



Supported by:



INFORMATION SECURITY
EDUCATION & AWARENESS



A joint initiative of DSCI & Government of Telangana



ADVOCACY ON DIGITAL SAFETY

www.isea.gov.in

<https://ccoe.dsci.in/>

www.endnowfoundation.org

एन्ड नाउ फाउंडेशन भारत की पहली गैर लाभ संगठन है, जो कि महिलाओं, किशोर और बच्चों के बीच ज़िम्मेदार ऑनलाइन व्यवहार पैटर्न्स को जगाने के लिए इंटरनेट आचार विचार एवं डिजिटल कल्याण को बढ़ावा देती है।



साइबर ज्ञान हमारे सम्मानित संस्थापक ट्रस्टी की याद में समर्पित है।

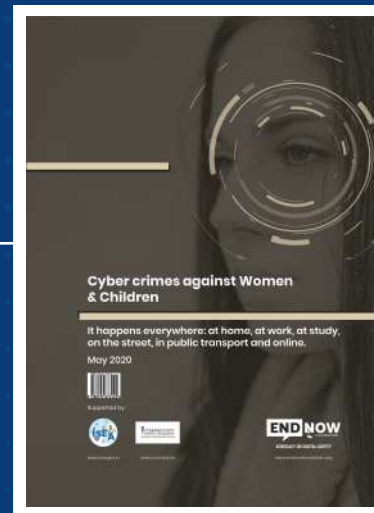
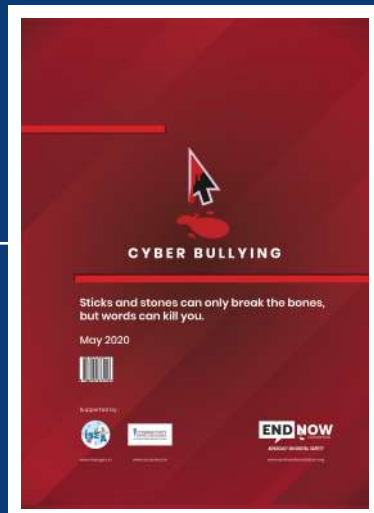
लेट श्री काशीनाथ बठीना , आईपीएस।



23 फरवरी 1938 - 26 जुलाई 2020

हमारी पब्लिकेशंस

(अमेज़न पर उपलब्ध है)





स्मार्टफोन

इक्कीसवीं सदी का सबसे बड़ा गैर नशा ।

अगर आपके स्मार्टफोन ने आपको अपना गुलाम बना लिया है, यहाँ उससे अलग होने के लिए स्टेप बाई स्टेप दृष्टिकोण है ।



अपने स्मार्टफोन पर अधिसूचना को अक्षम करें ।



दोस्तों और परिवार के साथ भोजन करते समय अपने फ़ोन को दूर रखें ।



अपने डिवाइस को बैडरूम से बहार चार्ज करें ।



डिवाइस को बैठक से फ़्री रखें ।



अपने स्मार्टफोन के बजाय अपने कंप्यूटर से सोशल मीडिया का उपयोग करें ।



अपने फ़ोन पर ग्रे स्केल मोड का उपयोग करें ।



अपने स्क्रीन पर केवल महत्वपूर्ण उपकरण रखें ।



एंड्राइड और IOS के उपयोग को नियंत्रित करने तथा डिजिटल भलाई के लिए स्क्रीन समय का उपयोग करें ।



ऑनलाइन गेमिंग बहुत सारे खतरों से घिरा हुआ है।

इसके नकारात्मक बोध को जानने के लिए आगे पढ़ें।



पूरे दिन खेलों की लत लग जाना।



स्वास्थ्य पर बुरा प्रभाव पड़ना।



परिवार और दोस्तों से अलग हो जाना।



कीमती समय की बर्बादी।



नींद की समस्या का सामना करना।



एक महंगा शौक।



आक्रामकता का स्तर बढ़ जाना।



नेत्र दृष्टि को प्रभावित करता है।

हम तुम्हारा खाता हैक कर लेंगे।

क्या मैं एक नया पासवर्ड लगा लू?



