्रेडिट/ओवरड्राफ्ट खाते	25,000
• व्यक्तिगत चालू/कैश क्रेडिट/ओवरड्राफ्ट खाते जिनकी वार्षिक औसत शेष राशि (धोखाधड़ी की घटना से पहले के 365 दिनों में) / सीमा 25 लाख रुपये तक हो	25,000
• 5 लाख रुपये तक की सीमा वाले क्रेडिट कार्ड	25,000
• अन्य सभी चालू/कैश क्रेडिट/ओवरड्राफ्ट खाते	बैंक की अनुमोदित नीति के अनुसार

यदि रिपोर्ट करने में सात कार्य दिवसों से अधिक की देरी होती है, तो ग्राहक की देयता बैंक की बोर्ड अनुमोदित नीति के अनुसार निर्धारित की जाएगी। बैंक को अपने ग्राहकों को उनके खाते खोलने के समय इन नीतियों की जानकारी देनी होगी और सार्वजनिक रूप से अपनी अनुमोदित नीति प्रदर्शित करनी होगी। मौजूदा ग्राहकों को भी बैंक की नीति के बारे में व्यक्तिगत रूप से सूचित किया जाना चाहिए।

तीसरे पक्ष द्वारा की गई धोखाधड़ी की स्थिति में, जहां गलती न तो बैंक की होती है और न ही ग्राहक की, बल्कि प्रणाली के किसी अन्य भाग में होती है, ग्राहक की कुल देयता निम्नानुसार होगी–

धोखाधड़ी की सूचना देने में लिया गया समय	ग्राहक की देयता (₹)
3 कार्य दिवसों के भीतर	शून्य देयता
4 से 7 कार्य दिवसों के भीतर	बैंक की अधिकतम देय राशि या लेनदेन मूल्य में से जो भी कम हो
7 कार्य दिवसों के बाद	बैंक की बोर्ड अनुमोदित नीति के अनुसार

उल्लिखित कार्य दिवसों की गणना ग्राहक की होम ब्रांच के कार्य अनुसूची के अनुसार की जाएगी, जिसमें सूचना प्राप्त करने की तिथि शामिल नहीं होगी।

4. शून्य देयता– सीमित देयता की प्रतिपूर्ति की समय–सीमा Reversal Timeline for Zero Liability/ Limited Liability of customer

ग्राहक द्वारा सूचना देने पर, बैंक को अनधिकृत इलेक्ट्रॉनिक लेनदेन की राशि को ग्राहक के खाते में 10 कार्य दिवसों के भीतर (शैडो रिवर्सल के माध्यम से) जमा करना होगा, चाहे बीमा दावा निपटान की प्रतीक्षा हो या न हो। बैंक अपने विवेकानुसार ग्राहकों की लापरवाही के मामलों में भी उनकी देयता माफ कर सकते हैं। यह क्रेडिट उस दिनांक के अनुसार किया जाएगा जिस दिन अनधिकृत लेनदेन हुआ था।

इस संदर्भ में माननीय सर्वोच्च न्यायालय द्वारा **एसबीआई बैंक बनाम पल्लव भौमिक एवं अन्य** Petition for Special Leave to Appeal (C)No.30677/2024 के मामले में गोवाहाटी उच्च न्यायालय के उस निर्णय को सही ठहराते हुए एसबीआई बैंक की अपील का खारिज किया जिसमें गोवाहाटी उच्च न्यायालय के द्वारा एसबीआई बैंक को पीड़ित के साइबर अपराध के जरिये ठगे गए 94,204.80/– रूपये वापस लौटाने के आदेश दिये थे। ■■

आर.बी.आई द्वारा जारी किया गया परिपत्र में दी गई गाईडलाइन की पालना करने के बाद भी साईबर अपराध से पीडित व्यक्ति को बैंक द्वारा राशि नही लौटाई जाती है तो पीडित व्यक्ति द्वारा न्यायालय की शरण ली जा सकती है या स्थाई लोक अदालत के माध्यम से भी अनुतोष प्राप्त किया जा सकता है एवं इस संबंध में अधिक जानकारी संबंधित जिले के जिला विधिक सेवा प्राधिकरण के कार्यालय से प्राप्त की जा सकती है।

मोबाइल एप्लिकेशन धोखाधड़ी

राष्ट्रीय साइबर अपराध खतरा विश्लेषण इकाई (NCTAU) की हाल की रिपोर्टों में पाया गया कि ये ऐप्स कॉल इंटरसेप्ट कर सकते हैं, एसएमएस डेटा एक्सेस कर सकते हैं, और व्यक्तिगत जानकारी जैसे पैन नंबर, आधार डिटेल और बैंकिंग क्रेडेंशियल्स चुरा सकते हैं।

आज के डिजिटल युग में, अधिकतर दैनिक कार्य मोबाइल ऐप्स के माध्यम से किए जाते हैं। लेकिन इन्हीं सुविधाजनक ऐप्स के बीच कुछ धोखाधड़ी वाले एंड्रॉइड ऐप्स भी तेजी से बढ़ रहे हैं, जो यूजर्स को आकर्षक ऑफर देकर फँसाते हैं। ये नकली ऐप्स असली प्लेटफॉर्म की नकल करते हैं और इनाम प्राप्ति या क्रेडिट कार्ड लाभ जैसे ऑफर देकर लोगों को लुभाते हैं। हालांकि, ये ऐप्स वास्तव में खतरनाक मैलवेयर होते हैं, जो व्यक्तिगत और वित्तीय जानकारी चुराने के लिए डिजाइन किए जाते हैं। गंभीर मामलों में, ये ऐप्स अनधिकृत लेन–देन और मानसिक तनाव का कारण भी बन सकते हैं।

नकली एंड्रॉइड ऐप्स असली ऐप्स से कैसे अलग होते हैं?

ये ऐप्स असली प्लेटफॉर्म की नकल करके यूजर्स को इनाम प्राप्ति या तत्काल क्रेडिट कार्ड अनुमोदन जैसे लुभावने ऑफर देकर फँसाते हैं। लेकिन इनमें अक्सर ऐसे मैलवेयर छिपे होते हैं जो संवेदनशील जानकारी इकट्ठा करने के लिए बनाए गए होते हैं।

ये हानिकारक ऐप्स कैसे काम करते हैं?

इन ऐप्स के चालाकी भरे तरीकों को समझकर आप खुद को बेहतर तरीके से सुरक्षित रख सकते हैं।

1. झूठे वादे और लुभावने ऑफर

ये ऐप्स आकर्षक ऑफर देकर यूजर्स को डाउनलोड करने के लिए प्रेरित करते हैं। आमतौर पर दिए जाने वाले ऑफर में शामिल हैं– रिवॉर्ड पॉइंट भुनाने का मौका त्वरित क्रेडिट कार्ड अनुमोदन डाउनलोड होने के बाद, ये ऐप्स वास्तविक दिखते हैं और यूजर से संवेदनशील जानकारी दर्ज करने के लिए कहते हैं, जैसे क्रेडिट कार्ड डिटेल्स।

2. फिशिंग तकनीक

धोखाधड़ी वाले ऐप्स असली सेवाओं के डिजाइन और इंटरफेस की नकल करते हैं, जिससे यूजर्स को फर्क करना मुश्किल हो जाता है।

इनके फिशिंग तकनीकों में शामिल हैं–

- आधिकारिक लोगो, ब्रांडिंग और फीचर्स की नकल करना
- झूठे चेतावनी संदेश भेजना

3. टार्गेटेड डेटा संग्रह

ये ऐप्स संवेदनशील डेटा चुराने के लिए डिजाइन किए गए होते हैं। वे सत्यापन के बहाने आधार या पैन कार्ड अपलोड करने के लिए कह सकते हैं, जिससे पहचान की चोरी और वित्तीय धोखाधड़ी का खतरा बढ़ जाता है।

4. अत्यधिक अनुमतियाँ और डेटा चोरी

इंस्टॉल होने के बाद, ये ऐप्स अत्यधिक अनुमतियाँ मांगते हैं, जो उनकी वास्तविक कार्यक्षमता के लिए आवश्यक नहीं होतीं। इनमें शामिल हैं–

- एसएमएस संदेश और कॉल लॉग्स का एक्सेस
- कॉन्टैक्ट्स और लोकेशन डेटा
- कैमरा और माइक्रोफोन तक पहुँच
- इन अनुमतियों को स्वीकृत करने पर, ऐप आपके वन–टाइम पासवर्ड (OTP), पिन नंबर और अन्य संवेदनशील डेटा को चुरा सकता है।

5. फोन फीचर्स को हाईजैक करना

इंस्टॉल होने के बाद, ये ऐप्स आपके फोन के महत्वपूर्ण फीचर्स को नियंत्रित कर सकते हैं, जैसे–

- डिफॉल्ट एसएमएस ऐप

- बदलकर बैंकिंग और अन्य वित्तीय लेन–देन से जुड़े ओटीपी इंटरसेप्ट करना।
- कॉल फॉरवर्डिंग सेटिंग्स में बदलाव करके आपकी बातचीत को सुनना या संचार को नियंत्रित करना।

6. डेटा चोरी और साइबर अपराध

संवेदनशील जानकारी प्राप्त करने के बाद, ये ऐप्स डेटा को विभिन्न माध्यमों से हैकर्स को भेजते हैं, जैसे– एसएमएस या टेलीग्राम बॉट्स

7. ईमेल या अन्य मैसेजिंग प्लेटफॉर्म

इसे डेटा एक्सफिल्ट्रेशन कहा जाता है, जिससे साइबर अपराधी चोरी किए गए डेटा का उपयोग अनधिकृत वित्तीय लेन–देन और पहचान की चोरी के लिए कर सकते हैं।

नकली ऐप्स की पहचान कैसे करें ?

हालांकि ये ऐप्स देखने में वास्तविक लग सकते हैं, लेकिन कुछ चेतावनी संकेत होते हैं जिनसे आप उन्हें पहचान सकते हैं–

- **अत्यधिक अनुमतियाँ**–यदि कोई ऐप एसएमएस, कॉल लॉग, या बैंकिंग डिटेल्स जैसी संवेदनशील जानकारी मांगता है, तो सतर्क रहें।
- **अविश्वसनीय स्रोत**– किसी थर्ड–पार्टी स्टोर या एसएमएस/ईमेल से भेजे गए लिंक से ऐप डाउनलोड करने से बचें।
- **बहुत अच्छे ऑफर**– यदि कोई ऐप अवास्तविक इनाम या लाभ देने का दावा करता है, तो सावधान रहें।

साइबर अपराधी लगातार नए तरीकों से लोगों को धोखा देने की कोशिश कर रहे हैं, इसलिए आपकी सतर्कता ही आपकी सबसे बड़ी सुरक्षा है। किसी भी ऐप को डाउनलोड करने से पहले हमेशा सोचें – 'क्या यह स्रोत विश्वसनीय है ?' आपकी सुरक्षा आपके हाथ में है।

- **फोन सेटिंग्स में बदलाव**– यदि कोई ऐप आपके डिफॉल्ट एसएमएस या कॉल सेटिंग्स को बदलता है, तो उसे तुरंत अनइंस्टॉल करें

खुद को सुरक्षित रखने के आसान उपाय

अपने डेटा और वित्तीय सुरक्षा को सुनिश्चित करने के लिए इन सावधानियों का पालन करें–

- **केवल आधिकारिक स्रोतों से ऐप डाउनलोड करें**– हमेशा गूगल प्ले स्टोर से ऐप डाउनलोड करें और डेवलपर की जानकारी की पुटि करें।
- **ऐप अनुमतियों की समीक्षा करें** – केवल आवश्यक अनुमतियों को ही स्वीकृति दें। अनावश्यक सुविधाओं की पहुँच को अस्वीकार करें।
- **दो–स्तरीय प्रमाणीकरण (2FA) सक्षम करें**– अपने बैंकिंग खातों की सुरक्षा के लिए अतिरिक्त सुरक्षा परत जोड़ें।
- **डिवाइस को नियमित रूप से अपडेट करें**– फोन और ऐप्स को समय–समय पर अपडेट करें ताकि नए सुरक्षा पैच लागू हो सकें।
- **बैंक स्टेटमेंट की निगरानी करें**– अपने लेन–देन की नियमित जांच करें और किसी भी अनधिकृत गतिविधि की तुरंत रिपोर्ट करें।
- **विश्वसनीय एंटीवायरस सॉफ्टवेयर इंस्टॉल करें**– संभावित खतरों से बचने के लिए अपने फोन पर एक अच्छा एंटीवायरस रखें।

अगर आप धोखाधड़ी के शिकार हो गए तो क्या करें ?

