मोबाइल (स्मार्ट फोन) — महत्ता, आवश्यकता, हानियाँ और सावधानियाँ

लाभार्थी—
बच्चे, किशोर, युवा, प्रौढ़ और वृद्ध एवं सभी कार्यक्षेत्र / वर्ग के लोग
(कर्मचारी से लेकर अधिकारी व नेतृत्वकर्ता तक)

जोड़े रखो — सरलता से रुचिकर परोसकर
आदत बनवाओ — याद दिलाकर – पुरस्कार देकर
उपयोग करो — प्रशंसा करके प्रचारक बनाकर

एक दृष्टि में

भाग 1: मोबाइल (स्मार्ट फोन) की महत्ता और आवश्यकता

भाग 2: मोबाइल (स्मार्ट फोन) उपयोग में हानियाँ और सावधानियाँ —— (''इन्टरनेट वेब दुनिया के जाल में फँसा वर्तमान जीवन'')

भाग 3: डिजिटल सुरक्षा

भाग 4: मोबाइल (स्मार्ट फोन) उपयोग के सामाजिक / पर्यावरणीय प्रभाव

भाग 5:. विषय सम्बन्धित जिज्ञासाएँ—— प्रश्न और उत्तर

भाग 1: मोबाइल (स्मार्ट फोन) की महत्ता और आवश्यकता

1. परिचय —
   — वर्तमान समय में मोबाइल (स्मार्ट फोन) की भूमिका
   — आवश्यकताओं की सहज और सस्ती आपूर्ति से

2. मोबाइल (स्मार्ट फोन) के विभिन्न उपयोग —
   — संचार के साधन — जानकारी का आदान–प्रदान
   — शिक्षा और कार्य — डिजिटल पेमेंट्स और बैंकिंग
   — मनोरंजन

3. मोबाइल (स्मार्ट फोन) का महत्त्व —

— व्यक्तिगत जीवन में
— व्यावसायिक जीवन में
— आपातकालीन परिस्थितियों में

भाग 2: मोबाइल (स्मार्ट फोन) उपयोग में हानियाँ और सावधानियाँ —
(‘‘इन्टरनेट वेब दुनिया के जाल में फँसा वर्तमान जीवन’’)

1. शारीरिक, मानसिक और भावनात्मक स्वास्थ्य सम्बन्धी हानियाँ और सावधानियाँ

2. व्यक्तिगत, पारिवारिक और सामाजिक स्तर पर अनजाने में या लालच या भय दिखाकर उत्पीड़न या आर्थिक शोषण / दोहन और सावधानियाँ

1. शारीरिक स्वास्थ्य सम्बन्धी हानियाँ और सावधानियाँ

— आँखों पर प्रभाव

— रीढ़ की हड्डी और गर्दन पर प्रभाव

— नींद पर प्रभाव

— मस्तिष्क कोशिकाओं और सुनने की क्षमता पर प्रभाव

2. मानसिक स्वास्थ्य सम्बन्धी हानियाँ और सावधानियाँ

— बिना बताए रिकार्डिंग
— बिना बताए अप्रामाणिक Apps द्वारा रिकार्डिंग
— सोशल मीडिया की बुरी लत
— याद और ध्यान की क्षमता में कमी
— फेक न्यूज और गलत जानकारी
— साइबर फिशिंग, स्पूफिंग, बुलिंग
— साइबर फ्राड / डिजिटल अरेस्ट

3: डिजिटल सुरक्षा

- सुरक्षित पासवर्ड का उपयोग
- फिशिंग और साइबर धोखाधड़ी
- प्राइवेसी सेटिंग्स
- मोबाइल अपडेट रखें

4: मोबाइल उपयोग के सामाजिक और पर्यावरणीय प्रभाव

— सामाजिक सम्बन्धों पर प्रभाव
— ई–वेस्ट और पर्यावरणीय प्रभाव

विशेष ध्यान दें: —

5: विषय सम्बन्धित जिज्ञासाएँ— प्रश्न और उत्तर

इन्टरनेट वेब दुनिया के जाल में फँसा वर्तमान जीवन
(मोबाइल (स्मार्ट फोन) उपयोग में हानियाँ और सावधानियाँ)

1. डिवाइस और उनके प्रभाव

2. हमें मोबाइल पर लगाए रखने के लिए मोबाइल स्क्रीन के पीछे सुपर कम्प्यूटर और एल्गोरिदम (प्रोग्रामिंग) का प्रयोग

3. वेब एडिक्शन – वेब के जाल में फँसा वर्तमान जीवन
4. जीवनशैली सम्बन्धी विकार – वर्तमान स्थिति
5. समस्या को पहचानें, स्वीकार करें और हल करें

1: मोबाइल (स्मार्ट फोन) की महत्ता और आवश्यकता—

1. परिचय —

— **वर्तमान समय में मोबाइल की भूमिका:**

मोबाइल फोन हमारे जीवन का अभिन्न हिस्सा बन चुका है। इसने हमारी जीवनशैली को (दृष्टिकोण, चिन्तन, चरित्र और व्यवहार को) पूरी तरह से बदल दिया है। **कैसे**?

— **आवश्यकताओं की सहज और सस्ती आपूर्ति से:**

आज के दौर में **संचार, जानकारी और मनोरंजन** (??) की आवश्यकताओं की सहज और सस्ती आपूर्ति के लिए मोबाइल फोन अपरिहार्य हो गया है।

मनोरंजन की परिभाषा ???— शारीरिक और मानसिक स्तर पर विकास हो।

अभी प्रगति के नाम पर कुसंस्कारों को पोषण दिया जाता है।

2. मोबाइल (स्मार्ट फोन) के विभिन्न उपयोग —

— संचार के साधन:

ऑडियो/वीडियो कॉलिंग, मैसेजिंग आदि के माध्यम से लोगों से जुड़े रहने के लिए।

— जानकारी का आदान–प्रदान:

इन्टरनेट ऐक्सेस, ईमेल, न्यूज चैनल के माध्यम से वैश्विक जानकारी तक पहुँच पाने के लिए।

— शिक्षा और कार्य:

ऑनलाइन कक्षाएँ, अनुसन्धान पेपर, AI चैटबॉट से सहायता, व्यापार और ऑफिस के कार्यों के लिए उपयोग।

— डिजिटल पेमेंट्स और बैंकिंग:

ऑनलाइन शापिंग और बैंकिंग के लिए UPI, Paytm, मोबाइल वॉलेट्स के माध्यम से पैसों का आदान–प्रदान।