सोशल मीडिया

अधिक मज़ेदार होता है जब आप सुरक्षा पर ध्यान देते हैं।

यहाँ साइबर दुनिया में सुरक्षित रहने के लिए कुछ सुझाव दिए गए हैं।



एक मज़बूत पासवर्ड का उपयोग करें।



सावधान वाले लिंक पर क्लिक करें।



अपने प्रत्येक सोशल मीडिया अकाउंट के लिए एक अलग पासवर्ड का उपयोग करें।



आपके द्वारा शेयर की जाने वाली व्यक्तिगत जानकारी के बारे में सावधान रहें।



अपने सुरक्षा उत्तर सेट करें (यह विकल्प अधिकांश सोशल मीडिया में उपलब्ध है)।



सोशल मीडिया चैनलों की व्यक्तिगत नीतियों से परिचित रहें।



सोशल मीडिया का उपयोग केवल कंप्यूटर से करें।



एंटी वायरस सॉफ्टवेयर स्थापित करके अपने कंप्यूटर को सुरक्षित करें।



मित्र अनुरोध स्वीकार करते समय सतर्क रहें।



अपना काम ख़तम करके लॉग ऑफ करना याद रखें।

साइबर बदमाशी

प्रकार



साइबर पीछा

ऐसे संदेशों को बार बार भेजना जिसमें धमकियां शामिल हैं या अत्यधिक डराने वाली हैं।



वेश बदलना

किसी और के होने का नाटक करना और किसी भी सामग्री को ऑनलाइन भेजना या पोस्ट करना जिससे उस व्यक्ति को बुरा लग रहा हो, उस व्यक्ति को परेशानी में दाल देता है।



बदनामी

किसी व्यक्ति को उसकी प्रतिष्ठा या उसकी दोस्ती को नुकसान पहुंचाने के लिए निर्दयी गॉसिप को ऑनलाइन भेजने या पोस्ट करना।



उत्पीड़न

बार बार कुछ आपत्तिजनक, अशिष्ट और अपमानजनक संदेश भेजना।



आउटिंग और टिकरी

ऑनलाइन किसीकी गुप्त या शर्मनाक जानकारी शेयर करना।



ज्वलंत

गुस्से और अश्लील भाषा के साथ इलेक्ट्रॉनिक संदेश का उपयोग करके ऑनलाइन लड़ना।



बहिष्कार

जानबूझकर किसी को मित्र सूची जैसे ऑनलाइन समूह से बहार करना।

भद्दा
विकृत
असफलता
स्वार्थी
मानसिक
लूज़र
बेकार

साइबर बदमाशी

प्रभाव के बाद

स्वास्थ्य के मुद्दे

आत्महत्या



डिप्रेशन



अल्कोहल



हिंसक



भद्दा
विकृत
असफलता
स्वार्थी
मानसिक
लूज़र
बेकार

आम साइबर खतरे

यहाँ साइबर खतरों से बचाव के कुछ सामान्य रूप हैं।

रैंसमवेयर

पुरुष्वॉल्ट सॉफ्टवेयर जो क्रिप्टोवैरोलॉजी का उपयोग कर डाटा को एन्क्रिप्ट करके उपयोगकर्ता की पहुँच को लॉक करता है, जबकि फाइल को फिर से खोलने और पुनर्स्थापित करने के लिए पीड़ित से भुगतान को बढ़ाता है।



मालवेयर

दुर्भावनापूर्वक सॉफ्टवेयर एक मशीन पर अनजाने में स्थापित होता है और तीसरे पक्ष के लिए आपराधिक कार्यवाही करता है।



बॉटनेट्स

एक गुप्त कुंजी जो आपराधिक उद्देश्य के लिए एक हमलावर द्वारा नियंत्रित किये जाने वाले उपकरणों और कनेक्शनों को प्रवेश प्रदान करता है।



स्मूफिंग

एक फ़र्जी खाते से गए ईमेल सन्देश एक वैध और विश्वसनीय स्रोत के रूप में एक उपयोगकर्ता प्रणाली या गोपनीय जानकारी तक पहुँचने के प्रयास के रूप में सन्देश भेजना।