- ऐप को तुरंत अनइंस्टॉल करें।
- अपने सभी खातों के पासवर्ड बदलें, खासकर बैंकिंग और ईमेल खातों के।
- अपने बैंक से संपर्क करें और किसी भी संदिग्ध लेन–देन की रिपोर्ट करें।
- राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (www.cybercrime.gov.in) या हेल्पलाइन (1930) पर शिकायत दर्ज करें। ■■

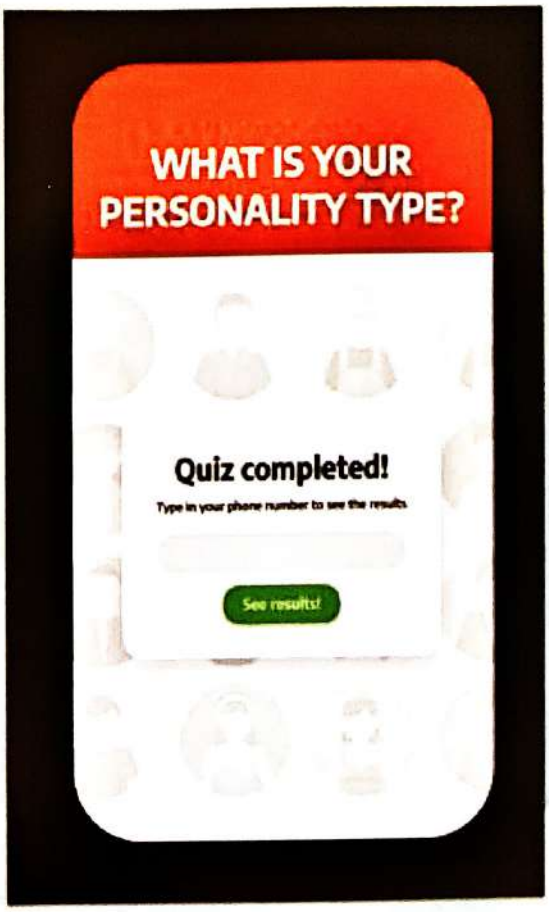
सतर्क रहें और साइबर धोखाधड़ी से बचें।

BIBLIOGRAPHY

Adware- सॉफ्टवेयर जो स्वचालित रूप से विज्ञापन दिखाता है।
Antivirus-सॉफ्टवेयर जो मैलवेयर का पता लगाता है और उसे हटाता है।
Backdoor- एक गुप्त तरीका जिससे हैकर्स सिस्टम में प्रवेश बना सकते हैं।
Biometric Authentication-उंगलियों के निशान, आँखों की पुतली, या चेहरे की पहचान के माध्यम से सत्यापन।
Botnet- हैकर्स द्वारा नियंत्रित कंप्यूटरों का नेटवर्क जो दुर्भावनापूर्ण कार्यों के लिए उपयोग किया जाता है।
Brute Force Attack- एक हमले जिसमें हैकर बार–बार प्रयास करके पासवर्ड तोड़ता है।
Cloud Security- क्लाउड स्टोरेज और सेवाओं की सुरक्षा।
Cookie- एक छोटी फाइल जो वेबसाइट द्वारा उपयोगकर्ता के कंप्यूटर पर संग्रहीत की जाती है।
Cryptography-डेटा को सुरक्षित रूप से एन्क्रिप्ट और डिक्रिप्ट करने की प्रक्रिया।
Cyber Attack-कंप्यूटर सिस्टम, नेटवर्क या डेटा को नुकसान पहुँचाने के लिए किया गया हमला।
Cyber Espionage- साइबर स्पेस में गुप्त जानकारी चुराने की प्रक्रिया।
Cyber Hygiene- साइबर सुरक्षा के लिए अच्छी आदतें और प्रथाएँ।
Dark Web- इंटरनेट का एक गुप्त हिस्सा जहां अवैध गतिविधियाँ होती हैं।
Data Breach- डेटा की अनधिकृत पहुँच या चोरी।
Data Encryption Standard (DES)- डेटा को एन्क्रिप्ट करने का एक पुराना मानक।
DDoS Attack- डिस्ट्रीब्यूटेड डिनायल–ऑफ–सर्विस (DDoS) हमला, जिसमें नेटवर्क पर ट्रैफिक का भार डाला जाता है।
Deepfake-कृत्रिम बुद्धिमत्ता (AI) का उपयोग करके बनाई गई नकली वीडियो या ऑडियो।
Encryption- डेटा को सुरक्षित रूप से कोड में बदलने की प्रक्रिया ताकि अधिकृत उपयोगकर्ता ही इसे पढ़ सकें।
Endpoint Security- नेटवर्क के अंतिम बिंदुओं (जैसे कंप्यूटर, मोबाइल) की सुरक्षा।
Ethical Hacking-सिस्टम की सुरक्षा कमजोरियों का पता लगाने के लिए कानूनी रूप से की गई हैकिंग।
Exploit- सॉफ्टवेयर या सिस्टम की कमजोरी का फायदा उठाने वाला कोड।
Fileless Malware-मैलवेयर जो फाइलों का उपयोग नहीं करता और सीधे मेमोरी में चलता है।
Firewall- एक सुरक्षा प्रणाली जो नेटवर्क पर अनधिकृत पहुँच को रोकती है।
Honeypot- एक जाल सिस्टम जो हैकर्स को आकर्षित करता है और उनकी गतिविधियों को रिकॉर्ड करता है।
Identity Theft- किसी व्यक्ति की पहचान चुराकर उसका गलत उपयोग करना।
Intrusion Detection System (IDS)-एक प्रणाली जो नेटवर्क पर संदिग्ध गतिविधियों का पता लगाती है।
Internet of Things (IoT)- इंटरनेट से जुड़े उपकरणों का नेटवर्क।
Keylogger- सॉफ्टवेयर या हार्डवेयर जो कीबोर्ड पर दबाए गए कुंजियों को रिकॉर्ड करता है।
Keystroke Dynamics- उपयोगकर्ता के टाइपिंग पैटर्न के आधार पर सत्यापन।
Logic Bomb- एक कोड जो विशेष परिस्थितियों में सक्रिय होकर नुकसान पहुँचाता है।
Malware- दुर्भावनापूर्ण सॉफ्टवेयर जो कंप्यूटर सिस्टम को नुकसान पहुँचाता है।
Man-in-the-Middle Attack- एक हमला जिसमें हैकर दो पक्षों के बीच संचार को बाधित करता है।
Multi-Factor Authentication (MFA)- सुरक्षा बढ़ाने के लिए एक से अधिक सत्यापन विधियों का उपयोग।
Network Sniffing- नेटवर्क ट्रैफिक को इंटरसेप्ट करके डेटा चोरी करना।
Obfuscation- कोड को इस तरह जटिल बनाना कि उसे समझना मुश्किल हो जाए।
Patch- सॉफ्टवेयर में सुरक्षा खामियों को ठीक करने के लिए अपडेट।
Penetration Testing- सिस्टम की सुरक्षा कमजोरियों का पता लगाने के लिए किया गया परीक्षण।
Phishing- धोखाधड़ी तकनीक जिसमें व्यक्ति से संवेदनशील जानकारी प्राप्त करने के लिए नकली ईमेल या लिंक भेजे जाते हैं।
Quantum Cryptography- क्वांटम यांत्रिकी के सिद्धांतों पर आधारित एन्क्रिप्शन तकनीक।
Ransomware- एक प्रकार का मैलवेयर जो डेटा को लॉक कर देता है और फिरौती मांगता है।
Rootkit-एक प्रकार का मैलवेयर जो सिस्टम के गहरे स्तर तक पहुंच बनाता है।
Sandbox- एक अलग वातावरण जहां संदिग्ध सॉफ्टवेयर को सुरक्षित रूप से जांचा जाता है।
Security Information and Event Management (SIEM)- सुरक्षा जानकारी और घटनाओं का प्रबंधन करने वाली प्रणाली।
Social Engineering- मनोवैज्ञानिक हेरफेर के माध्यम से संवेदनशील जानकारी प्राप्त करना।
Spam- अनचाहे और大量 में भेजे गए संदेश (जैसे ईमेल)।
Spyware- सॉफ्टवेयर जो गुप्त रूप से उपयोगकर्ता की गतिविधियों पर नजर रखता है।
Tokenization- संवेदनशील डेटा को टोकन में बदलकर सुरक्षित करना।
Trojan Horse- एक प्रकार का मैलवेयर जो वैध सॉफ्टवेयर की तरह दिखता है।
Two-Factor Authentication (2FA)- दो–चरणीय सत्यापन प्रक्रिया जो सुरक्षा बढ़ाती है।
VPN (Virtual Private Network)- एक सुरक्षित नेटवर्क कनेक्शन जो इंटरनेट पर डेटा को गोपनीय रखता है।
Watering Hole Attack-एक हमला जिसमें हैकर विश्वसनीय वेबसाइट को संक्रमित करता है।
Zero Trust Security- एक सुरक्षा मॉडल जो किसी भी उपयोगकर्ता या डिवाइस पर भरोसा नहीं करता।

Think twice before giving away personal information.

Social Media questionnaires and quizzes are often used by scammers to steal your personal information.



डार्क वेब

The Mysterious World of Internet

सामान्य तौर पर इंटरनेट सर्फेस वैब, डीप वैब, व डार्क वैब के रूप में उपयोग में लिया जाता है। आमजन द्वारा इंटरनेट का केवल 3 प्रतिशत भाग को ही उपयोग में लिया जाता है जिसे सर्फेस वैब के नाम से जाना जाता है जबकि इंटरनेट का 97 प्रतिशत भाग डीप वैब होता है और इसी डीप वैब का एक छोटा सा हिस्सा डार्क वैब के रूप में जाना जाता है डार्क वेब को अक्सर डीप वेब के साथ भ्रमित किया जाता है। डीप वेब इंटरनेट का वह हिस्सा है जो सर्च इंजन्स के माध्यम से इंडेक्स नहीं किया जाता, जैसे ऑनलाइन बैंकिंग पेज, प्राइवेट डेटाबेस, या सदस्यता वाली वेबसाइट्स। डार्क वेब, डीप वेब का एक छोटा हिस्सा है, जो गैरकानूनी गतिविधियों के लिए इस्तेमाल किया जा सकता है।

डार्क वैब इंटरनेट का वह हिस्सा है जो सामान्य सर्च इंजन्स जैसे Google, Bing या Yahoo के माध्यम से एक्सेस नहीं किया जा सकता। डार्क वेब के बारे में जानना न केवल रोचक है, बल्कि यह हमें इंटरनेट की गहराइयों और उसके खतरों के प्रति सचेत भी करता है।

डार्क वेब क्या है ?

डार्क वेब, इंटरनेट का एक छोटा किंतु महत्वपूर्ण हिस्सा है, जो सामान्य ब्राउजरों और सर्च इंजन्स के माध्यम से दिखाई नहीं देता। इसे एक्सेस करने के लिए विशेष सॉफ्टवेयर और टूल्स की आवश्यकता होती

समग्र इंटरनेट का 96% भाग डीप वैब और डार्क वेब है, हम इटंरनेट कंटेट के केवल 4% हिस्से का इस्तेमाल करते है।

सेक्सटॉर्शन

सेक्सटॉर्शन एक प्रकार का साइबर अपराध है, जिसमें अपराधी पीड़ित को ब्लैकमेल करते हैं और उनकी निजी तस्वीरें या वीडियो सार्वजनिक करने की धमकी देते हैं। यह अपराध अक्सर सोशल मीडिया, डेटिंग ऐप्स, या ईमेल के माध्यम से किया जाता है। सेक्सटॉर्शन का शिकार कोई भी हो सकता है, चाहे वह महिला हो, पुरुष हो, या यहां तक कि किशोर भी।

1. फेक आईडी के जरिए धोखा

अपराधी फेक आईडी बनाकर पीड़ित से दोस्ती करते हैं और उन्हें विश्वास दिलाते हैं कि वे उनके सच्चे दोस्त हैं। धीरे–धीरे वे पीड़ित को निजी तस्वीरें या वीडियो भेजने के लिए मजबूर करते हैं। एक बार तस्वीरें मिलने के बाद, वे पीड़ित को धमकी देते हैं कि अगर उन्हें पैसे नहीं

है, जैसे Tor Browser (The Onion Router) नेटवर्क उपयोगकर्ताओं को गुमनामी (Anonymity) प्रदान करता है, जिससे उनकी पहचान और स्थान छिपे रहते हैं। इस गोपनीयता के कारण डार्क वेब एक रहस्यमय और खतरनाक जगह है।

डार्क वेब का उपयोग क्यों किया जाता है ?