— मनोरंजन: (Mind distracted. Time & money wasted)

सोशल मीडिया, वीडियो, सीरियल, फिल्में, टीवी, खेल/जुआ आदि के लिए।

3. मोबाइल (स्मार्ट फोन) का महत्त्व —

— व्यक्तिगत जीवन में:

परिवार और दोस्तों से जुड़े रहने और परस्पर सेवा और सहायता (सुविधा सम्वर्धन, पीड़ा निवारण और पतन निवारण) करने का साधन।

— व्यावसायिक जीवन में:

कार्यक्षेत्र में मोबाइल के बढ़ते उपयोग
और काम को सरल बनाने में भूमिका।
AI चैटबॉट (chatgpt etc) की सहायता लेना।

— आपातकालीन परिस्थितियों में:

त्वरित सहायता प्राप्त करने
में मोबाइल की भूमिका।

2: मोबाइल (स्मार्ट फोन) उपयोग में हानियाँ और सावधानियाँ (''इन्टरनेट वेब दुनिया के जाल में फँसा वर्तमान जीवन'')

1. शारीरिक स्वास्थ्य सम्बन्धी हानियाँ और सावधानियाँ —

— **आँखों पर प्रभाव:** मोबाइल स्क्रीन के अत्यधिक उपयोग से आँखों में थकान, सूखापन और दृष्टि प्रभावित होती है।

— उपाय: उच्च गुणवत्ता के मोबाइल स्क्रीन का प्रयोग, 20–20–20 का नियम (हर 20 मिनट में 20 सेकण्ड के लिए 20 फीट दूर देखें)।

— **रीढ़ की हड्डी और गर्दन पर प्रभाव:** लगातार झुके रहने से गर्दन (सर्वाइकल स्पोंडिलोसिस—आपकी गर्दन में दर्द, चोट या अकड़न महसूस होती है।) और रीढ़ की हड्डी में दर्द हो सकता है। (back pain)

— उपाय: सही पॉश्चर (मुद्रा) में बैठें, अपने कार्य से कुछ समय का विराम लें।
शरीर को पीछे की ओर स्ट्रेच करें।

— **नींद पर प्रभाव:** रात में मोबाइल के उपयोग से नींद की गुणवत्ता पर असर — आधी–अधूरी नींद। (Blue Light Effect)

— उपाय: सोने से कम से कम एक घण्टे पहले मोबाइल का उपयोग बन्द कर दें। सोने से पहले स्वाध्याय और मंत्र लेखन करें, ऑडियो सुनें।

— **मस्तिष्क कोशिकाओं और सुनने की क्षमता पर प्रभाव:**
कम गुणवत्ता के मोबाइल/Ear buds से उच्च तीव्रता के रैडिएशन और ऊँची आवाज में सुनने के कारण।

— उपाय: SAR value मानक मात्रा से कम होना चाहिए। स्पीकर मोड या हेड फोन/वायर्ड इयर फोन का अधिक उपयोग करें।

2: मोबाइल (स्मार्ट फोन) उपयोग में हानियाँ और सावधानियाँ—

2. मानसिक स्वास्थ्य सम्बन्धी हानियाँ और सावधानियाँ—

लक्ष्य विस्मरण, चिन्तन / विवेक / निर्णय में भ्रम,

चरित्र में अशालीनता, व्यवहार में मर्यादाहीनता

— **बिना बताए रिकार्डिंग:** जाने–पहचाने या अनजाने किसी भी व्यक्ति द्वारा आपसी बातचीत (ऑडियो या वीडियो कॉल) को बिना आपको बताए रिकार्ड करना और बाद में उस रिकार्डिंग का दुरुपयोग करना।

— उपाय: अपनी व्यक्तिगत / गोपनीय बातों को मोबाइल पर करने से बचें।

सावधानी हटी, दुर्घटना घटी।

Prevention is better than cure.

— बिना बताए अप्रामाणिक Apps द्वारा रिकार्डिंग:

विभिन्न Apps को ऑडियो/वीडियो permission यूजर द्वारा स्वयं दिए जाने के कारण, उपयोगकर्ता को बिना बताए कभी–भी ऑडियो/वीडियो रिकार्डिंग की जा सकती है।

सतर्क रहें, सावधान रहें। सावधानी हटी, दुर्घटना घटी।

Prevention is better than cure.

— उपाय: केवल Google द्वारा स्वीकृत–अधिकृत Apps ही उपयोग करें। **पारिवारिक–व्यक्तिगत क्षणों में और कमरों में इन्टरनेट बन्द रखें। इन्टरनेट कम्पनियों से फ्री सुविधा मिलने के कारणों पर सोचें–विचारें।**

आपकी अपनी व्यक्तिगत गोपनीयता महत्त्वपूर्ण है।

— **सोशल मीडिया की बुरी लत:** लगातार सोशल मीडिया (Facebook etc) पर रहने से तनाव, अवसाद और आत्म–सम्मान में कमी।

— उपाय: समय की सीमा निर्धारित करें, डिजिटल डिटॉक्स करें, ज्ञानवर्धक कॉन्टेन्ट ही देखें।

— **याद और ध्यान की क्षमता में कमी:** याद रखने और ध्यान करने की समय व क्षमता दोनों में निरन्तर कमी होते जाना।

भ्रम की स्थिति बढ़ते जाना।

— उपाय: डिजिटल उपवास रखें।

जप, ध्यान, प्राणायाम, पुस्तक स्वाध्याय जैसी प्रक्रियाओं की सहायता लें।

— **फेक न्यूज और गलत जानकारी:** सोशल मीडिया और मैसेजिंग ऐप्स पर गलत जानकारी का फैलाव।

— उपाय: किसी भी जानकारी की सत्यता की जाँच करें, विश्वास योग्य स्रोतों से ही जानकारी प्राप्त करें, तभी आगे बढ़ाएँ। दूसरों का समय भी बहुत महत्त्वपूर्ण है। उनके समय का भी सम्मान करें।

— **साइबर बुलिंग:** ऑनलाइन उत्पीड़न (अभद्र–अश्लील भाषा, चित्रों, वीडियो तथा धमकियों से किसी को भी परेशान करना) **साइबर बुलिंग** कहलाता है। **साइबर बुलिंग से तात्पर्य** इन्टरनेट या मोबाइल टेक्नोलॉजी का प्रयोग करके असभ्य, घटिया या तकलीफदेह सन्देश, टिप्पणियाँ और इमेज/वीडियो भेजकर किसी को जानबूझकर तंग करना या डराना–धमकाना है। किसी साइबर बुली द्वारा दूसरों को डराने–धमकाने के लिए टेक्स्ट मैसेज, ई–मेल, सोशल मीडिया प्लेटफार्म, वेब पेज, चैट रूम आदि का प्रयोग किया जाता है।