वॉर्म

स्टैंड अलोन सॉफ्टवेयर जिसे प्रयास करने और अन्य नेटवर्क पर खुद को दोहराने के लिए एक मेज़बान कार्यक्रम की आवश्यकता नहीं होती है, और यह फैलने वाले डाटा और सॉफ्टवेयर को नुकसान पहुंचाता है।



टोजन्स

कंप्यूटर प्रोग्राम जिसमें विनाशकारी कोड होता है, जो हानिरहित प्रोग्रामिंग को प्रच्छन्न करता है।



सेवा से इंकार DDOS

बैंडविड्थ की बाढ़ जो कि ऑनलाइन स्यतेम को अनुपलब्ध बनाता है।



वायरस

एक प्रकार का मालवेयर जो निष्पादित होने पर कंप्यूटर से इसकी प्रोग्रामिंग कि नक़ल करके फैलता है और उपयोगकर्ता कार्यक्रमों और फाइलों को संक्रमित करने के तरीके को बदलने के लिए जो वे संचालित करते हैं या पूरी तरह से काम करना बंद कर देते हैं।



फिशिंग

एक DNS सर्वर सॉफ्टवेयर आलोचनीयता एक्सपोज़ हो जाता है, या एक होस्ट फाइल अदला-बदली होती है और एक वैध वेबसाइट एक स्कैन साइट पर दुर्भावनापूर्ण रूप से पुनर्निर्देशित होती है जहाँ अनजाने आगंतुक अपने गोपनीय जानकारी दर्ज करते हैं।



स्पाइवेयर

उपयोगकर्ता कि गतिविधियों को गुप्त रूप से मॉनिटर करने के लिए उपयोग किये जाने वाले हार्ड ड्राइव पर आपराधिक मालवेयर।



फार्मिंग

एक DNS सर्वर सॉफ्टवेयर आलोचनीयता एक्सपोज़ हो जाता है, या एक होस्ट फाइल अदला-बदली होती है और एक वैध वेबसाइट एक स्कैन साइट पर दुर्भावनापूर्ण रूप से पुनर्निर्देशित होती है जहाँ अनजाने आगंतुक अपने गोपनीय जानकारी दर्ज करते हैं।



ऐडवेयर

खोज अनुरोधों को पुनर्निर्देशित कर सकते हैं या अपने निर्माता के लिए राजस्व उत्पन्न करने वाले कुछ विज्ञापनों को स्वचालित रूप से प्रस्तुत कर सकते हैं।





फिशिंग अटैक अलर्ट

साइबर अपराधियों से खुद को बचाने के लिए कमर कसलें।

पहले 5 लाल झंडे

वेब लिंक अपरिचित साइट्स को जन्म दे सकते हैं (जांच करने के लिए उनको चेक करते रहें)।



एक ऐसा लगाव है जिसकी आप उम्मीद नहीं कर रहे थे।



पूरे समय खराब वर्तनी और व्याकरण नोटिस कर सकते हैं।



यह व्यक्तिगत जानकारी (पासवर्ड, सारी बैंक जानकारी, आदि) पूछता है।



प्रेषक आपको नाम से संबोधित नहीं करता है।



सुरक्षित कैसे रहें

1



किसी भी लिंक या अटैचमेंट पर क्लिक न करें जिसे आप सत्यापित नहीं कर सकते हैं।

2



जानकारी के लिए अनुरोधों को सत्यापित करने के लिए कॉल करें (भले ही यह आप के किसी परिचित व्यक्ति से लगता है)।

3



जब भी सन्देश हो, मदद के लिए हमेशा इष्टतम से संपर्क करें।

ब्लू लाइट के संपर्क में आने से आपके मस्तिष्क और शरीर पर क्या प्रभाव पड़ता है।

मेलाटोनिन को बाधित करके स्मार्टफोन प्रकाश नींद स्केड्यूल खराब करती है।
यह सभी प्रकार की स्वास्थ्य समस्याओं की ओर जाता है।