डार्क वेब का उपयोग कई तरह के उद्देश्यों के लिए किया जाता है। कुछ लोग इसे गोपनीयता और सुरक्षा के लिए इस्तेमाल करते हैं, जबकि साइबर अपराधी इसे अवैध गतिविधियों के लिए उपयोग में लाते हैं।

1. गोपनीयता और सुरक्षा– कुछ देशों में सरकारें अपने नागरिकों की ऑनलाइन गतिविधियों पर नजर रखती हैं और उनकी अभिव्यक्ति की आजादी को सीमित करती हैं। ऐसे में, डार्क वेब उन लोगों के लिए एक सुरक्षित स्थान है, जो सेंसरशिप से बचना चाहते हैं। पत्रकार, कार्यकर्ता और विपक्षी समूह अक्सर डार्क वेब का उपयोग करते हैं ताकि वे सुरक्षित रूप से संवाद कर सकें और जानकारी साझा कर सकें।

2. गैरकानूनी गतिविधियाँ– डार्क वेब की गुमनामी का फायदा उठाकर कई लोग अवैध काम करते हैं। यहाँ ड्रग्स, हथियार, कूट रचित दस्तावेज, और चोरी किए गए डिजिटल डेटा जैसी चीजों की बिक्री होती है। साइबर क्रिमिनल्स डार्क वेब का उपयोग हैकिंग, फिशिंग और अन्य साइबर अपराधों के लिए करते हैं।

3. जानकारी का आदान–प्रदान– कुछ लोग डार्क वेब का उपयोग ऐसी जानकारी साझा करने के लिए करते हैं, जो सामान्य इंटरनेट पर उपलब्ध नहीं है। इसमें शोध, राजनीतिक विचार, और अन्य संवेदनशील डेटा शामिल होते हैं।

डार्क वेब के खतरे

डार्क वेब एक खतरनाक स्थान है, खासकर उन लोगों के लिए जो इसके बारे में ज्यादा नहीं जानते। कुछ प्रमुख खतरे इस प्रकार हैं–

1. साइबर अपराध– डार्क वेब पर साइबर अपराधियों की भरमार है। यदि आप सावधान नहीं हैं, तो आपके पर्सनल डेटा, बैंक खाते, या यहाँ तक कि आपकी पहचान भी चोरी हो सकती है।

2. गैरकानूनी सामग्री– डार्क वेब पर अवैध, अश्लील और अनैतिक सामग्री आसानी से मिल जाती है। इस तरह की सामग्री को देखना या डाउनलोड करना दंडनीय अपराध है।

3.मानसिक स्वास्थ्य पर प्रभाव– डार्क वेब पर मौजूद हिंसक और अश्लील सामग्री लोगों के मानसिक स्वास्थ्य पर नकारात्मक प्रभाव डालती है।

4. कानूनी प्रभाव– डार्क वेब का उपयोग करते समय यदि आप किसी गैरकानूनी गतिविधि में शामिल होते हैं, तो आपको कानूनी परेशानियों का सामना करना पड़ सकता है।

डार्क वेब पर डेटा लीक होने से बचाने के लिए कोशिश करें कि किसी भी थर्ड पार्टी एप को गैर–जरूरी पर्सनल जानकारी न दें। इसके साथ ही किसी भी अनजान वेबसाइट से कोई भी एप डाउनलोड न करें।

डार्क वेब इंटरनेट का एक रहस्यमय और जटिल हिस्सा है, जो अच्छे और बुरे दोनों तरह के उद्देश्यों के लिए इस्तेमाल किया जा सकता है। डार्क वेब की दुनिया में कदम रखने से पहले यह याद रखें कि गुमनामी और स्वतंत्रता के साथ–साथ जिम्मेदारी भी आती है। ■■

डार्क वेब पर इस तरह खोजें अपना डेटा

डार्क वेब पर आपकी ईमेल आईडी और पर्सनल जानकारी मौजूद हैं या नहीं, इसके लिए गूगल स्कैन की मदद ली जा सकती है।

- सबसे पहले गूगल वन एप में साइन अप करें। वहीं, गूगल सर्च पर जाकर गूगल वन डार्क वेब रिपोर्ट सर्च करें।
- इसके बाद वन गूगल डॉटकाम पर जाकर डार्क वेब रिपोर्ट सेक्शन में जाकर ट्राई नाउ पर क्लिक करें।
- ऐसा करने के बाद रन स्कैन पर क्लिक करें।
- ऐसा करने के बाद डार्क वेब पर जो भी डेटा होगा, वो सामने आ जाएगा। व्यू ऑल रिजल्ट पर जाकर डेटा लीक की सारी जानकारी सामने आ जाएगी।

मिलेंगे, तो वे उन तस्वीरों को सार्वजनिक कर देंगे।

2. वेबकैम हैकिंग

अपराधी वेबकैम हैक करके पीड़ित की निजी वीडियो रिकॉर्ड कर लेते हैं। फिर वे उस वीडियो को लेकर पीड़ित को ब्लैकमेल करते हैं और पैसे की मांग करते हैं।

3. सोशल मीडिया पर फंसाना

अपराधी सोशल मीडिया पर पीड़ित को लुभावने मैसेज भेजते हैं और उन्हें निजी तस्वीरें भेजने के लिए प्रेरित करते हैं। एक बार तस्वीरें मिलने के बाद, वे पीड़ित को धमकी देते हैं कि अगर उनकी मांग पूरी नहीं हुई, तो वे उन तस्वीरों को उनके दोस्तों और परिवार के साथ साझा कर देंगे।

सेक्सटॉर्शन से बचाव के उपाय

- किसी अजनबी को अपनी निजी तस्वीरें या वीडियो कभी न भेजें।
- सोशल मीडिया पर अपनी प्राइवेसी सेटिंग्स को मजबूत रखें।
- अगर आप सेक्सटॉर्शन का शिकार होते हैं, तो तुरंत पुलिस से संपर्क करें और मदद लें। ■■

सेक्सटॉर्शन में पीड़ित को शर्मिंदा होने की जरूरत नहीं है। यह अपराधी की गलती है, पीड़ित की नहीं।

डिजिटल अरेस्ट

साइबर ठगी का नया जाल

2024 में, भारत को डिजिटल गिरफ्तारी धोखाधड़ी से सिर्फ पहले चार महीनों में ही 1,777 करोड़ रूपये का नुकसान हुआ। कर्नाटक में सबसे ज्यादा कुल 641 मामले दर्ज किए गए और 109 करोड़ रूपये का नुकसान हुआ। महाराष्ट्र और उत्तर प्रदेश ने भी बड़े पैमाने पर वित्तीय नुकसान झेला।

तेजी से बढ़ती डिजिटल दुनिया में साइबर ठगी के मामले भी हो रहे हैं और इनमें सबसे खतरनाक डिजिटल अरेस्ट स्कैम है। यह सामान्य साइबर धोखाधड़ी से अलग है क्योंकि इसमें अपराधी खुद को कानून प्रवर्तन अधिकारी बताकर लोगों को डराते हैं और उनसे पैसे या संवेदनशील जानकारी हासिल करने की कोशिश करते हैं।

डिजिटल अरेस्ट एक साइबर धोखाधड़ी की तकनीक है जिसमें ठग लोगों पर झूठे आरोप लगाकर उन्हें डराते हैं और उनसे पैसे वसूली करने की कोशिश करते हैं। ये ठग खुद को कस्टम, इनकम टैक्स विभाग या किसी अन्य जांच एजेंसी का अधिकारी बताते हैं। उनका मकसद आपको डराकर पैसे निकलवाना होता है।

यह स्कैम कैसे काम करता है ?

1. ठग पीड़ित को फोन करके खुद को किसी सरकारी एजेंसी का अधिकारी बताते हैं।
2. वे पीड़ित से वीडियो कॉल (WhatsApp,Skype आदि) पर बात करने को कहते हैं।
3. वीडियो कॉल में वे पीड़ित को डिजिटल अरेस्ट वारंट दिखाकर धमकाते हैं, जिसमें कर चोरी, मनी लॉन्ड्रिंग या अन्य अपराध का झूठा आरोप होता है।
4. कुछ मामलों में, वे नकली पुलिस स्टेशन या सरकारी कार्यालय का सेटअप दिखाते हैं ताकि पीड़ित को लगे कि कॉल असली है।
5. वे पीड़ित को कहते हैं कि नाम साफ करने, जांच में मदद करने या जमानत राशि भरने के लिए बैंक अकाउंट या UPI के जरिए पैसे ट्रांसफर करें।
6. जैसे ही पैसे ट्रांसफर होते हैं, ठग गायब हो जाते हैं और पीड़ित को आर्थिक नुकसान के साथ पहचान की चोरी (Identity Theft) जैसी समस्याओं का भी सामना करना पड़ सकता है।

डिजिटल अरेस्ट स्कैम से कैसे बचें ?

- ☞ किसी भी ऐसे कॉल से सतर्क रहें, जिसमें कोई खुद को सरकारी अधिकारी बताकर आप पर आरोप लगाए।
- ☞ असली सरकारी अधिकारी कभी भी फोन पर पैसे या बैंक डिटेल्स नहीं मांगते।
- ☞ साइबर अपराधी आपको डराने और जल्दी पैसे ट्रांसफर करने का दबाव डाल सकते हैं –ऐसी चालों में न फँसें।
- ☞ अगर किसी कॉल पर शक हो तो संबंधित सरकारी विभाग से सीधे संपर्क करें और जानकारी सत्यापित करें।
- ☞ अपने बैंकिंग व व्यक्तिगत जानकारी किसी अनजान व्यक्ति से साझा न करें। आधार नंबर, बैंक डिटेल्स या OTP किसी को न बताएं।
- ☞ किसी भी संदिग्ध कॉल या संदेश की शिकायत www-sancharsaathi.gov.in/sfc/ पर करें।
- ☞ सरकारी एजेंसियां आधिकारिक कार्यों के लिए WhatsApp Skype जैसे प्लेटफॉर्म का उपयोग नहीं करतीं।
- ☞ अगर आपको लगे कि आप ठगी के शिकार हो रहे हैं, तो तुरंत साइबर अपराध की रिपोर्ट करने के लिए 1930 पर कॉल करें या www.cybercrime.gov.in पर जाएं।

अगर आप ठगी के शिकार हो गए हैं तो क्या करें ?

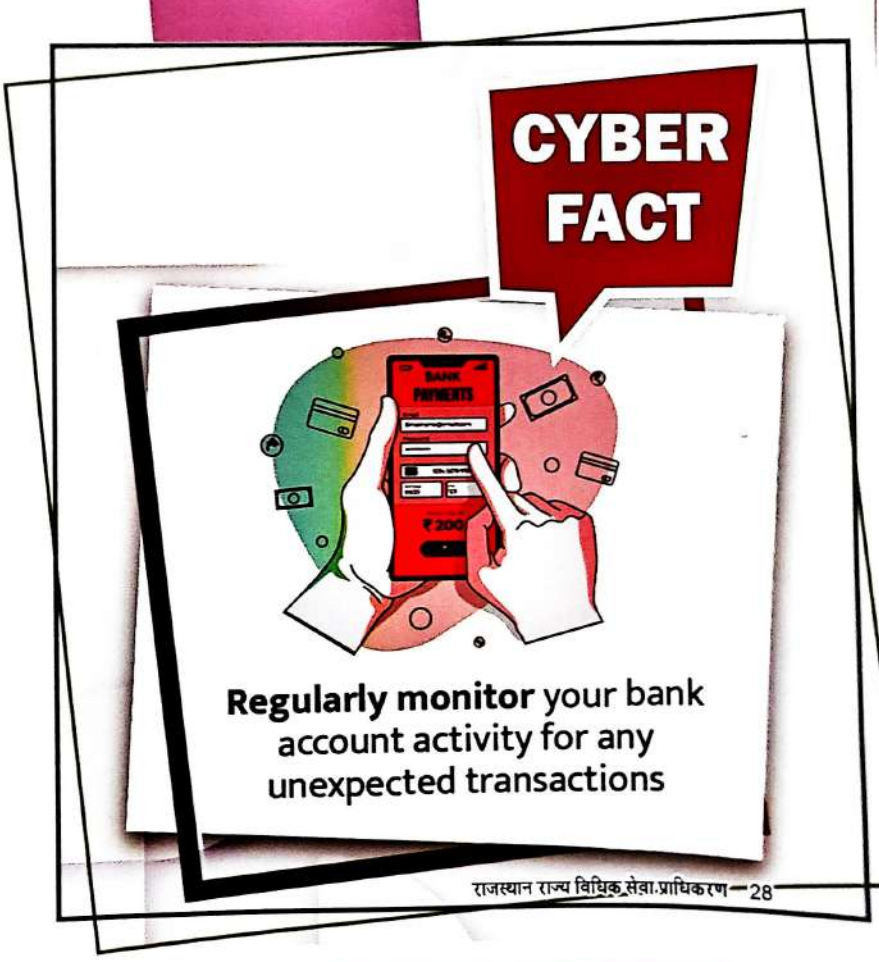
- ➲ तुरंत अपने बैंक को सूचित करें और अपने खाते को फ्रीज करवाएं।
- ➲ राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल www.cybercrime.gov.in पर शिकायत दर्ज करें।
- ➲ कॉल रिकॉर्डिंग, बैंक ट्रांजैक्शन और मैसेज जैसी सभी सबूतों को सुरक्षित रखें।
- ➲ अगर जरूरत पड़े तो किसी कानूनी सलाहकार की मदद लें।

आपको IVR कॉल आए और उसमें ऑटोमेटिक वॉइस बताए कि आपका पार्सल रिटर्न हो गया है, इसलिए 9 दबाएं जिस पर एक व्यक्ति आपसे संपर्क करेगा और आपकी जानकारी लेकर कहेगा कि पार्सल में ड्रग्स, पासपोर्ट जैसी अवैध चीजें हैं और आपके खिलाफ FIR दर्ज है। फिर वह आपको साइबर क्राइम पुलिस से जोड़ने का दावा करेगा और आप के खिलाफ गिरफ्तारी वारंट जारी होने का कह कर आपको डिजिटल अरेस्ट होने के लिए उकसाएगा।

डर और घबराहट में आप मामले को सुलझाने के लिए उसकी बात मान लेते हैं। वह आपको स्काइप या किसी अन्य ऐप पर जोड़कर नियम बताएगा– कॉल डिस्कनेक्ट नहीं कर सकते, बाहर नहीं जा सकते, किसी को बता नहीं सकते। और वह कानूनी सजा का भय दिखा कर बैंक से पैसे ट्रांसफर करवाने की मांग करेगा।

डिजिटल अरेस्ट एक धोखा है!
भारतीय कानून में डिजिटल अरेस्ट जैसी कोई भी कानूनी प्रक्रिया मौजूद नहीं है।

सतर्क रहें, पुलिस को सूचित करें।



बच्चों को ऑनलाइन गेम्स और लाइव चैट में सुरक्षित कैसे रखें?