साइबर बुलिंग के परिणाम— ये आर्थिक, शारीरिक, मानसिक और भावनात्मक दुष्परिणामों के रूप में किसी का भी दैनिक जीवन प्रभावित कर सकते हैं।

सुरक्षा उपायों का अनुपालन— जागरूकता और सावधानी से आप बिना किसी डर के इन्टरनेट और मोबाइल टेक्नोलॉजी का प्रयोग कर सकते है। आपको सतर्क होने और स्वयं को और अपने दोस्तों को साइबर बुलिंग से बचाने के लिए सुरक्षा उपायों का अनुपालन करने की जरूरत है।

बचाव— आप साइबर बुलिंग का शिकार होने से अपने आपको कैसे बचा सकते हैं?

- सोशल मीडिया प्लेटफार्म पर **अनजान व्यक्तियों की फ्रेंड रिक्वेस्ट स्वीकार न करें।** साइबर बुली अपने शिकार से दोस्ती करने के लिए जाली एकाउंट भी बना सकता है। अनुभव सिद्ध ढंग से उन्हीं लोगों को ऑनलाइन जोड़ें, जिन्हें आप ऑफ लाइन जानते हैं।

- सोशल मीडिया या अन्य ऑनलाइन प्लेटफार्म पर अपनी **निजी सूचना जैसे जन्म तिथि, पता और फोन नम्बर साझा न करें।** आपकी आनलाइन पोस्ट तक कौन पहुँच सकता है, इसके लिए आप सोशल मीडिया प्लेटफार्म पर प्राइवेसी सेटिंग में जाएँ। अपनी प्रोफाइल तक केवल आपके दोस्तों की पहुँच को ही सीमित करने का प्रयास करें। (किन्तु याद रखें सभी पोस्टों के लिए प्राइवेसी का विकल्प सभी सोशल मीडिया प्लेटफार्म प्रदान नहीं करते हैं।) उदाहरण के लिए किसी एक प्लेटफार्म पर पिक्चर, स्टोरीज बाइ–डीफाल्ट ही पब्लिक होती हैं।

- याद रखें कि आप जो भी आनलाइन पोस्ट करते है, वह वहीं रहता है, इसलिए महत्त्वपूर्ण है कि सतर्क रहें और सोशल मीडिया प्लेटफार्म पर कमेंट्स या पोस्ट में अपना फोन नम्बर और अन्य निजी ब्यौरे साझा न करें।

- कभी भी **अनजान स्रोतों से अनावश्यक साफ्टवेयर और एप्स जैसे डेटिंग एप, आनलाइन गेम आदि को इंस्टाल न करें।** चैट रूम में चैटिंग करते समय आपको विशेष रूप से सतर्क होना चाहिए। चैट रूम में अपने निजी ब्यौरे कभी साझा न करें और अपनी पहचान को सीमित करें।

- यदि किसी दोस्त या अनजान व्यक्ति की पोस्ट पढ़कर आप दुःखी महसूस करें, तो उस पर आक्रामक उत्तर न दें। इससे बुली इस प्रकार के मैसेज पोस्ट करने के लिए प्रोत्साहित होगा। यदि पीड़ा करने वाला पोस्ट/मैसेज आपके दोस्त का हो तो दोबारा ऐसा न करने का अनुरोध उससे कर सकते हैं। यदि आप बार–बार इस प्रकार के मैसेज/पोस्ट प्राप्त करते हैं, तो कृपया तत्काल **अपने माता–पिता या बड़ों या अपने किसी समझदार विश्वसनीय को इसकी जानकारी दें,** जिससे वे आपकी सहायता कर सकें।

- कृपया यह भी याद रखें कि एक अच्छा इन्टरनेट उपयोगकर्ता होने के नाते आपको घटिया कमेंट या दुःखदायी मैसेज या परेशान करने वाली पिक्चर्स / वीडियोज आनलाइन शेयर नहीं करनी चाहिए। कृपया सतर्क रहें और यह जाँच करें कि आपकी पोस्ट/कमेंट/वीडियो आपके दोस्त या किसी अन्य व्यक्ति के लिए भी परेशान करने वाली न हों। यदि ऐसा है तो कृपया पोस्ट न करें। **आपको भी साइबर बुली करने वाला** नहीं बनना चाहिए क्योंकि ऐसा करना दण्डनीय अपराध है। यह पीड़ित को प्रतिकूल रूप से प्रभावित करता है।

यदि आप साइबर बुलिंग के पीड़ित हैं तो आपको क्या करना चाहिए?

यदि आपको महसूस होता है कि आप साइबर बुलिंग के पीड़ित हैं, तो **कृपया अपने बड़ों को / अपने किसी समझदार विश्वसनीय को** अविलम्ब सूचित करें ताकि वे हस्तक्षेप कर सकें और आपकी सहायता कर सकें। निम्नलिखित सुझाव स्थिति से निपटने में सहायक हो सकते हैं।

1. तत्काल अपने माता–पिता/बड़ों/समझदार विश्वसनीय को सूचित करें—

यदि कोई आपको डरा धमका रहा है, तो तत्काल अपने माता–पिता/बड़ों/अपने किसी समझदार विश्वसनीय को सूचित करें। यह न सोचें कि वे लोग आपके आनलाइन कार्यकलापों को प्रतिबन्धित कर देंगे या आपसे कम्प्यूटर/स्मार्टफोन का उपयोग न करने के लिए कहेंगे।

उन्हें सूचित करना महत्त्वपूर्ण है **ताकि वे आपकी सहायता व मार्गदर्शन कर सकें। पूरी बात स्पष्ट रूप से आपने माता–पिता/बड़ों/समझदार विश्वसनीय को अवश्य बताएँ।**

2. बुली करने वाले की पहचान करना—

बुली की **पहचान करने की कोशिश करें** कि वह जानकार व्यक्ति है या अनजान व्यक्ति। आपको यह पता लगाने कि कोशिश करनी चाहिए कि बुली आपको क्यों परेशान कर रहा है? बुली आपका दोस्त या कोई परिचित व्यक्ति हो सकता है। आप बुली तक पहुँचने में **अपने माता–पिता/अध्यापकों/अपने किसी समझदार विश्वसनीय की मदद ले सकते हैं** और अपने आपको बुली करने से उसे रोक सकते हैं।