आपके नींद के कार्यक्रम में व्यवधान आपको विचलित कर सकता है और अगले दिन आपकी स्मरणशक्ति को भी खराब कर सकता है।



कुछ सबूत है कि समय के साथ रेटिना को नुक्सान पहुंचाकर नीली रौशनी हमारी दृष्टि को नुक्सान पहुंचा सकती है - हालांकि कुछ और शोध की ज़रूरत है।



स्मार्टफोन की रौशनी के कारण एक खराब रात की नींद, सीखने को कठिन बना सकती है।

शोधकर्ता इस बारे में जांच कर रहे हैं कि नीली बत्ती से मोतियाबिंद हो सकता है या नहीं।



लम्बे समय तक पर्याप्त नींद नहीं लेने से न्यूरोटोक्सिन का निर्माण हो सकता है जिससे आपको अच्छी नींद प्राप्त करने में कठिनाई होती है।



रात में प्रकाश के संपर्क में आने और अशांत नींद में एक सम्बन्ध है और यह ब्रेस्ट कैंसर और प्रोस्टेट कैंसर के जोखिम को बढ़ता है।



जिन लोगों के मेलाटोनिन का स्तर कम हो गया है और जिनके शरीर की घड़ियाँ प्रकाश के संपर्क में आती हैं, वे डिप्रेसन से ज़्यादा ग्रस्त हैं।



मेलाटोनिन और नींद को बाधित करके स्मार्टफोन की रौशनी "हार्मोन" के साथ खिलवाड़, भूख को नियंत्रित और संभावित रूप से "मोटापे" (obesity) के जोखिम को बढ़ा सकती है।



पूरी जानकारी के लिए
919xxxxxxx पर कॉल करें।



फेक न्यूज़

फैलाने के लिए लोग सोशल मीडिया, मेसेजिंग
और इंटरनेट का गलत इस्तेमाल कर रहे हैं।

यह ऐसे तरीके दिए गए हैं जिनसे आप नकली समाचारों को देख सकते हैं।



स्रोत और URL की जांच करें।



फैक्ट चेकिंग साइट्स देखें।
(www.factly.in)



सुर्खियों से परे पढ़ें।



जांच करें कि क्या यह एक मज़ाक है।



डेट की जांच करें।



निर्णय से पहले अपने पक्ष की जांच
करें।



असामान्य स्वरूपण के लिए देखें।



गूगल रिवर्स इमेज चेक करें।

सोशल मीडिया और इंटरनेट पर फ़र्जी खबरें छापना



स्त्रोत पर विचार करें

क्या यह विश्वसनीय है, अच्छी तरह से जानते हैं? उस स्त्रोत पर विचार करें जो एक प्रतिष्ठित समाचार चैनल या ऑनलाइन समाचार वेबसाइट से है।



URL कि जांच करें

क्या यह वैद्य लगता है? क्या वेबसाइट के विश्वसनीय होने का ट्रैक रिकॉर्ड है? कई साइट समाप्त होने वाले समान साइट का उपयोग करती हैं।



लेखक कौन है?

क्या आपने लेखक का नाम ऑनलाइन देखने के लिए खोज की कि क्या वे विश्वसनीय और सम्मानित है? कई नकली साइट लेखक के नाम का उपयोग नहीं करेंगी।



हैडलाइन से परे पढ़ें

क्या लेख संतुलित और निष्पक्ष लगता है? दरवाज़े पर अपने पूर्वाग्रह कि जांच करते समय टोन और व्युपोज़ के लिए हमेशा आलोचनात्मक अध्ययन करें।



पूर्वाग्रह की अवहेलना

ऐसी कहानियों पर विश्वास करना आसान है जो आपके आंतरिक विचारों कि पुष्टि करती है। लेकिन अगली बार आप सोशल मीडिया पर अपनी राजनितिक नस्लीय या धार्मिक विचारों को देखते रहें।



दूसरी राय लें

यदि कोई कहानी आपको हर गुस्से में और गहराई से बताती है, तो संपर्क करने या फॉरवर्ड करने से पहले डीबंकिंग साइट्स से संपर्क करने का परामर्श लें।