डिजिटल युग में बच्चे कई प्रकार की चुनौतियों और खतरों का सामना करते हैं, जिनमें गोपनीयता संबंधी चिंताएँ,अयोग्य सामग्री के संपर्क में आना,धोखाधड़ी,और बाल शोषण (चाइल्ड ग्रूमिंग)शामिल हैं। हालाँकि साइबर सुरक्षा सुनिश्चित करने के लिए कई उपाय मौजूद हैं, लेकिन केवल तकनीक बच्चों को इन खतरों से पूरी तरह सुरक्षित नहीं रख सकती।

इक्कीसवीं सदी में एक बच्चा हर दिन कई घंटे ऑनलाइन वीडियो गेम खेलने और इंटरनेट सर्फिंग में बिताता है। इंटरनेट पर, उन्हें कई अवसरों के साथ–साथ विभिन्न प्रकार के जोखिमों का भी सामना करना पड़ता है।

विशेषज्ञता की कमी के कारण, वे डिजिटल तकनीक और इंटरनेट के उपयोग से जुड़े संभावित जोखिमों या खतरों का आकलन नहीं कर सकते। वे पूरी तरह से इन खतरों से अनजान हो सकते हैं। बच्चे अनजाने में गोपनीय जानकारी साझा कर सकते हैं और कई तरीकों से स्वयं गंभीर परिणामों में फंस सकते हैं। वे सोशल इंजीनियरिंग, साइबरबुलिंग, हैकिंग, वायरस, हानिकारक मैलवेयर, साइबर स्टॉकिंग जैसी साइबर सुरक्षा खतरों के शिकार हो सकते हैं। खोज इंजनों, ऑनलाइन मार्केटिंग और सोशल नेटवर्किंग वेबसाइटों के माध्यम से ये खतरें उन तक आसानी से पहुँच सकते हैं।

हालाँकि, किसी कंपनी की इंटरनेट उपस्थिति जितनी बढ़ती है, साइबर हमलों का जोखिम भी उतना ही अधिक होता है। अन्य किसी भी समूह की तुलना में, बच्चे इन हमलों के प्रति अधिक संवेदनशील होते हैं। कई माता–पिता यह सोचते हैं कि घर पर अपने बच्चों को इंटरनेट का उपयोग करने देना पूरी तरह सुरक्षित है। लेकिन यह सत्य नहीं है क्योंकि इंटरनेट के माध्यम से बच्चे दुनिया में कहीं भी और किसी से भी संपर्क कर सकते हैं। इसलिए साइबर फ्रॉड और ऑनलाइन खतरों से बचाव के लिए, बच्चों को जागरूक करना और उन्हें सुरक्षित रहने के उपाय सिखाना आवश्यक है।

बच्चों को कैसे हो सकता है नुकसान ?

- **ऑनलाइन गेम्स में फ्रॉड**–फर्जी लिंक्स और इन–गेम खरीदारी के माध्यम से बच्चों के अकाउंट्स हैक हो सकते हैं।

माता–पिता हेतु साइबर सुरक्षा संबंधी सुझाव

क्या करें

- ✓ सुरक्षित ब्राउजिंग और कम्प्यूटर उपयोग के बारे में अपने बच्चों के साथ खुली बातचीत करें।
- ✓ यह सुनिश्चित करें कि आपके बच्चे अगर आपको अपनी किसी समस्या के बारे में बताये तो उन्हें किसी भी प्रकार की परेशानी न हो ।
- ✓ अपने बच्चों को यह समझाये कि सारे सोशल नेटवर्किंग प्रोफाइल निजी (Private) हो।
- ✓ कंप्यूटर को हमेशा खुले स्थान में रखें एवं यह नियम बनाये कि जब भी बच्चे ऑनलाइन हो तो दरवाजा हमेशा खुला हों।
- ✓ अपने बच्चो को उन साइट से तुरंत बाहर निकलने की सलाह दें जिसमें वे अपने आप को असहज या चिंतित महसूस करते हो ।
- ✓ यदि आपको अपने बच्चे में किसी भी प्रकार का अनुचित बदलाव प्रतीत होता है तो जल्द से जल्द पुलिस से संपर्क करें।
- ✓ खुद भी सोशल मीडिया सुरक्षा के बारे में जानकारी प्राप्त करें एवं बच्चों के साथ खुली चर्चा करें।
- ✓ अपने बच्चों के फेसबुक, व्हाट्सएप एवं अन्य सोशल मीडिया पर ऑनलाइन गतिविधियों पर ध्यान दें एवं अचानक बदले व्यवहार इत्यादि पर नजर रखें।

USE UNIQUE PASSWORDS

Choose a password that is easy to remember, yet hard to guess. A phrase is great way to create a strong password that's easy to remember.

क्या ना करें

- ✓ अपने बच्चों को उन सोशल मीडिया में अकाउंट बनाने न दें जिसमें उम्र सीमा निर्धारित की गई हो एवं जिसके लिए वे योग्य न हो।
- ✓ छोटे बच्चों को अनावश्यक रूप से बिना अपनी निगरानी के गुगल ब्राउज करने की अनुमति न दें।
- ✓ बच्चों द्वारा घर पर उपयोग किए जाने वाले कम्प्यूटर पर व्यक्तिगत निगरानी सुनिश्चित करें तथा केवल किसी भी सुरक्षित सर्च इंजन या अन्य ऐसे उपकरण के हवाले न छोड़ें।
- ✓ अपने बच्चे को स्नैपचैट जैसे ऍप्स जो तुरंत पोस्ट हटा देते है, का उपयोग करने की अनुमति न दें।

- ➢ **लाइव चैट में खतरा**– लाइव चैट करने पर निजी जानकारी चोरी होने का जोखिम होता है।
- ➢ **फर्जी ऑफर्स और प्रॉमो कोड्स**– मुफ्त गेम आइटम्स के लालच में बच्चों के डिवाइस में वायरस आ सकते हैं।
- ➢ **सोशल मीडिया फ्रॉड**– फर्जी प्रोफाइल्स के जरिए बच्चों से निजी जानकारी हासिल करना।
- ➢ **फिशिंग अटैक्स**– लुभावने ऑफर्स देकर बच्चों को फर्जी लिंक्स पर क्लिक करवाना।
- ➢ **कैट फशिंग**– ऑनलाइन दोस्त बनाकर बच्चों से भावनात्मक जुड़ाव कर उनकी निजी जानकारी लेना।
- ➢ **रैंसमवेयर अटैक्स**– बच्चों के डिवाइस को लॉक कर फिरौती की मांग करना।

बच्चों को साइबर फ्रॉड से कैसे बचाएं?

- ➢ **जागरूकता फैलाएं**–बच्चों को साइबर फ्रॉड और ऑनलाइन खतरों के बारे में बताएं।
- ➢ **पेरेंटल कंट्रोल का इस्तेमाल**– बच्चों के डिवाइस पर सुरक्षा सेटिंग्स और पेरेंटल कंट्रोल ऑन करें।
- ➢ **स्ट्रॉन्ग पासवर्ड बनाएं**– बच्चों को मजबूत पासवर्ड बनाने और उसे गोपनीय रखने की सलाह दें।
- ➢ **फर्जी ऑफर्स से सावधान करें**– किसी भी अज्ञात लिंक पर क्लिक करने से पहले आपसे पूछने के लिए कहें।
- ➢ **निजी जानकारी सुरक्षित रखें**–नाम, पता, फोन नंबर, स्कूल की जानकारी किसी अजनबी से शेयर न करें।
- ➢ **सोशल मीडिया सेटिंग्स**– बच्चों के सोशल मीडिया अकाउंट्स की प्राइवेसी सेटिंग्स सुरक्षित रखें।
- ➢ **एंटीवायरस सॉफ्टवेयर**– बच्चों के डिवाइस को सुरक्षित रखने के लिए एंटीवायरस सॉफ्टवेयर इंस्टॉल करें।

ऑनलाइन दुनिया में बच्चों की सुरक्षा हमारी सबसे बड़ी जिम्मेदारी है। उन्हें साइबर फ्रॉड के खतरों से अवगत कराकर और सही ज्ञान देकर हम उन्हें सुरक्षित रख सकते हैं। याद रखें, थोड़ी सी सावधानी और जागरूकता बच्चों को ऑनलाइन खतरों से बचा सकती है।

डाटा और साइबर हाइजीन

डिजिटल युग की अमेद्य ढाल

क्या कभी सोचा है कि एक साधारण वीडियो ऐप के मालिक दुनिया के सबसे अमीर लोगों में से एक कैसे बन जाते हैं? ये ऐप न तो हवाई जहाज बनाते हैं, न ही दवाएं तैयार करते हैं, फिर भी अरबों की कमाई करते हैं। इसका कारण है – डाटा।

जब हम सोशल मीडिया ऐप्स या मुफ्त सेवाओं का उपयोग करते हैं, तो हम अनजाने में अपनी व्यक्तिगत जानकारी साझा कर देते हैं। कंपनियां हमारी पसंद–नापसंद, आदतें और व्यवहार को समझकर हमें लक्ष्य बनाती हैं। यही कारण है कि डाटा को 'नए युग का तेल' कहा जाता है।

डाटा की कीमत और प्रभाव

डाटा से हमारी सोच, भाषा, आदतें और यहां तक कि निर्णय लेने की क्षमता भी प्रभावित होती है। उदाहरण के लिए, यदि किसी बच्चे को बचपन से खेलकूद की जानकारी दी जाती है, तो वह एक खिलाड़ी बन सकता है। वहीं, अगर उसे विज्ञान की दुनिया से जोड़ा जाए, तो वह वैज्ञानिक या डॉक्टर बन सकता है।

आज का डिजिटल युग पूरी तरह से डाटा पर निर्भर है। यदि डाटा गलत हाथों में चला जाए, तो गंभीर परिणाम हो सकते हैं।

डाटा चोरी और साइबर अपराध

फ्री ऐप्स और वेबसाइट्स पर हम अपनी निजी जानकारियां साझा करते हैं, लेकिन यह जानकारी कहां जाती है?

साइबर अपराधी इस चोरी किए गए डाटा का उपयोग बैंकिंग धोखाधड़ी, पहचान की चोरी, और अन्य आपराधिक गतिविधियों के लिए कर सकते हैं। डार्क वेब पर इस डाटा को बेचा जाता है, जिससे अवैध लेन–देन किए जाते हैं।

व्यक्ति की ऑनलाइन गतिविधियों का पूरा रिकॉर्ड, चाहे वह Google हो या बोट्स, इंटरनेट पर हमेशा उपलब्ध रहता है। यह जानकारी साइबर अपराधियों के लिए एक खजाने से कम नहीं है। इसलिए डिजिटल युग में जागरूकता ही सुरक्षा की कुंजी है। साइबर हाइजीन अपनाकर आप साइबर अपराधियों के गलत इरादों को विफल कर सकते हैं।

Hari Om Attri
Member Secretary
Rajasthan State Legal Service Authority

From Courtroom to Community: A Sensitive and Socially-Oriented Judicial Approach Reshaping Rajasthan's Cyber Response

(Article by Hari Om Attri Member Secretary and co-authored by Ms. Rashmi Nawal, Deputy Secretary, Rajasthan State Legal Services Authority)

The digital revolution has transformed the way society functions. From mobile banking and online education to e-governance and digital commerce, technology has brought speed and convenience into everyday life. Yet, alongside this transformation, cyber crime has emerged as one of the most complex and fast-growing threats confronting citizens. Financial fraud, identity theft, digital impersonation, online exploitation and misuse of social media platforms now affect not only urban populations but also rural households and first-time digital users.

Rashmi Nawal
Deputy Secretary - I
Rajasthan State Legal Service Authority

In Rajasthan, a significant institutional response to this challenge has unfolded in recent weeks-beginning with a judicial pronouncement and extending into policy reform and grassroots implementation.

The Judicial Foundation

The development traces its origin to the judgment delivered by Hon'ble Mr. Justice Ravi Chirania in Adnan Haidar Bhai v. State of Rajasthan. While the matter before the Court involved allegations of serious cyber fraud, the judgment recognised that such cases are not isolated incidents but part of a broader and evolving pattern of digital crime.

The Court identified key realities:

Cyber offences are technologically sophisticated and often executed through multiple digital layers.

Funds can be transferred rapidly across accounts, making detection and recovery difficult.

Victims frequently include senior citizens, women, rural digital users and economically vulnerable individuals.

Traditional investigative frameworks require technological strengthening to effectively address such crimes.