3. बुली करने वाले को ब्लॉक करें—

यदि बुली आपको डराने–धमकाने के लिए सोशल मीडिया प्लेटफार्म का उपयोग कर रहा है, तो आप **उसे ब्लॉक कर सकते हैं।** सभी सोशल मीडिया एप या सेवाओं में यूजर को ब्लॉक करने का विकल्प है।

4. पोस्ट/मैसेज को तिथि के अनुसार <u>कॉपी और सेव</u> करें—

आपके विरुद्ध प्रयोग किए गए पोस्ट/मेसेज सेव करें। कानूनी कार्रवाई किए जाने के मामले में, इस प्रकार के मैसेज/पोस्ट का उपयोग साक्ष्य के रूप में किया जा सकता है।

5. बुली करने वाले को कभी भी आक्रामक उत्तर न दें—

बुली करने वाला चाहता है कि आप आक्रामक हो जाएँ और आपकी उससे बहस हो। इससे अनावश्यक रूप से सूचना में फायदा होता है। इसलिए बेहतर तरीका यह है कि आप **विनम्रतापूर्वक व्यक्ति को इसे बन्द करने के लिए कहें** और यदि वह नाराज हो जाता है तो उसके साथ चैट बन्द कर दें और उसे ब्लॉक कर दें। यदि आपके माता–पिता/बड़ों को जरूरत महसूस हो तो, वे बुली के खिलाफ शिकायत करने के लिए पुलिस स्टेशन से सम्पर्क कर सकते हैं।

6. कैसे और कहाँ करें शिकायत?

साइबर बुलिंग से जुड़े मामलों में आप **राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल** **https://cybercrime.gov.in/** पर जाकर अपनी शिकायत दर्ज करा सकते हैं। महिलाएँ यहाँ पर अपनी पहचान उजागर किए बिना भी अपनी शिकायत दर्ज करा सकती हैं। पोर्टल पर आप अपनी शिकायत की स्थिति को भी जान सकते हैं।

इसके साथ ही आप अपने निकटतम थाने में स्वयं प्रस्तुत होकर अपनी शिकायत दर्ज करा सकते हैं। यदि आपको लगता है कि थाने में आपको मदद नहीं मिल पा रही है, तो आप जिले में क्राइम ब्रांच के दफ्तर में जाकर भी अपनी शिकायत दर्ज करा सकते हैं। यदि किसी ने फोटो और वीडियो अपलोड किए हैं तो शिकायत के बाद उस आईडी को ब्लॉक करने की प्रक्रिया सुनिश्चित की जा सकेगी। इसके अलावा हेल्पलाइन नंबर 1930 पर भी शिकायत दर्ज करवाई जा सकती है।

— साइबर फ्राड / डिजिटल अरेस्ट:

यह एक प्रकार की साइबर ठगी है। यह लोगों का शोषण करने के लिए एक नया और खतरनाक तरीका है। डिजिटल अरेस्ट स्कैम में फोन करने वाले कभी पुलिस, सीबीआई, नारकोटिक्स, आरबीआई और दिल्ली या मुम्बई पुलिस अधिकारी बनकर आत्मविश्वास से बात करते हैं। वॉट्सएप या स्काइप कॉल पर जब कनेक्ट करते हैं तो आपको फर्जी अधिकारी एकदम असली से लगते हैं। वे लोग पीड़ित व्यक्ति को इमोशनली और मेंटली टॉर्चर करते हैं। **यकीन दिलाते हैं कि आपके साथ या आपके परिजन के**

साथ कुछ बुरा हो चुका है या होने वाला है। सामने बैठा व्यक्ति पुलिस की वर्दी में होता है, ऐसे में ज्यादातर लोग डर जाते हैं और उनके जाल में फँसते चले जाते हैं।

साइबर फ्राड में फोन करने वाला व्यक्ति **मित्र के रूप में या अपने किसी सम्बन्धी की आवाज में** (AI Voice cloning) पैसों की तत्काल आवश्यकता बताता हुआ पैसे किसी अन्य खाते में तुरन्त देने को कहता है।

डिजिटल अरेस्ट का खेल कैसे खेला जाता है?

- अनजान नम्बर से व्हाट्सएप / स्काइप पर वीडियो कॉल आती है।
- किसी केस में फँसने या परिजन के किसी मामले में पकड़े जाने का जानकारी दी जाती है।
- धमकी देकर वीडियो कॉल पर लगातार बने रहने के लिए मजबूर किया जाता है।
- स्कैमर्स मनी लॉन्ड्रिंग, ड्रग्स का धन्धा या अन्य अवैध गतिविधियों का आरोप लगाते हैं।

- पीड़ित को परिवार या फिर किसी को भी इस बारे में कुछ न बताने की धमकी दी जाती है।
- वीडियो कॉल करने वाले व्यक्ति का बैकग्राउण्ड पुलिस स्टेशन जैसा नजर आता है।
- पीड़ित को लगता है कि पुलिस उससे ऑनलाइन पूछताछ कर रही है या मदद कर रही है।
- केस को बन्द करने और गिरफ्तारी से बचने के लिए मोटी रकम की माँगी जाती है।

डिजिटल अरेस्ट को कैसे पहचानें?

डिजिटल अरेस्ट की पहचान करने के लिए **सतर्कता की जरूरत** है। अगर आपके पास किसी अनजान नंबर से कोई फोन या वॉट्सएप कॉल आती है तो रिसीव करते वक्त मुम्बई पुलिस की एडवाइजरी को याद रखें।

मुम्बई पुलिस की एडवाइजरी—

- पुलिस अधिकारी कभी भी अपनी पहचान बताने के लिए **वीडियो कॉल नहीं करेंगे।**

- पुलिस अधिकारी कभी भी आपको **कोई एप डाउनलोड करने के लिए नहीं कहेंगे।**

- पहचान पत्र, FIR की कॉपी और गिरफ्तारी वारंट **ऑनलाइन साझा नहीं किया जाएगा।**

- पुलिस अधिकारी कभी भी **वॉयस या वीडियो कॉल पर बयान दर्ज नहीं करते हैं।**

- पुलिस अधिकारी कॉल पर **पैसे या पर्सनल जानकारी देने के लिए डराते–धमकाते नहीं हैं।**

- पुलिस कॉल के दौरान **अन्य लोगों से बात करने से नहीं रोकती है।**

- **कानून में डिजिटल अरेस्ट का कोई प्रावधान नहीं है**, क्राइम करने पर असली वाली गिरफ्तारी होती है।