नकली समाचार खोलना

गलत और विघटन के 9 प्रकार



गलत सम्बन्ध

जब हेडलाइंस दृश्य या कैप्शन सामग्री का समर्थन नहीं करते हैं।



गलत सन्दर्भ

जब वास्तविक सामग्री को झूठी प्रासंगिक जानकारी के साथ साझा किया जाता है।



हेरफेर की गई सामग्री

जब कुछ वास्तविक जानकारी या कल्पना को धोखा देने की लिए हेरफेर किया जाए।



व्यंग्य या पैरोडी

नुकसान पहुंचाने का कोई इरादा नहीं है लेकिन मूर्ख बनाने की क्षमता है।



भ्रामक सामग्री

किसी मुद्दे या व्यक्ति को प्रसिद्ध करने के लिए सूचना को भ्रमित करना।



सामग्री को बढ़ा देना

जब वास्तविक स्रोत लगाए जाते हैं।



निर्मित सामग्री

वह सामग्री जो 100% झूठी है और उसे धोखा देने और नुकसान पहुंचाने की लिए डिज़ाइन की गयी है।



प्रचार प्रसार

जब सामग्री का उपयोग दृष्टिकोण मूल्यों और ज्ञान का प्रबंध करने की लिए किया जाता है।



प्रायोजित सामग्री

विज्ञापन या PR संपादकीय सामग्री के रूप में प्रच्छन्न है।

नकली समाचार खोलना

फोटो सत्यापन



मूल स्रोत और सामग्री (जिसमें स्थान, डाटा और अनुमानित समय शामिल है) की पहचान और सत्यापन करें।



कैमरा मॉडल / टाइम स्टैम्प की जानकारी के लिए फोटोफॉरेन्सिक/फाइंडएक्सिफ़ जैसे टूल का हमेशा उपयोग करें।



कई स्रोतों को खोजने की कोशिश करें। चुनौती साबित करने की लिए मूल स्रोत को चुनौती दें - प्रश्नों का पालन करें।



वुल्फराम अल्फा जांच का उपयोग करते हुए अगर मौसम फोटो में कैद हो जाता है। (उदाहरण के लिए धूप, बरसात, तूफ़ान) वास्तव में उस क्षेत्र का मौसम होता है।



हमेशा गूगल पर टिनआई / रिवर्स इमेज सर्च जैसे टूल का उपयोग करें।

नकली समाचार खोलना

वीडियो सत्यापन



मूल स्रोत और सामग्री (जिसमें स्थान, दिनांक और अनुमानित समय शामिल है) को पहचानें और सत्यापित करें।



कुछ एकाधिक स्रोतों को खोजने का प्रयास करें। चुनौती साबित करने के लिए मूल स्रोत को चुनौती दें - प्रश्नों का पालन करें।



एमनेस्टी इंटरनेशनल के डाटा दर्शक का उपयोग करें।

(<https://citizenevidence.amnestyusa.org>)



अपलोडर का नाम और अपलोडर के डाटा की जांच करें।



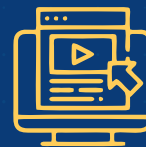
सोशल मीडिया/सम्बन्ध खाते क्या जानकारी देते हैं जो स्थान, गतिविधि, विश्वसनीयता, पूर्वाग्रह या अपलोडर के एजेंडा को इंगित करें।



ये खाते कितने समय से सक्रिय हैं? वे कितने सक्रिय हैं।



वह व्यक्ति जो ऑनलाइन डाटा बेस या नेटवर्किंग प्लेटफॉर्म में सूचीबद्ध है।
उद्धरण : लिंकड इन।



सोशल मीडिया, ब्लॉग या वेबसाइट सहित अन्य खाते - अपलोडर से सम्बन्ध है ?