The directions issued were constructive and systemic in nature. They focused on enhancing institutional coordination, improving technical expertise within investigative agencies, strengthening forensic infrastructure, ensuring better regulatory vigilance in banking processes, and promoting awareness among citizens.

The approach reflected a sensitive and socially oriented judicial outlook—recognising the human dimension of cyber crime and the necessity of building resilient systems to protect society.

Executive Response: Policy Commitment and Budgetary Backing

Following the judgment, the Government of Rajasthan initiated steps aligned with the directions issued. In subsequent proceedings, the Additional Chief Secretary (Home) informed that the State was taking measures to modernise infrastructure and strengthen specialised manpower for combating cyber offences. Media reports highlighted commitments relating to the appointment of subject-matter experts to assist courts in cyber-related matters and the development of modern technological facilities capable of addressing emerging digital challenges.

The seriousness of this response was further reflected in the Rajasthan Budget 2026–27, presented in the Legislative Assembly just days ago. A major announcement was the establishment of the Rajasthan Cyber Crime Control Centre (R4C).

The R4C is envisioned as a centralised, coordinated and technologically equipped hub to strengthen:

- Prevention of cyber offences.
- Real-time detection mechanisms.
- Investigation through specialised expertise.
- Coordination among cyber police stations, banks, telecom operators and digital intermediaries.

By incorporating cyber security as a defined budgetary priority, the State has moved from conceptual acknowledgment to structured fiscal commitment. Budgetary allocation ensures that infrastructure, technology and human resources are supported with necessary financial backing.

This alignment between judicial direction and executive planning reflects institutional maturity and responsiveness.

RSLSA's Initiative: Translating Policy into Citizen Protection

While policy reform strengthens the system, meaningful protection requires that assistance reaches the individual victim. In this context, the Rajasthan State Legal Services Authority (RSLSA) has undertaken a significant and structured initiative by launching a comprehensive framework for the constitution and operational mechanism of Cyber Redressal Units at State and District levels.

This initiative ensures that cyber justice does not remain abstract but becomes accessible and practical.

Objectives of the Cyber Redressal Units

The scheme aims to:

- Provide free legal aid to eligible cyber victims under Section 12 of the Legal Services Authorities Act, 1987.
- Facilitate coordination between victims, cyber police stations and financial institutions.
- Assist in fund recovery processes through proper legal channels.
- Strengthen access to justice for economically weaker and digitally inexperienced sections.
- Promote cyber safety awareness and digital literacy.
- Ensure monitoring and follow-up through structured reporting mechanisms.

Particular emphasis is placed on vulnerable groups such as rural first-time digital payment users, women, SC/ST communities, senior citizens and economically disadvantaged citizens.

State-Level Structure

At the State level, the RSLSA Cyber Redressal Unit functions as an apex coordinating body. It comprises:

- A Nodal Officer nominated by RSLSA.
- An advocate with expertise in cyber laws.
- A senior police officer from the State Cyber Crime Wing.
- A technical expert with knowledge of computer systems and NCRP portal navigation.
- Supporting administrative staff.

The State Unit supervises district-level units, conducts training programmes, organises capacity-building workshops for judicial officers and panel lawyers, and coordinates with banks, cyber cells and relevant government departments. Quarterly review meetings ensure accountability and uniformity in approach.

A State Level Cyber Crime Monitoring Committee further reviews trends, examines implementation of SOPs, and coordinates with stakeholders including police authorities, banking institutions and technical agencies.

District-Level Implementation

Each District Legal Services Authority (DLSA) has constituted a Cyber Redressal Unit headed by the Chairman of the DLSA. The district units are designed to provide immediate and practical support:

- Walk-in cyber victims are received during working hours.
- Immediate counselling is provided on urgent actions such as reporting to 1930 and blocking accounts or cards.
- Assistance is provided for filing complaints on the National Cybercrime Reporting Portal.
- Eligible victims are assigned panel lawyers within 48 hours.
- Applications for release of frozen funds are facilitated before trial courts.
- Para Legal Volunteers extend support in rural and remote areas.

Dedicated helplines are maintained to address cyber-related grievances, and confidentiality protocols are observed in sensitive cases.

Awareness and Prevention

Recognising that prevention is equally important, RSLSA has integrated awareness-building into its strategy. The scheme includes:

- Awareness camps for children, women and senior citizens.
- Preparation and distribution of concise booklets on cyber safety.
- Dissemination of information through television, radio, social media and digital platforms.

Mobile legal clinics for rural outreach.

Collaboration with the State Government to incorporate cyber safety modules in school education.

These measures aim to build informed digital participation and reduce fear associated with online transactions.

The appreciation for this comprehensive and proactive implementation drive is rightly attributed to the vision and guidance of Hon'ble Mr. Justice Sanjeev Prakash Sharma, Acting Chief Justice and Executive Chairman, RSLSA. Under his leadership, RSLSA has ensured that legal services evolve in response to contemporary digital challenges and extend beyond conventional litigation to preventive and community-based support.

A Coherent Institutional Response

When viewed in totality, Rajasthan's evolving cyber response reflects three interconnected dimensions:

1. A socially sensitive judicial approach identifying systemic needs.
2. An executive commitment demonstrated through administrative action and budgetary allocation for R4C.
3. A proactive legal services framework ensuring victim assistance, awareness and structured coordination at the grassroots level.

This coordinated response strengthens public confidence in institutional preparedness. It demonstrates that as society embraces digital advancement, governance structures are adapting with equal seriousness and foresight.

From judicial recognition of systemic challenges to policy reform and community-level implementation, Rajasthan's model represents a balanced and comprehensive approach—ensuring that digital progress is accompanied by digital protection, and that justice extends meaningfully from principle to practice

DATA IS WORTH GOLD TO CRIMINALS

Make privacy your priority

साइबर हाइजीन क्यों महत्वपूर्ण है ?

ऑनलाइन सुरक्षा सुनिश्चित करता है – साइबर हाइजीन के जरिए अपने डिजिटल डिवाइस, व्यक्तिगत जानकारी और डेटा को सुरक्षित रख सकते हैं। इससे साइबर अपराधियों द्वारा की जाने वाली धोखाधड़ी, हैकिंग और डेटा चोरी से बचा जा सकता है।

फिशिंग और मालवेयर हमलों से बचाव– साइबर अपराधी ईमेल, फर्जी वेबसाइट और संदिग्ध लिंक के माध्यम से हमारे सिस्टम में वायरस और मालवेयर डाल सकते हैं। अच्छी साइबर हाइजीन का पालन करके हम इन खतरों से बच सकते हैं।

पासवर्ड सुरक्षा को मजबूत करता है– मजबूत पासवर्ड का उपयोग करना, नियमित रूप से पासवर्ड बदलना और टू–फैक्टर ऑथेंटिकेशन (2FA) लागू करना साइबर हमलों से बचने में मदद करता है।

वित्तीय धोखाधड़ी से सुरक्षा

ऑनलाइन बैंकिंग, डिजिटल पेमेंट और ई–कॉमर्स वेबसाइटों पर सुरक्षित लेन–देन करने के लिए साइबर हाइजीन का पालन करना जरूरी है। इससे वित्तीय धोखाधड़ी और फ्रॉड से बचा जा सकता है।

व्यक्तिगत गोपनीयता की रक्षा करता है

सोशल मीडिया पर ओवरशेयरिंग और असुरक्षित नेटवर्क का उपयोग हमारी गोपनीयता को खतरे में डालता है। साइबर हाइजीन अपनाकर व्यक्तिगत जानकारी को सुरक्षित रख सकते हैं। ■■

साइबर हाइजीन के सर्वोत्तम उपाय

- ☑ मजबूत और अद्वितीय पासवर्ड का उपयोग करें।
- ☑ मल्टी–फैक्टर ऑथेंटिकेशन (MFA) सक्षम करें।
- ☑ सॉफ्टवेयर और सिस्टम को नियमित रूप से अपडेट करें।
- ☑ महत्वपूर्ण डेटा का नियमित बैकअप लें।
- ☑ एंटीवायरस और एंटीमैलवेयर सॉफ्टवेयर इंस्टॉल और अपडेट करें।
- ☑ फिशिंग हमलों से सतर्क रहें, संदिग्ध ईमेल और लिंक पर क्लिक न करें।
- ☑ वाई–फाई नेटवर्क को सुरक्षित करें और WPA2/WPA3 एन्क्रिप्शन का उपयोग करें।
- ☑ कर्मचारियों को साइबर सुरक्षा प्रशिक्षण दें।
- ☑ संवेदनशील डेटा को एन्क्रिप्ट करें।
- ☑ फायरवॉल का उपयोग करें, ताकि अनधिकृत पहुंच को रोका जा सके।
- ☑ अपनी प्रोफाइल प्राइवेसी सेटिंग्स को समय–समय पर जांचें और केवल विश्वसनीय लोगों के साथ ही जानकारी साझा करें।
- ☑ अनजान वेबसाइटों से डाउनलोड करने से बचें और केवल आधिकारिक स्रोतों से ही सॉफ्टवेयर इंस्टॉल करें।
- ☑ अनावश्यक रूप से सार्वजनिक वाई–फाई (जैसे रेलवे स्टेशन, कैफे आदि) का उपयोग करने से बचें, और यदि उपयोग करना आवश्यक हो तो VPN (Virtual Private Network) का इस्तेमाल करें।
- ☑ लैपटॉप, मोबाइल और अन्य डिवाइसेस में मजबूत पासवर्ड और ऑटो–लॉक फीचर का उपयोग करें।

साइबर क्राइम कानून और सजा

कानून सख्त है, लेकिन सुरक्षा की जिम्मेदारी भी जरूरी है। हर ऑनलाइन कदम सोच–समझकर उठाएं, क्योंकि कानून कार्रवाई करता है, लेकिन सावधानी ही सबसे बेहतर बचाव है!

डिजिटल युग में साइबर अपराध तेजी से बढ़ रहे हैं। इंटरनेट और डिजिटल तकनीक के व्यापक उपयोग के कारण साइबर अपराधी नए–नए तरीके अपनाकर अपराध कर रहे हैं। भारत में साइबर अपराधों को रोकने और नियंत्रित करने के लिए सूचना प्रौद्योगिकी अधिनियम, 2000 (IT Act, 2000) लागू किया गया है। इसके अलावा, डिजिटल पर्सनल डेटा प्रोटेक्शन एक्ट, 2023 (DPDP Act, 2023) भी डेटा सुरक्षा को सुनिश्चित करने के लिए एक महत्वपूर्ण कानून है।

भारत में साइबर अपराधों के लिए प्रमुख कानून

1. सूचना प्रौद्योगिकी अधिनियम, 2000 (IT Act, 2000)

भारत में साइबर अपराधों से निपटने के लिए यह प्रमुख कानून है। इसे 2008 में संशोधित किया गया था ताकि साइबर अपराधों, जैसे साइबर आतंकवाद, डेटा सुरक्षा, और ऑनलाइन धोखाधड़ी को कवर किया जा सके। यह अधिनियम इलेक्ट्रॉनिक संचार के माध्यम से किए गए अपराधों के लिए कानूनी ढांचा प्रदान करता है।

2. डिजिटल पर्सनल डेटा प्रोटेक्शन एक्ट, 2023 (DPDP Act, 2023)

यह अधिनियम नागरिकों के डिजिटल डेटा की सुरक्षा सुनिश्चित करता है और डेटा उल्लंघन की स्थिति में सख्त दंड का प्रावधान करता है।

3. भारतीय न्याय संहिता (BNS) और अन्य कानून

आईटी अधिनियम के अलावा, साइबर अपराधों को भारतीय न्याय संहिता (BNS) और धन शोधन निवारण अधिनियम (PMLA) के तहत भी दंडनीय बनाया गया है।

आईटी अधिनियम, 2000 के तहत साइबर अपराध और सजा

- **धारा 43**–कंप्यूटर सिस्टम को नुकसान पहुंचाना–3 साल तक की जेल या 5 लाख तक जुर्माना
- **धारा 66**–कंप्यूटर हैकिंग–3 साल तक की जेल या 2 लाख तक जुर्माना
- **धारा 66B**–चोरी हुए कंप्यूटर संसाधन का उपयोग–3 साल तक की जेल या 1 लाख तक जुर्माना
- **धारा 66C**–पहचान की चोरी–3 साल तक की जेल या 1 लाख तक जुर्माना
- **धारा 66D**–ऑनलाइन धोखाधड़ी 3 से 7 साल की जेल और 10 लाख तक जुर्माना
- **धारा 67**–इलेक्ट्रॉनिक माध्यम से अश्लील सामग्री प्रसारित करना–5 साल तक की जेल और 10 लाख तक जुर्माना
- **धारा 66F**–साइबर आतंकवाद–आजीवन कारावास
- **धारा 72**–गोपनीयता उल्लंघन– 2 साल तक की जेल या 1 लाख तक जुर्माना