(पीड़ित व्यक्ति को यह यकीन दिलाया जाता है कि वह आपराधिक गतिविधियों में शामिल है और आखिरकार उनसे बड़ी रकम ऐंठ ली जाती है। इस पूरी प्रक्रिया को बहुत ही नियोजित तरीके से अपनाया जाता है, जिससे वारदात होने के बाद पीड़ित व्यक्ति कभी अपराध की रिपोर्ट ना कर सके। फँसे हुए व्यक्ति को धमकी या लालच देकर घंटों या कई दिनों तक कैमरे के सामने बने रहने के लिए मजबूर किया जाता है जिससे वह घबराहट में अपनी कई निजी जानकारी दे देता है, जिसका इस्तेमाल कर उसके अकाउण्ट से पैसा निकालना, उसके नाम से फर्जी काम भी किए जाते हैं और कैश रकम लेना तो इसमें शामिल ही रहता है।...पूरे स्कैम की शुरुआत एक सरल मैसेज, ईमेल, या व्हाट्सऐप सन्देश से होती है. जिसमें दावा किया जाता है कि पीड़ित व्यक्ति किसी तरह की आपराधिक गतिविधियों में संलग्न है। इसके बाद उसे वीडियो या फोन कॉल करके कुछ खास प्रक्रिया से गुजरने के लिए दबाव डाला है और पुष्टि के लिए कई तरह की जानकरियाँ भी माँगी जाती हैं। ऐसे कॉल करने वाले खुद को पुलिस, नॉरकोटिक्स, साइबर सेल पुलिस, इनकमटैक्स या सीबीआई अधिकारियों की तरह पेश करते हैं। वे बाकायदा किसी ऑफिस से यूनिफॉर्म में कॉल करते हैं।)

—— उपाय: डिजिटल अरेस्ट से कैसे बचें?

<u>वीडियो हिन्दी</u>   <u>Video English</u>

प्रधानमंत्री नरेंद्र मोदी जी ने डिजिटल अरेस्ट स्कैम से बचने के लिए लोगों को **'रुको, सोचो और एक्शन लो'** की सलाह दी है। प्रधानमंत्री मोदी जी ने कहा कि ऐसे धोखाधड़ी करने वाले लोग समाज के दुश्मन हैं और नागरिकों को अपनी व्यक्तिगत जानकारी साझा नहीं करनी चाहिए।

भारतीय कम्प्यूटर आपातकालीन प्रतिक्रिया टीम (सीईआरटी–एन) ने लोगों को डिजिटल अरेस्ट से बचाने के लिए एडवाइजरी जारी की है। सीईआरटी ने बताया डिजिटल अरेस्ट से कैसे बच सकते हैं—

1. सतर्क रहे, सुरक्षित रहें— कोई भी **सरकारी जाँच एजेंसी** आधिकारिक संचार के लिए **वॉट्सएप या स्काइप जैसे प्लेटफॉर्म्स का उपयोग नहीं करतीं।** जबकि ऑनलाइन ठग इन्हीं का इस्तेमाल कर रहे हैं। शुरुआत में शक होने पर तुरन्त फोन काट दें। फोन पर लम्बी बातचीत करने से बचें।

2. इग्नोर करें— साइबर ठग डिजिटल अरेस्ट के लिए पीड़ितों को फोन कॉल, ई–मेल से सन्देश भेजते हैं। बताते हैं कि आप मनी लॉन्ड्रिंग या चोरी जैसे अपराधों के तहत जाँच के दायरे में हैं। **ऐसे किसी कॉल और ई–मेल पर ध्यान न दें।**

3. घबराएँ नहीं— साइबर ठग कॉल पर बातचीत के दौरान गिरफ्तारी या कानूनी कार्रवाई की धमकी देते हैं। उनकी बातचीत और फर्जी तर्कों से घबराहट हो सकती है, लेकिन **घबराना नहीं है। न ही बैंक डिटेल व यूपीआई आईडी शेयर करनी है।**

4. जल्दबाजी करने से बचें— कॉल या वीडियो कॉल पर ठगों के सवालों और तर्कों का जवाब देने में **जल्दबाजी न करें। शान्त रहें, सिर्फ सुनें।** अनजान नम्बरों से आए सामान्य और वीडियो कॉल पर भी कोई निजी जानकारी न दें।

5. साक्ष्य जुटाएँ— कॉल के **स्क्रीनशॉट या वीडियो रिकॉर्डिंग सेव करें** ताकि आवश्यक होने पर उपयोग कर सकें।

ट्राई मोबाइल नंबरों के सत्यापन/ डिस्कनेक्शन/ गैरकानूनी गतिविधियों की रिपोर्ट करने के लिए कभी भी कोई संदेश या कॉल नहीं भेजता है। ट्राई के नाम से आने वाले ऐसे मैसेज/कॉल से सावधान रहें। ऐसी कोई भी कॉल या संदेश संभावित रूप से धोखाधड़ी माना जाना चाहिए और इसे संचार साथी प्लेटफार्म पर चक्षु माड्यूल (https://sancharsaathi.gov.in/sfc/) के माध्यम से दूरसंचार विभाग को अथवा ग्रह मंत्रालय के साइबर क्राइम पोर्टल https://www.cybercrime.gov.in पर सूचित किया जा सकता है।

6. फिशिंग से बचें—

फ़िशिंग एक आम प्रकार का साइबर हमला है जो ईमेल, टेक्स्ट मैसेज, फ़ोन कॉल और संचार के अन्य तरीकों के ज़रिए लोगों को निशाना बनाता है। फ़िशिंग हमले का उद्देश्य प्राप्तकर्ता को हमलावर की मनचाही कार्रवाई के झाँसे में फँसाना होता है, जैसे कि वित्तीय जानकारी, सिस्टम लॉगिन क्रेडेंशियल या अन्य सम्वेदनशील जानकारी का खुलासा करना। इसमें **ठग आपके कम्प्यूटर तक पहुँचकर व्यक्तिगत जानकारी चुराते हैं।** साइबर अपराधियों के लिए इसका उपयोग करना आसान, सस्ता और प्रभावी है। साइबर अपराधियों द्वारा चुराए जाने वाले डेटा में व्यक्तिगत पहचान योग्य