10 घर से काम के लिए सुरक्षा युक्तियाँ



अपनी कार्यस्थल डिवाइस का उपयोग करें जिसमें सुरक्षा के सारे एहतियात हों।



हमेशा सभी खातों और उपकरणों के लिए टू-फैक्टर-ऑथेंटिकेशन और एक जटिल पासवर्ड का उपयोग करें।



सुरक्षित कनेक्शन के माध्यम से डाटा तक पहुँचने के लिए VPN का उपयोग करें।



संवेदनशील डाटा खो न जाए ये सुनिश्चित करने के लिए डाटा हानि रोकथाम (DLP) उपकरण सक्षम करें।



मालवेयर हमलों से बचने के लिए नियमित रूप से OS और एंटीवायरस को अपडेट करें।



कोविड-19 स्कैम, फिशिंग, इ-मेल दुर्भावनापूर्ण डोमेन और नकली ऐप्स के बारे में जागरूक रहें।



असुरक्षित, मुक्त, सार्वजनिक वाई-फाई, हॉटस्पॉट या नेटवर्क का उपयोग करने से बचें।



सुनिश्चित करें कि केवल प्रामाणिक सत्यापित URL ही एक्सेस किये गए हैं।



अपने सिस्टम और क्लाउड में डाटा का नियमित बैकअप (वन-ड्राइव, जी-ड्राइव, आदि.)।



USB पोर्ट और सिस्टम ब्लूटूथ कनेक्टिविटी को अक्षम करें।

मुझे एक अच्छी जॉब तुरंत मिल
गयी !

मैं तुम्हारे सारे पैसे चुरा लूँगा !!



घर प्रत्येक दिन हज़ारों लोग "ऑनलाइन जॉब्स स्कैम" के शिकार हो रहे हैं। इनमे से एक मत बनिए।

यहाँ बताया गया है कि आप इंटरनेट जॉब घोटाला कैसे कर सकते हैं।



आपको तुरंत नौकरी के लिए चुना गया है।



साक्षात्कार त्वरित सन्देश प्लेटफार्म पर
निर्धारित किया गया है।



अस्पष्ट नौकरी की आवश्यकता और नौकरी
का विवरण।



कंपनी या नौकरी के बारे में खोज परिणाम
दिखाई नहीं देते हैं।



गैर-लिखित इ-मेल।



आपको गोपनीय जानकारी प्रदान करने के
लिए कहा जाता है।



कोई संपर्क जानकारी या कंपनी के हस्ताक्षर
के साथ इ-मेल।



आपको भुगतान करने के लिए कहा जाता
है।

धोखाधड़ी का शिकार न हो

मज़ेदार सौदा है, मेरी बाइक कब मिलेगी ??



आप तुरंत अपने फ़ोन से पैसे भेज सकते हैं !



ऐसा न करें



अग्रिम में भुगतान।



भुगतान अनुरोधों को को अनुमोदित से तुरंत रिपोर्ट करें।



व्यक्तिगत जानकारी जैसे PIN, OTP, खाता संख्या, आदि साझा करना।



संदिग्ध खातों की तुरंत शिकायत करें।



कॉल करते समय किसी भी मौद्रिक लेनदेन को सुविधाजनक बनाएं।

खबरदार : ऑनलाइन प्लेटफ़ार्म के माध्यम से भुगतान मज़बूत है लेकिन धोखाधड़ी के लिए अतिसंवेदनशील है।

99 % भुगतान फिशिंग और सोशल इंजीनियरिंग अपराधों से ग्रस्त है।

कार्ड धोखाधड़ी



हमेशा अपने कार्ड और उसके विवरण की रक्षा करें।



लेन देन करते समय अपने कार्ड को अपनी दृष्टि से बहार न जाने दें।



अपने कार्ड से डेबिट की गई राशि की पुष्टि करने के लिए रिटेलर से पूछें।



नए कार्ड के आते ही उस पर हस्ताक्षर करें।



अपने ऑनलाइन विवरणों के खिलाफ अपनी रसीदों की जांच करें।



कार्ड लेन देन से अपनी रसीदों को ध्यान से त्यागें और अपने वित्तीय मामलों में सम्बंधित जानकारी।



अपने कार्ड को किसी सार्वजनिक स्थान पर अनअटेंडेड न रखें / हर समय अपने साथ निजी सामान रखें।