डिजिटल पर्सनल डेटा प्रोटेक्शन एक्ट, 2023 के तहत दंड

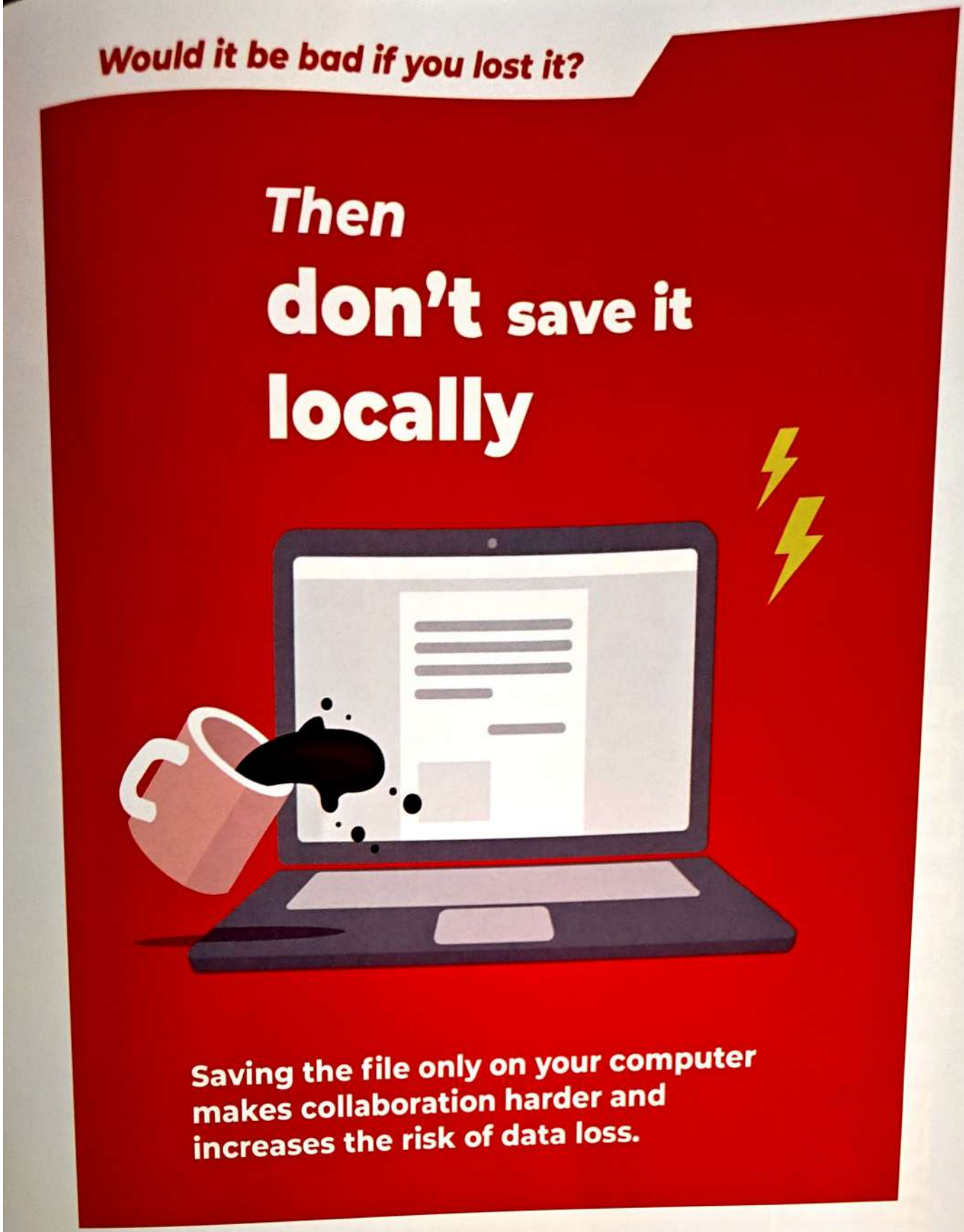
- **डेटा उल्लंघन**–250 करोड़ रूपये तक का जुर्माना
- **अवैध डेटा प्रोसेसिंग**–सख्त दंड और कानूनी कार्रवाई
- **नागरिकों के डेटा अधिकारों का उल्लंघन**– कड़ी सजा और वित्तीय दंड

भारतीय न्याय संहिता (BNS) के तहत साइबर अपराध और दंड

- **धारा 316, 317**–ऑनलाइन धोखाधड़ी–7 साल तक की जेल और जुर्माना
- **धारा 329, 330**– ई–मेल फॉर्जरी–2–7 साल की जेल
- **धारा 353, 354**–साइबर बुलिंग और धमकी–2 साल की जेल और जुर्माना

साइबर अपराधों से निपटने की दिशा में सरकार के प्रयास

सरकार द्वारा 'राष्ट्रीय साइबर सुरक्षा नीति, 2013 जारी की गई जिसके तहत सरकार ने अति–संवेदनशील सूचनाओं के संरक्षण के लिये



'**राष्ट्रीय अतिसंवेदनशील सूचना अवसंरचना संरक्षण केंद्र** (National Critical Information Infrastructure protection centre-NCIIPC) का गठन किया।

विभिन्न स्तरों पर सूचना सुरक्षा के क्षेत्र में मानव संसाधन विकसित करने के उद्देश्य से सरकार ने **'सूचना सुरक्षा शिक्षा और जागरूकता'** (Information Security Education and Awareness: ISEA) परियोजना प्रारंभ की है।

सरकार द्वारा **कंप्यूटर इमरजेंसी रिस्पॉन्स टीम** (CERT-In) की स्थापना की गई जो कंप्यूटर सुरक्षा के लिये राष्ट्रीय स्तर की मॉडल एजेंसी है।

देश में साइबर अपराधों से समन्वित और प्रभावी तरीके से निपटने के लिए **साइबर स्वच्छता केंद्र** भी स्थापित किया गया है। यह इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय (Ministry of Electronics and Information Technology-MeitY के तहत भारत सरकार की **डिजिटल इंडिया मुहिम** का एक हिस्सा है।

भारत सूचना साझा करने और साइबर सुरक्षा के संदर्भ में सर्वोत्तम कार्य प्रणाली अपनाने के लिये अमेरिका, ब्रिटेन और चीन जैसे देशों के साथ समन्वय कर रहा है। अंतर–एजेंसी समन्वय के लिये **'भारतीय साइबर अपराध समन्वय केंद्र'** (Indian Cyber Crime Co-ordination Centre-I4C) की स्थापना की गई है।

साइबर धोखाधड़ी की रिपोर्ट कैसे और कहाँ करें?

डिजिटल युग में साइबर धोखाधड़ी का शिकार होने पर त्वरित और सही कदम उठाना आवश्यक है।

1. निकटतम पुलिस स्टेशन पर जाएं

यदि आप साइबर धोखाधड़ी का शिकार होते हैं, तो सबसे पहले अपने निकटतम पुलिस स्टेशन पर जाकर शिकायत दर्ज करें। पुलिस आपकी शिकायत को आवश्यकतानुसार साइबर क्राइम सेल को संदर्भित करेगी।

2. राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल पर ऑनलाइन शिकायत दर्ज करें

भारत सरकार ने साइबर अपराधों की रिपोर्टिंग के लिए राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल स्थापित किया है। इस पोर्टल पर आप ऑनलाइन शिकायत दर्ज कर सकते हैं–

- पोर्टल का लिंक: https://cybercrime.gov.in

इस पोर्टल में दो मुख्य सेक्शन हैं–

- **महिला और बच्चों से संबंधित अपराधों की रिपोर्टिंग**– यहाँ आप गुमनाम रूप से भी शिकायत दर्ज कर सकते हैं।
- **अन्य साइबर अपराधों की रिपोर्टिंग**– वित्तीय धोखाधड़ी, हैकिंग, डेटा चोरी आदि की शिकायतें यहाँ दर्ज की जा सकती हैं।

3. साइबर क्राइम हेल्पलाइन नंबर पर कॉल करें

त्वरित सहायता के लिए राष्ट्रीय साइबर क्राइम हेल्पलाइन नंबर पर कॉल करें–

- हेल्पलाइन नंबर: 1930

यह टोल–फ्री नंबर है, जहाँ साइबर धोखाधड़ी से संबंधित शिकायत दर्ज की जा सकती हैं।

4. CERT-IN से संपर्क करें

भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-IN) साइबर सुरक्षा से संबंधित घटनाओं की निगरानी करता है। किसी भी संदिग्ध गतिविधि या अवांछित व्यवहार की रिपोर्ट की जा सकती हैं–

- ईमेल: incident@cert-in.org.in
- हेल्पडेस्क: +91 1800 11 4949

रिपोर्ट करते समय निम्नलिखित जानकारी प्रदान करें–

- घटना का समय
- प्रभावित सिस्टम / नेटवर्क की जानकारी
- देखे गए लक्षणों की जानकारी

5. खोए या चोरी हुए मोबाइल फोन की रिपोर्ट करें

मोबाइल फोन खोने पर या चोरी होने पर निम्नलिखित कदम उठाएँ–

1. पुलिस में प्राथमिकी (FIR) दर्ज करें; अपने निकटतम पुलिस स्टेशन में जाएं और घटना की रिपोर्ट करें।
2. दूरसंचार विभाग (DoT) को सूचित करें; FIR दर्ज करने के बाद, दूरसंचार विभाग के हेल्पलाइन नंबर 14422 पर कॉल करें या केंद्रीय उपकरण पहचान रजिस्टर (CEIR) पोर्टल पर ऑनलाइन शिकायत दर्ज करें।

सत्यापन के बाद, DoT फोन को ब्लैकलिस्ट कर देगा, जिससे उसका दुरुपयोग रोका जा सकेगा। यदि कोई व्यक्ति नया सिम कार्ड लगाकर डिवाइस का उपयोग करने की कोशिश करता है, तो सेवा प्रदाता नया उपयोगकर्ता पहचानकर पुलिस को सूचित करेगा।

संचार साथी पोर्टल

संचार साथी पोर्टल भारत सरकार द्वारा शुरू किया गया एक ऑनलाइन प्लेटफॉर्म है, जिसे दूरसंचार विभाग (DoT) ने विकसित किया है। यह पोर्टल नागरिकों को मोबाइल फोन सुरक्षा और साइबर धोखाधड़ी से बचाने में मदद करता है।

संचार साथी पोर्टल की मुख्य विशेषताएँ–

1. CEIR (Central Equipment Identity Register)

- यदि मोबाइल चोरी या गुम हो जाता है, तो इस पोर्टल पर जाकर उसका IMEI नंबर ब्लॉक कर सकते हैं ताकि कोई और उसका इस्तेमाल न कर सके।
- यदि फोन मिल जाता है, तो IMEI को अनब्लॉक भी कर सकते हैं।

2. Know Your Mobile (KYM) सुविधा

- यह किसी भी मोबाइल फोन के IMEI नंबर की सत्यता जांचने में मदद करता है।
- इससे यह पता कर सकते हैं कि फोन असली है या नकली।
- IMEI की जांच पोर्टल, SMS या KYM ऐप के माध्यम से की जा सकती है।

3. Telecom Analytics for Fraud Management and Consumer Protection (TAFCOP)

- यह सुविधा यह जानने में मदद करती है कि आपके आधार कार्ड से कितने मोबाइल नंबर जुड़े हुए हैं।
- यदि कोई अनधिकृत सिम जारी किया गया है, तो उसे रिपोर्ट कर सकते हैं और उसे बंद करा सकते हैं।

संचार साथी पोर्टल का उपयोग कैसे करें ?