जानकारी शामिल होती है – जैसे वित्तीय खाता डेटा, क्रेडिट कार्ड नंबर,और मेडिकल रिकॉर्ड – साथ ही संवेदनशील व्यावसायिक डेटा, जैसे ग्राहक नाम और संपर्क जानकारी, मालिकाना उत्पाद रहस्य और गोपनीय संचार। हमलावर भय और तात्कालिकता की भावना का फायदा उठाते हैं, तथा प्रायः ऐसी रणनीति अपनाते हैं जिसके तहत उपयोगकर्ता को बताया जाता है कि यदि वे ईमेल का जवाब नहीं देते हैं तो उनका खाता प्रतिबन्धित कर दिया गया है या निलम्बित कर दिया जाएगा।

क्या है फिशिंग हमला—

अपराधी फ़िशिंग के माध्यम से आपको **नकली ईमेल या सन्देश भेजते हैं,** जो किसी प्रतिष्ठित कम्पनी, आपकी बैंक, आपकी क्रेडिट कार्ड कम्पनी, ऑनलाइन शॉपिंग की तरह मिलते–जुलते होते हैं, अगर आप सतर्क नहीं हैं तो आप इनके झाँसे में जल्द ही आ जाते हैं। इन नकली ईमेल या सन्देश का उद्देश्य से आपकी पर्सनल आइडेंटिफाइएबल इन्फ़ॉर्मेशन को चुराना है।

पर्सनल आइडेंटिफाइएबल इन्फ़ॉर्मेशन के अन्तर्गत **आपकी निजी जानकारियाँ आती हैं जैसे –** 1. आपका नाम 2. आपकी ईमेल यूजर आई.डी. 3. आपका पासवर्ड 4. आपका मोबाइल नम्बर या फोन नम्बर 5. आपका पता 6. बैंक खाता नम्बर 7. एटीएम कार्ड, डेबिट कार्ड तथा क्रेडिट कार्ड नम्बर 8. एटीएम कार्ड, डेबिट कार्ड तथा क्रेडिट कार्ड आदि का वैलिडेशन कोड 9. आपकी जन्मतिथि

फ़िशिंग के बारे में अधिक **विस्तृत जानकारी अन्तिम पृष्ठ पर** है।

7. धोखाधड़ी को रिपोर्ट करें—

किसी भी सन्दिग्ध गतिविधि की रिपोर्ट साइबर क्राइम हेल्पलाइन 1930 या वेबसाइट cybercrime.gov.in पर तुरन्त करें।

भाग 3. डिजिटल सुरक्षा

— **सुरक्षित पासवर्ड का उपयोग:** कमजोर पासवर्ड से आपके किसी भी अकाउण्ट के हैक होने का खतरा रहता है।

— उपाय: मजबूत पासवर्ड का उपयोग करें। (8 से 10 अक्षर) कैपिटल् व स्माल अक्षरों और विशेष चिह्नों का प्रयोग करें। नियमित रूप से पासवर्ड बदलें और पासवर्ड सही से याद रखें। पासवर्ड अपने आस–पास किसी को भी न बताएँ।

— फिशिंग और साइबर धोखाधड़ी:

अनजान लिंक और ईमेल्स पर क्लिक करने से अकाउंट्स के हैक होने का खतरा।

— उपाय: किसी भी सन्दिग्ध लिंक पर क्लिक न करें, दो–स्तरीय प्रमाणीकरण का उपयोग करें। **समझदारी से काम लें। लालच और भय से बचें।**

— **प्राइवेसी सेटिंग्स:**

सोशल मीडिया पर अपनी जानकारी की सुरक्षा के लिए प्राइवेसी सेटिंग्स को सही ढंग से सेट करें।

— उपाय: नियमित रूप से अपनी प्राइवेसी सेटिंग्स की समीक्षा करें।

— **मोबाइल अपडेट रखें:**

अपडेट न होने से पुराने Apps बन्द हो सकते हैं। मोबाइल की सुरक्षा में सेंध लग सकती है।

— उपाय: मोबाइल में ऑटो अपडेट ऑन रखें और सूचित करने पर तुरन्त अपडेट करें।

4. मोबाइल उपयोग के सामाजिक और पर्यावरणीय प्रभाव

— **सामाजिक सम्बन्धों पर प्रभाव:**

मोबाइल के अत्यधिक उपयोग से **पारिवारिक और सामाजिक सम्बन्धों में दूरी और मूल्यों में कमी आ रही है।**

— उपाय:

परिवार और दोस्तों के साथ समय बिताने के लिए मोबाइल का सीमित उपयोग करें। वास्तविक जीवन जीएँ।

— ई–वेस्ट और पर्यावरणीय प्रभाव:

मोबाइल उपकरणों का उचित निस्तारण न होने से पर्यावरण को नुकसान।

— उपाय: ई–वेस्ट का सही तरीके से निस्तारण करें। जब तक आवश्यक न हो, नया मोबाइल न खरीदें।

विशेष ध्यान दें: —

— ध्यान रखें कि मोबाइल एक उपयोगी उपकरण है, लेकिन इसके **जिम्मेदार उपयोग के बिना** इसके नकारात्मक प्रभाव भी हो सकते हैं / **हो रहे हैं।**

— अपने और अपने परिवार की सुरक्षा के लिए **समझदारी से काम लें। हमेशा सतर्क रहें। लालच (पैसा और वासना–काम भाव) और भय से बचें। तकनीक का सही तरीके से उपयोग करें।** जिस App की जब जरूरत हो, उसे उसी समय उपयोग करके बन्द कर दें।

भाग 5. विषय सम्बन्धित जिज्ञासाएँ, प्रश्न और उत्तर—

यदि आपके कोई प्रश्न, जिज्ञासा या सुझाव हों तो हमें बेझिझक बताएँ।

भाग 2: मोबाइल उपयोग में हानियाँ और सावधानियाँ—

फ़िशिंग तकनीक— साइबर अपराधी जानकारी चुराने के लिए **तीन प्राथमिक फ़िशिंग तकनीकों का उपयोग** करते हैं:

दुर्भावनापूर्ण वेब लिंक,

दुर्भावनापूर्ण अनुलग्नक और

धोखाधड़ीपूर्ण डेटा–प्रविष्टि फ़ॉर्म।

दुर्भावनापूर्ण वेब लिंक— फ़िशिंग लिंक उपयोगकर्ताओं को जालसाज़ वेबसाइटों या दुर्भावनापूर्ण सॉफ़्टवेयर से संक्रमित साइटों पर ले जाते हैं, जिन्हें मैलवेयर (मैलवेयर **एक आम साइबर हमला है** और एंड–यूज़र सिस्टम और सर्वर पर डिलीवर और इंस्टॉल किए गए विभिन्न दुर्भावनापूर्ण प्रोग्रामों के लिए एक व्यापक शब्द है। ये हमले कम्प्यूटर, सर्वर या कम्प्यूटर नेटवर्क को नुकसान पहुँचाने के लिए डिज़ाइन किए गए हैं, और साइबर अपराधियों द्वारा वित्तीय लाभ के लिए डेटा प्राप्त करने के लिए उपयोग किए जाते हैं।) भी कहा जाता है । **दुर्भावनापूर्ण लिंक को विश्वसनीय लिंक के रूप में** दिखा**या** जा सकता है और ईमेल में लोगो और अन्य छवियों में एम्बेड किया जा सकता है।

दुर्भावनापूर्ण अनुलग्नक—

हालाँकि ये वैध फ़ाइल अटैचमेंट की तरह लग सकते हैं, लेकिन वास्तव में ये **मैलवेयर से संक्रमित फ़ाइल अटैचमेंट** होते हैं जो कम्प्यूटर और उनकी फ़ाइलों को खतरे में डाल सकते हैं।

धोखाधड़ीपूर्ण डेटा प्रविष्टि फॉर्म—

ये तकनीकें नकली फ़ॉर्म का उपयोग करती हैं जो उपयोगकर्ताओं को संवेदनशील जानकारी भरने के लिए प्रेरित करती हैं – जैसे कि उपयोगकर्ता आईडी, पासवर्ड, क्रेडिट कार्ड डेटा और फ़ोन नंबर। एक बार जब उपयोगकर्ता वह जानकारी जमा कर देते हैं, तो इसका उपयोग साइबर अपराधियों द्वारा पहचान की चोरी सहित विभिन्न धोखाधड़ी गतिविधियों के लिए किया जा सकता है।

फिशिंग हमलों के प्रकार—

फ़िशिंग अब सिर्फ़ क्रेडेंशियल और डेटा चोरी से कहीं ज़्यादा हो गई है। हमलावर किस तरह से अभियान चलाता है, यह फ़िशिंग के प्रकार पर निर्भर करता है। फ़िशिंग के प्रकारों में शामिल हैं:

• **ईमेल फ़िशिंग:**

किसी भी **दुर्भावनापूर्ण ईमेल सन्देश** को दिया जाने वाला सामान्य शब्द जिसका उद्देश्य उपयोगकर्ताओं को निजी जानकारी प्रकट करने के लिए धोखा देना होता है। हमलावर आम तौर पर खाता क्रेडेंशियल, व्यक्तिगत रूप से पहचान योग्य जानकारी (PII) और कॉर्पोरेट व्यापार रहस्य चुराने का लक्ष्य रखते हैं। हालाँकि, किसी विशिष्ट व्यवसाय को लक्षित करने वाले हमलावरों के अन्य उद्देश्य हो सकते हैं।

- **स्पीयर फिशिंग:** ये ईमेल संदेश **किसी संगठन के विशिष्ट लोगों को भेजे जाते हैं**, आमतौर पर उच्च-विशेषाधिकार प्राप्त खाताधारकों को, ताकि उन्हें संवेदनशील डेटा का खुलासा करने, हमलावर को पैसा भेजने या मैलवेयर डाउनलोड करने के लिए धोखा दिया जा सके।

- **लिंक हेरफेर:** संदेशों में एक **दुर्भावनापूर्ण साइट का लिंक** होता है जो आधिकारिक व्यवसाय की तरह दिखता है, लेकिन प्राप्तकर्ताओं को हमलावर द्वारा नियंत्रित सर्वर पर ले जाता है, जहाँ उन्हें एक नकली लॉगिन पृष्ठ पर प्रमाणित करने के लिए राजी किया जाता है, जो हमलावर को क्रेडेंशियल भेजता है।

- **व्हेलिंग (सीईओ धोखाधड़ी):** ये सन्देश आम तौर पर **किसी कम्पनी के हाई-प्रोफाइल कर्मचारियों को भेजे जाते हैं** ताकि उन्हें यह विश्वास दिलाया जा सके कि सीईओ या अन्य कार्यकारी ने पैसे ट्रांसफर करने का अनुरोध किया है। सीईओ धोखाधड़ी फ़िशिंग के अन्तर्गत आती है, लेकिन हमलावर किसी लोकप्रिय वेबसाइट को धोखा देने के बजाय, लक्षित निगम के सीईओ को धोखा देता है।

• **सामग्री इंजेक्शन:** एक हमलावर जो किसी **आधिकारिक साइट में दुर्भावनापूर्ण सामग्री इंजेक्ट** कर सकता है, वह उपयोगकर्ताओं को साइट तक पहुँचने के लिए धोखा देगा, उन्हें दुर्भावनापूर्ण पॉपअप दिखाएगा या उन्हें फ़िशिंग वेबसाइट पर पुनर्निर्देशित करेगा।

- **मैलवेयर:** किसी **लिंक पर क्लिक करने या किसी अटैचमेंट को खोलने** के लिए धोखा दिए जाने पर उपयोगकर्ता अपने डिवाइस पर मैलवेयर डाउनलोड कर सकते हैं। **रैनसमवेयर, रूटकिट या कीलॉगर** आम मैलवेयर अटैचमेंट हैं जो डेटा चुराते हैं और लक्षित पीड़ितों से पैसे ऐंठते हैं।

- **स्मिशिंग: एसएमएस सन्देशों का उपयोग** करके, हमलावर उपयोगकर्ताओं को उनके स्मार्टफ़ोन से दुर्भावनापूर्ण साइटों तक पहुँचने के लिए प्रेरित करते हैं। हमलावर लक्षित शिकार को एक दुर्भावनापूर्ण लिंक के साथ एक टेक्स्ट सन्देश भेजते हैं जो छूट, पुरस्कार या मुफ्त पुरस्कार का वादा करता है।

- **विशिंग:** हमलावर **आवाज बदलने वाले सॉफ़्टवेयर का इस्तेमाल करके** लक्षित पीड़ितों को सन्देश छोड़ते हैं कि उन्हें एक नंबर पर कॉल करना चाहिए जहाँ उन्हें ठगा जा सकता है। लक्षित पीड़ितों से बात करते समय हमलावर के उच्चारण या लिंग को छिपाने के लिए भी आवाज बदलने वाले सॉफ़्टवेयर का इस्तेमाल किया जाता है ताकि वे धोखेबाज़ व्यक्ति होने का दिखावा कर सकें।