1. फोन खो जाने पर IMEI ब्लॉक करें–

- संचार साथी पोर्टल पर जाएं।
- (CEIR) सेक्शन में जाएं और "Block Stolen/Lost Mobile" विकल्प चुनें।
- FIR कॉपी और मोबाइल बिल अपलोड करें।
- अनुरोध दर्ज करने के बाद आपको एक रिपोर्ट आईडी मिलेगी, जिससे आप स्थिति ट्रैक कर सकते हैं।

2. IMEI नंबर चेक कर–

- IMEI नंबर प्राप्त करने के लिए अपने फोन में *#06# डायल करें।
- KYM पोर्टल पर IMEI दर्ज करें और सत्यापन करें।
- SMS द्वारा जांचने के लिए "KYM <IMEI नंबर>" 14422 पर भेजें।

अपने आधार से जुड़े सिम नंबर जांचें (TAFCOP सेवा)–

- पोर्टल पर TAFCOP सेक्शन खोलें।
- अपना मोबाइल नंबर दर्ज करें और OTP से लॉगिन करें।
- आपके नाम पर जारी सभी सिम नंबरों की सूची दिखाई देगी।
- किसी भी अनजान नंबर को रिपोर्ट कर उसे निष्क्रिय करने का अनुरोध करें।

संदिग्ध धोखाधड़ी संचार की रिपोर्ट करें (चक्षु सुविधा)

किसी संदिग्ध कॉल, एसएमएस, या व्हाट्सएप संदेश के माध्यम से साइबर धोखाधड़ी का संदेह होने पर 'चक्षु' सुविधा के माध्यम से रिपोर्ट कर सकते हैं। इसमें संदेश का स्क्रीनशॉट अपलोड करना आवश्यक होता है।

सावधानी

साइबर अपराध के शिकार होने पर जल्द से जल्द कार्रवाई करें और संबंधित प्राधिकरणों को सूचित करें ताकि समय पर सहायता प्राप्त हो सके और अपराधियों के खिलाफ कड़ी कार्रवाई की जा सके।

फेसबुक या अन्य सोशल मीडिया अकाउंट संबंधित शिकायतों हेतु

- अगर कोई फर्जी फेसबुक या इंस्टाग्राम अकाउंट बन गया है तो यू.आर.एल. के साथ फर्जी प्रोफाइल का स्क्रीनशॉट ले लें या आवेदन में प्रोफाइल के यू.आर.एल. का उल्लेख करें।
- शिकायत प्रति के साथ स्व–सत्यापित पहचान पत्र संलग्न करें।

फर्जी वेबसाइट संबंधी फर्जीवाड़ा हेतु

- वेबसाइट के यू.आर.एल. के साथ नकली वेबसाइट का स्क्रीनशॉट लिया जाना चाहिए और शिकायत कॉपी के साथ जमा किया जाना चाहिए।
- धोखाधड़ी वाले लेनदेन की स्व सत्यापित प्रति, यदि कोई हो तो शिकायत प्रति के साथ संलग्न किया जाना चाहिए।

साइबर सुरक्षा के सामान्य टिप्स

अपने डिवाइस को अपडेट रखें – अपने कंप्यूटर, लैपटॉप और मोबाइल को हमेशा नए सुरक्षा अपडेट और पैच के साथ अपडेट करें।

सुरक्षा सॉफ्टवेयर का उपयोग करें – अपने सिस्टम को एंटीवायरस और अन्य सुरक्षा सॉफ्टवेयर से सुरक्षित करें और इसे समय–समय पर अपडेट करें।

सिर्फ भरोसेमंद स्रोतों से सॉफ्टवेयर डाउनलोड करें – हमेशा आधिकारिक और विश्वसनीय वेबसाइटों से ही ऐप या सॉफ्टवेयर डाउनलोड करें। पाइरेटेड सॉफ्टवेयर का उपयोग न करें।

मजबूत पासवर्ड का इस्तेमाल करें – अपने सभी डिवाइस और ऑनलाइन खातों को मजबूत पिन या पासवर्ड से सुरक्षित रखें और इसे किसी के साथ साझा न करें।

बैंकिंग जानकारी गुप्त रखें– अपने नेट–बैंकिंग पासवर्ड, ओटीपी, एटीएम पिन, सीवीवी नंबर आदि किसी से भी साझा न करें, चाहे वह बैंक अधिकारी ही क्यों न हो।

Wi-Fi को सुरक्षित रखें– अपने वाई–फाई राउटर का डिफॉल्ट पासवर्ड बदलें और एक मजबूत पासवर्ड सेट करें। नवीनतम एन्क्रिप्शन सेटिंग्स का उपयोग करें।

सार्वजनिक Wi-Fi का सावधानी से उपयोग करें– सार्वजनिक नेटवर्क का उपयोग करते समय सतर्क रहें और इनमें बैंकिंग या निजी खातों में लॉगिन करने से बचें।

नेट बैंकिंग का उपयोग करते समय सावधानी बरतें– सार्वजनिक कंप्यूटर पर नेट बैंकिंग का उपयोग करते समय वर्चुअल कीबोर्ड का उपयोग करें और काम पूरा होने के बाद ब्राउजर की हिस्ट्री हटा दें।

ईमेल अटैचमेंट खोलने से पहले स्कैन करें – किसी भी अनजान या संदिग्ध ईमेल अटैचमेंट को खोलने से पहले वायरस स्कैन जरूर करें।

पहचान प्रमाण साझा करने से पहले सोचें – अपनी निजी जानकारी केवल उन लोगों या कंपनियों के साथ साझा करें, जिनकी विश्वसनीयता सुनिश्चित हो।

मोबाइल का IMEI नंबर सुरक्षित रखें – अपने मोबाइल का IMEI नंबर नोट करके सुरक्षित स्थान पर रखें ताकि चोरी होने की स्थिति में फोन ब्लॉक या ट्रेस किया जा सके।

एटीएम उपयोग करते समय सतर्क रहें – एटीएम का इस्तेमाल करते समय अपने आस–पास नज़र रखें और स्किमिंग डिवाइस या किसी अजनबी से सतर्क रहें।

परिवार और दोस्तों को जागरूक करें – इंटरनेट सुरक्षा और साइबर अपराधों के बारे में अपने परिवार व दोस्तों से बातचीत करें और उन्हें सतर्क रहने के लिए प्रेरित करें।

ई–वॉलेट में कार्ड डिटेल सेव न करें – सुरक्षा उल्लंघन की स्थिति में धोखाधड़ी से बचने के लिए अपने कार्ड या बैंक खाता विवरण को ई–वॉलेट में स्टोर न करें।

संभावित धोखाधड़ी की सूचना दें –यदि आपको लगता है कि आपकी सुरक्षा से समझौता हुआ है, तो तुरंत संबंधित अधिकारियों को सूचित करें।

SHARING IS CARING BUT NOT ALWAYS

साइबर फ्रॉड के प्रसिद्ध मामले

जामताड़ा फिशिंग स्कैम

झारखंड के जामताड़ा जिले में कुछ युवाओं ने फिशिंग कॉल्स के जरिए हजारों लोगों को ठगा। वे बैंक अधिकारी बनकर ओटीपी पूछते और अकाउंट खाली कर देते थे। यह मामला भारत में फिशिंग स्कैम के बढ़ते खतरे को दर्शाता है।

आधार डेटा लीक मामला

आधार से जुड़ी एक बड़ी साइबर घटना में लाखों भारतीय नागरिकों की निजी जानकारी हैक कर लीक कर दी गई। इस डेटा ब्रीच के कारण गोपनीयता को लेकर गंभीर चिंताएं उठीं। इसके बाद सरकार ने डेटा सुरक्षा के उपायों को मजबूत किया और आधार तक अनधिकृत पहुंच को रोकने के लिए सख्त कदम उठाए।

कॉसमॉस बैंक हैक

पुणे के कॉसमॉस बैंक को हैकर्स ने मैलवेयर से निशाना बनाया। स्विफ्ट प्रणाली को हैक कर ₹94 करोड़ की राशि विदेशी खातों में ट्रांसफर कर दी गई। यह भारत में बैंकिंग प्रणाली पर सबसे बड़े साइबर हमलों में से एक था।

कामनवेल्थ गेम्स टिकट धोखाधड़ी

दिल्ली में हुए कॉमनवेल्थ गेम्स के दौरान साइबर अपराधियों ने एक फर्जी वेबसाइट बनाई और टिकट बुकिंग के नाम पर लोगों से पैसे वसूले। कई दर्शक नकली टिकट खरीदकर स्टेडियम के बाहर फंस गए।

पेटीएम डेटा लीक केस

पेटीएम के सीईओ विजय शेखर शर्मा को उनके ही एक कर्मचारी ने ब्लैकमेल किया। उसने कंपनी के संवेदनशील डेटा को लीक करने की धमकी देकर फिरौती मांगी थी। इस मामले ने डेटा सुरक्षा में कर्मचारियों की भूमिका पर सवाल खड़े कर दिए।

डिजिटल अरेस्ट धोखाधड़ी

साइबर अपराधी खुद को पुलिस अधिकारी बताकर डिजिटल अरेस्ट के नाम लोगों को डराकर ठगी करते हैं। वे फर्जी कानूनी नोटिस भेजते हैं और गिरफ्तार करने के लिए धमकाते है। वे कॉल, ईमेल या मैसेज के जरिए शिकार बनाते हैं।

सहारा इंडिया साइबर फ्रॉड

धोखेबाजों ने सहारा इंडिया के नाम से फर्जी वेबसाइट बनाई और निवेशकों को पैसा जमा करने के लिए कहा। हजारों लोगों से करोड़ों रुपये की ठगी की गई।

MOVIES

डिजिटल युग में, साइबर अपराध तेजी से बढ़ता हुआ खतरा बन गया है। इस विषय पर आधारित कई फिल्में और डॉक्यूमेंट्रीज बनाई गई हैं, जो न केवल मनोरंजन प्रदान करती हैं, बल्कि हमें ऑनलाइन सुरक्षा के प्रति जागरूक भी करती हैं।

सर्वेल्ड

यह डॉक्यूमेंट्री फोन सर्विलांस और स्पाइवेयर के गलत इस्तेमाल को बताती है। यह बताती है कि कैसे सरकारें पेगासस जैसे टूल्स का इस्तेमाल करके लोगों की जासूसी करती हैं। यह पत्रकारों, कार्यकर्ताओं और नेताओं की निजी जिंदगी पर पड़ने वाले असर को दिखाती है और डिजिटल निजता व सरकारी निगरानी के बीच के टकराव पर सवाल उठाती है।

बिलियन डॉलर हीस्ट

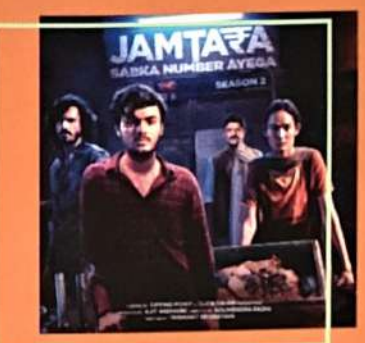
यह डॉक्यूमेंट्री बांग्लादेश बैंक पर हुए साइबर हमले पर आधारित है। हैकर्स के एक ग्रुप ने बांग्लादेश बैंक के SWIFT सिस्टम को हैक कर 1 बिलियन डॉलर ट्रांसफर करने की कोशिश की। यह रकम फिलीपींस के कसीनो, चीन और श्रीलंका के खातों में पहुंच गई और डार्क वेब के जरिए गायब कर दी गई। अमेरिका और बांग्लादेश जांच में जुटे, लेकिन हैकर्स का मास्टरमाइंड ली वेई कभी पकड़ा नहीं गया। यह चोरी आज भी रहस्य बनी हुई है।

बिगेस्ट हीस्ट एवर

यह डॉक्यूमेंट्री क्रप्टोकरेंसी एक्सचेंज हैक पर आधारित है। इसमें एक दंपति ने $4.5 बिलियन की बिटकॉइन चोरी को लांडर करने की कोशिश की। यह इतिहास की सबसे बड़ी क्रिप्टो चोरी थी। एफबीआई ने इस जोड़े को गिरफ्तार किया और उनके पास से लाखों डॉलर की क्रिप्टोकरेंसी बरामद की।

साइबर वार– हर स्क्रीन क्राइम सीन

यह वेब सीरीज मुंबई पुलिस के साइबर क्राइम डिपार्टमेंट की सच्ची घटनाओं से प्रेरित है। इसमें दिखाया गया है कि कैसे पुलिस डिजिटल अपराधों की जांच करती है और उन्हें हल करती है। हर एपिसोड एक नए साइबर अपराध जैसे हैकिंग, फिशिंग, डेटा चोरी, और ऑनलाइन फ्रॉड को उजागर करता है।



जामताड़ा–सबका नंबर आएगा

यह वेब सीरीज झारखंड के जामताड़ा जिले में होने वाले फिशिंग स्कैम पर आधारित है। कहानी में कुछ युवा लोगों को ऑनलाइन ठगने के लिए फर्जी कॉल्स करते हैं। यह डिजिटल धोखाधड़ी, साइबर क्राइम और छोटे शहर के अपराधियों की कहानी को शानदार तरीके से पेश करती है।

रेड रूम्स

यह फिल्म इंटरनेट पर होने वाले खतरनाक अपराधों की एक डरावनी और भावनात्मक कहानी दिखाती है। इसमें डार्क वेब के उन भयानक पहलुओं को उजागर किया गया है जहां गुप्त रूप से अपराध होते हैं। फिल्म दर्शाती है कि कैसे निर्दोष लोग साइबर अपराधियों का शिकार बनते हैं और इन खतरों से बचने के लिए सतर्कता जरूरी है।

हैक्ड

एक 19 वर्षीय लड़का एक बड़ी उम्र की महिला के प्रति आसक्त हो जाता है। और बदला लेने के लिए उसका डिजिटल जीवन हैक कर उसे प्रताड़ित करने लगता है। फिल्म साइबर स्टॉकिंग, निजता के उल्लंघन और डिजिटल खतरों को उजागर करती है।

NATIONAL CYBER CRIME

BANKS REPORTING PORTAL

State Bank of India- https://sbi.co.in/web/customer-care/addresses-and-helpline-nos-of-grievances-redressal-cell

NATIONALISED BANKS

Bank of Baroda- https://www.bankofbaroda.in/customer-support/grievance-redressal
Bank of India- https://www.bankofindia.co.in/forms/Grievance
Bank of Maharashtra- https://bankofmaharashtra.in/complaints_grievances
Canara Bank-https://canarabank.com/User_page.aspx?menulevel=5&menuid=5&CatID=2
Central Bank of India- https://www.centralbankofindia.co.in/en/customer_care
Indian Bank- https://www.indianbank.in/departments/online-customer-complaints/#
Indian Overseas Bank- https://www.iob.in/Grievances_Redressal_mechanism
Punjab National Bank- https://www.pnbindia.in/Lodge-Complaint.html
Union Bank of India- https://www.unionbankofindia.co.in/english/grievances-redressal.aspx
Punjab & Sind Bank- https://punjabandsindbank.co.in/content/recomp
UCO Bank- https://www.ucobank.com/english/Grievance-Redressel.aspx