- **"ईविल ट्विन" वाई-फाईः मुफ्त वाई-फाई का दुरुपयोग** करके, हमलावर उपयोगकर्ताओं को दुर्भावनापूर्ण हॉटस्पॉट से कनेक्ट करने के लिए धोखा देते हैं, ताकि वे मैन-इन-द-मिडल शोषण कर सकें।

- **फ़ार्मिंग:** फ़ार्मिंग एक **दो-चरणीय हमला** है जिसका उपयोग अकाउंट क्रेडेंशियल चुराने के लिए किया जाता है। पहले चरण में लक्षित पीड़ित पर **मैलवेयर इंस्टॉल किया जाता** है और उन्हें ब्राउज़र और एक **नकली वेबसाइट पर रीडायरेक्ट किया जाता** है, जहाँ उन्हें धोखा देकर क्रेडेंशियल का खुलासा किया जाता है। DNS पॉइज़निंग का उपयोग उपयोगकर्ताओं को नकली डोमेन पर रीडायरेक्ट करने के लिए भी किया जाता है।

- **एंगलर फ़िशिंग:** सोशल मीडिया का उपयोग करते हुए, हमलावर **आधिकारिक संगठन होने का दिखावा** करते हुए पोस्ट का जवाब देते हैं और उपयोगकर्ताओं को धोखा देकर उनके खाते की जानकारी और व्यक्तिगत जानकारी प्राप्त कर लेते हैं।

- **वाटरिंग होल:** एक समझौता की गई साइट अन्तहीन अवसर प्रदान करती है, इसलिए एक हमलावर कई लक्षित उपयोगकर्ताओं द्वारा उपयोग की जाने वाली साइट की पहचान करता है, **साइट पर एक भेद्यता का फायदा उठाता** है, और इसका उपयोग उपयोगकर्ताओं को मैलवेयर डाउनलोड करने के लिए धोखा देने के लिए करता है। लक्षित उपयोगकर्ता मशीनों पर मैलवेयर इंस्टॉल होने के साथ, एक हमलावर उपयोगकर्ताओं को नकली वेबसाइटों पर पुनर्निर्देशित कर सकता है या डेटा चोरी करने के लिए स्थानीय नेटवर्क पर पेलोड पहुँचा सकता है।

References: (Thanks to all.)

Adopt “zero trust model” on Internet to save ourself from any fraud.

मोबाइल और इन्टरनेट — महत्ता, आवश्यकता, हानियाँ और सावधानियाँ

https://geocities.ws/brijesh/amritvachan/folders-special/mobile-importance-need-downside-and-precautions.html

Play list of podcast of Shri Amit Dubey, Cyber Security Expert -

https://www.youtube.com/watch?v=J8qvn_HZb_A&list=PLqhVpp_JBawktbYZaJBn9gMaE1dG6kLJu

1st Episode Link: Here's How Hackers Are Targeting You,... https://www.youtube.com/watch?v=J8qvn_HZb_A

2nd Episode Link: Mobile Phone Hack Trick से ऐसे बचें |... https://www.youtube.com/watch?v=JtPiRdjO4IU

3rd Episode Link: Mobile Phone Hack, OTP Fraud, WhatsAp... https://www.youtube.com/watch?v=48VNZ1FpkBY

4th Episode Link: Mobile से आपको HACK किया जा रहा | Wha... https://www.youtube.com/watch?v=8RM4W_mWjTc

5th Episode Link: Mobile Phone Hack, OTP Fraud, WhatsAp... https://www.youtube.com/watch?v=WSJZh3cZuM0

6th Episode Link: How Hackers Hack Mobile Phone, Bank A... https://www.youtube.com/watch?v=shiTy3kAvoo

7th Episode Link: Hackers Hacking Mobile Phone, OTP, Ba... https://www.youtube.com/watch?v=bn4nc78AxEo

8th Episode Link: Podcast with Cyber Expert Amit Dubey ... https://www.youtube.com/watch?v=1HmmTwnfXyo

9th Episode Link: Podcast Cyber Expert Amit Dubey | Sha... https://www.youtube.com/watch?v=x_dOL6Ma8iw

10th Episode Link: Hacker Hacks Hotel, Steals Diamonds W... https://www.youtube.com/watch?v=2pSz_PnG-Bw

11th Episode Link: Hacker Steals iPhones Worth 10 Crore ... https://www.youtube.com/watch?v=Ic3hsZOvUcY

12th Episode Link: What is Dark Web? How To Access Dark ... https://www.youtube.com/watch?v=mtbn2R1zMpo
13th Episode Link: How Hackers Hack Mobile Phone Using A... https://www.youtube.com/watch?v=6q603E5w8zc
14th Episode Link: How AI Solved 19 Yr Old Murder Case |... https://www.youtube.com/watch?v=jpJ4d7zdlSU
15th Episode Link: Mobile Phone Listens To You Even When... https://www.youtube.com/watch?v=ZTIw6cgrwmA
16th Episode Link: How China is Preparing Cyber Army | C... https://www.youtube.com/watch?v=bnpNNAkTX_w
17th Episode Link: Mobile Phone Hacked by Downloading Image... https://www.youtube.com/watch?v=OaMmuUzmEhA
18th Episode Link:

हैकर्स की नई ट्रिक, बचने का एक तरीका
Cyber crime exposed: Digital arrest, OTP scams, password leak

SMS, Call and Email spoofing —

https://www.youtube.com/watch?v=shiTy3kAvoo&t=2501s

E-sim fraud - How to prevent —

https://www.youtube.com/watch?v=shiTy3kAvoo&t=2432s

Digital Arrest से कैसे बाहर निकलें? Hacking Expert Amit Dubey से जानिए
https://www.youtube.com/watch?v=f_tSA2OAmSU

How to activate or deactivate call forwarding on Jio, Airtel, Vi, and BSNL https://www.91mobiles.com/hub/call-forwarding-codes-jio-airtel-vi-bsnl-how-to-activate/

MobiArmour: Mobi Armour by MobiArmour

https://play.google.com/store/apps/details?id=com.prosthetik.supernova

About this app: Introducing "MobiArmour (Mobi Armour): Your Guardian in the Digital Realm" – the all-inclusive solution dedicated to fortifying your digital existence against an array of potential hazards. In a time where technology assumes an integral role in our everyday lives, guaranteeing your online security has never held more significance.

WTMP — Who touched my phone?

https://play.google.com/store/apps/details?id=com.wtmp.svdsoftware

About this app: WTMP — Who touched my phone?
Application will record those who will use your phone using the front camera in the background mode, invisibly for user. You will see who, when and what did to your favorite device while it is not under your attention.