INDIAN BANKS

Axis Bank Limited- https://www.axisbank.com/contact-us/grievance-redressal/retail-banking-grievance-redressal
Bandhan Bank Limited- https://bandhanbank.com/grievance-redressal
Dhanalaxmi Bank Limited- https://www.dhanbank.com/footer/grievance_redressal.aspx
Federal Bank Limited- https://www.federalbank.co.in/grievance-redressal
HDFC Bank Limited - https://leads.hdfcbank.com/applications/webforms/apply/grievance_redressal_form.asp?_ga=2.122705289.329845265.1540272882-1750795496.1540183009
ICICI Bank Limited -https://www.icicibank.com/complaints/complaints.page
IndusInd Bank Limited -https://www.indusind.com/in/en/personal/grievance-redressal.html
IDFC FIRST Bank Limited-https://www.idfcfirstbank.com/customer-service
Kotak Mahindra Bank Limited- https://www.kotak.com/en/customer-service/grievance-redressal/banking-service.html
RBL Bank Limited- GrievanceRedressalProcess.pdf (drws17a9qx558.cloudfront.net)
YES Bank Limited -https://www.yesbank.in/complaints
IDBI Bank Limited- https://www.idbibank.in/banking-complaints-i.aspx

SMALL FINANCE BANKS

Au Small Finance Bank Limited- https://www.aubank.in/support/contact-us
FINCARE Small Finance Bank Limited- https://fincarebank.com/complaints-and-grievances-form
Ujjivan Small Finance Bank Limited- https://www.ujjivansfb.in/complaint-existing-customer
Utkarsh Small Finance Bank Limited- https://www.utkarsh.bank/help-and-support

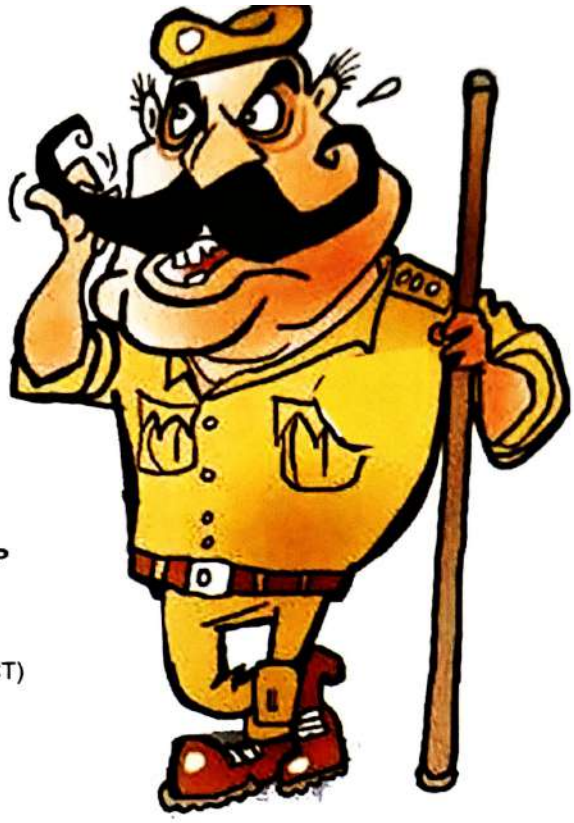
PAYMENT BANKS

Airtel Payments Bank Limited-
https://www.airtel.in/bank/static/contact-us
Paytm Payments Bank Limited-
https://www.paytmbank.com/Policies/Customer-Grievance-Redressal-Policy-for-Paytm-Payments
Jio Payments Bank Limited-
https://www.jiopaymentsbank.com/grievance-redressal

FOREIGN BANKS

Standard Chartered Bank-
https://www.sc.com/in/important-information/grievance-redressal/
Bank of America- https://bofa-india.com/contactus.html
Barclays Bank- https://www.barclays.in/home/grievance-redressal-mechanism/
American Express Banking Corp- https://icm.aexp-static.com/Internet/IntlHomepage/japa/IN_en/shared/pdfs/complaint-form.pdf?inav=in_sitefooter_company_information_complaints

CYBER POLICE STATIONS



CYBER POLICE STATION (AJMER)
AJMER (DISTRICT)
1452626026 (OFF)
sho.cyberps.ajmer@rajasthan.in

CYBER POLICE STATION (ALWAR)
ALWAR (DISTRICT)
01442990331 (OFF)
pscyber.alwar@rajpolice.gov.in

CYBER POLICE STATION (ATS & SOG)
ATS & SOG (DISTRICT)

CYBER POLICE STATION (BARAN)
BARAN (DISTRICT)

CYBER POLICE STATION (BARMER)
BARMER (DISTRICT)
2982222004 (OFF)
dysp.cybercell.barmer@rajpolice.gov.in

CYBER POLICE STATION (BHARATPUR)
BHARATPUR (DISTRICT)
56644299187 (OFF)
cyberps.bharatpur@rajpolice.gov.in

CYBER POLICE STATION (BHILWARA)
BHILWARA (DISTRICT)

CYBER POLICE STATION (BIKANER)
BIKANER (DISTRICT)
ps.cybercrimebikaner@rajpolice.gov.in

CYBER POLICE STATION (BUNDI)
BUNDI (DISTRICT)
ps.cyber.bundi@rajpolice.gov.in

CYBER POLICE STATION (BUNDI)
BUNDI (DISTRICT)
ps.cyber.bundi@rajpolice.gov.in

CYBER POLICE STATION (CHURU)
CHURU (DISTRICT)
ps.cyber.churu@rajpolice.gov.in

CYBER POLICE STATION (DAUSA)
DAUSA (DISTRICT)
ps.cyber.dausa@rajpolice.gov.in

CYBER POLICE STATION (DCP (CRIME) JODHPUR COMMISSIONERATE)
DCP (CRIME) JODHPUR COMMISSIONERATE (DISTRICT)

CYBER POLICE STATION, COMMISSIONERATE JAIPUR
DEPUTY COMMISSIONER OF POLICE - CRIME- JAIPUR COMMISSIONERATE (DISTRICT)

CYBER POLICE STATION (DUNGARPUR)
DUNGARPUR (DISTRICT)
8824101020 (OFF)
pscyber-dun-rj@gov.in

CYBER POLICE STATION (GANGA NAGAR)
GANGA NAGAR (DISTRICT)
1542948311 (OFF)
ps.cyber.sgnr@rajpolice.gov.in

CYBER POLICE STATION (HANUMANGARGH)
HANUMANGARGH (DISTRICT)
ccps-han-rj@gov.in

CYBER POLICE STATION (JAISALMER)
JAISALMER (DISTRICT)
ccpsjmr@rajpolice.gov.in

CYBER POLICE STATION (JALORE)
JALORE (DISTRICT)
cyberpsjlr@rajpolice.gov.in

CYBER POLICE STATION (JHUNJHUNU)
JHUNJHUNU (DISTRICT)
ps.cyber.jhunjhunu@rajpolice.gov.in

CYBER POLICE STATION (KARAULI)
KARAULI (DISTRICT)
ccps-kar-rj@gov.in

CYBER POLICE STATION (KOTA CITY)
KOTA CITY (DISTRICT)
ccps.kotacity@rajpolice.gov.in

CYBER POLICE STATION (NAGAUR)
NAGAUR (DISTRICT)
cyberthananagaur@rajpolice.gov.in

CYBER POLICE STATION (PALI)
PALI (DISTRICT)

CYBER POLICE STATION (PRATAPGARH)
PRATAPGARH (DISTRICT)
ps.cyber.pratapgarh@rajpolice.gov.in

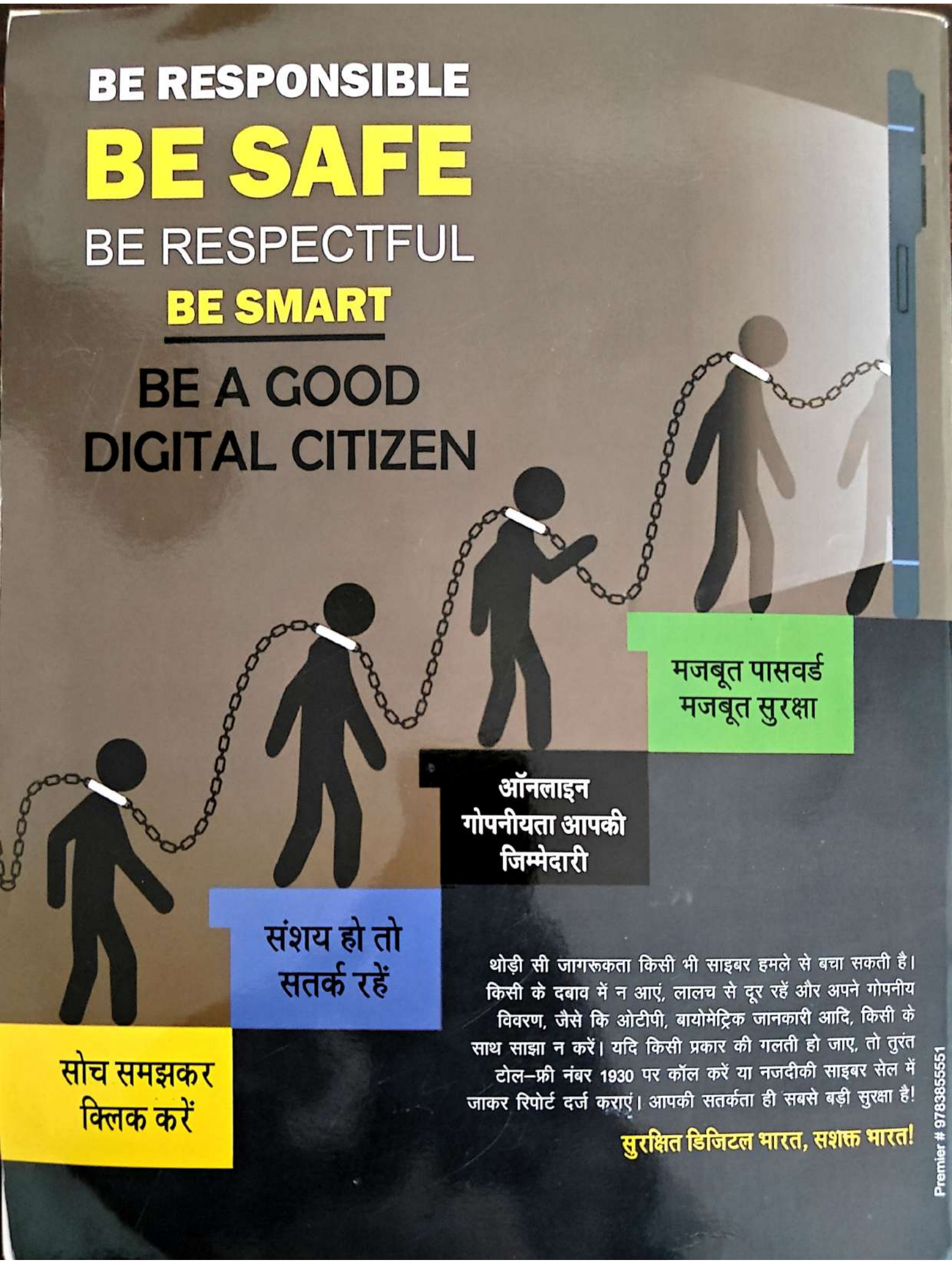
CYBER POLICE STATION (RAJSAMAND)
RAJSAMAND (DISTRICT)

DY.SP., CYBER CRIME, SAWAI MADHOPUR
SAWAI MADHOPUR (DISTRICT)

CYBER POLICE STATION (SIROHI)
SIROHI (DISTRICT)

CYBER POLICE STATION (TONK)
TONK (DISTRICT)
ps.cyberpolice.tonk@rajpolice.gov.in

CYBER POLICE STATION (UDAIPUR)
UDAIPUR (DISTRICT)
cyberpoliceudr23@rajpolice.gov.in


BE RESPONSIBLE
BE SAFE
BE RESPECTFUL
BE SMART
BE A GOOD
DIGITAL CITIZEN
मजबूत पासवर्ड
मजबूत सुरक्षा
ऑनलाइन
गोपनीयता आपकी
जिम्मेदारी
संशय हो तो
सतर्क रहें
सोच समझकर
क्लिक करें
थोड़ी सी जागरूकता किसी भी साइबर हमले से बचा सकती है। किसी के दबाव में न आएं, लालच से दूर रहें और अपने गोपनीय विवरण, जैसे कि ओटीपी, बायोमेट्रिक जानकारी आदि, किसी के साथ साझा न करें। यदि किसी प्रकार की गलती हो जाए, तो तुरंत टोल-फ्री नंबर 1930 पर कॉल करें या नजदीकी साइबर सेल में जाकर रिपोर्ट दर्ज कराएं। आपकी सतर्कता ही सबसे बड़ी सुरक्षा है!
सुरक्षित डिजिटल भारत, सशक्त भारत!
Premier # 9783855551