कभी भी अपना पिन न लिखें और न ही किसी को बताएं।



जब आप लेन देन करते हैं तो सुनिश्चित करें की आप अपडेट किये गए एंटीवायरस और OS सॉफ्टवेयर का उपयोग कर रहे हैं।



केवल विश्वसनीय स्रोत से खरीदें। इंटरनेट खरीददारी के लिए, सिक्योरिटी प्रोटोकॉल 3D-सिक्योर का इस्तेमाल करें।



जब रिप्लेसमेंट कार्ड आये, तो एक्सपायर्ड, अप्रयुक्त, अवरुद्ध कार्ड्स और मैग्नेटिक स्ट्रिप या चिप को टुकड़ों में काट दें।

नकद मशीन (ATM)

हमेशा अपने आसपास दूसरे के बारे में जागरूक रहने की कोशिश करें।



अगर छेड़छाड़ के कोई संकेत है तो ATM का उपयोग न करें।

यदि ATM कार्ड वापस न करे तो इसे अपने बैंक को रिपोर्ट करें।

अपना पिन बचाएं।

भुगतान अवधि (POS)

कार्ड स्किमिंग रिटेल आउटलेट्स पर भी हो सकता है, विशेष रूप से बार, रेस्टोरेंट क्षेत्र, पार्किंग टिकट मशीन और अनाम पेट्रोल स्टेशन।



भुगतान के लेन देन के दौरान कार्ड से कभी दृष्टि (और यदि संभव हो तो स्पर्श) न खींचें।

आग्रह करें कि आपको कार्ड हर समय दिखाई दे।



"KYC" घोटाला कैसे काम करता है।





OTP की रक्षा करें

आपके वन टाइम पासवर्ड (OTP) का इस्तेमाल आपके बैंक खाते से
पैसे चुराने के लिए किया जा सकता है।
परेशानी से बहार रहने के लिए इसे साझा करने से बचना चाहिए।



कभी भी अपना वन टाइम पासवर्ड (OTP) शेयर न करें।



अपना ATM PIN बार बार बदलते रहें।



अपने CVV को कभी साझा न करें।



सुरक्षित ऑनलाइन लेन देन के लिए https:// और लॉक आइकॉन की जांच करें।



ई-कॉमर्स वेबसाइट पर क्रेडिट/डेबिट के विवरण को कभी भी न सहेजें।



अपना **पिन**
दर्ज करने
से पहले

सोचें।

इसे न करें

- अग्रिम भुगतान।
- व्यक्तिगत विवरण साझा करना।
पिन नंबर, OTP खाता, आदि।
- स्थानांतरण, कॉल पर रहते हुए पैसे प्राप्त करना।

आपके पिन के माध्यम से UPI भुगतान की आवश्यकता नहीं है।

paytm

पे PhonePe

G Pay

खबरदार : ऑनलाइन प्लेटफार्म के माध्यम से भुगतान मज़बूत है लेकिन धोखाधड़ी के लिए अतिसंवेदनशील है।

99 % भुगतान फिशिंग और सोशल इंजीनियरिंग अपराधों से ग्रस्त है।

डेबिट कार्ड स्किमिंग कैसे काम करता है।

चोरों द्वारा बैंक से चोरी करने के कुछ तरीके यहाँ दिए गए हैं।

जालसाज पूरे डिवाइस को स्विच करते हैं।



धोखेबाज़ एक स्किमर स्थापित करते हैं।



धोखेबाज़ एक नया कुंजी पैड स्थापित करते हैं।



धोखेबाज़ एक कैमरा स्थापित करते हैं।



अपनी सुरक्षा कैसे करें।

- गैस स्टेशन और स्टोर के बैंक में ATM सुरक्षित हो सकता है।
- जैसे ही आप इसे स्लॉट से हटाते हैं, यह कार्ड स्किमर को ढीला कर सकता है।
- जैसे ही आप अपना पिन दर्ज करते हैं, कुंजी पैड को अपने दूसरे हाथ से ढक दें।
- यदि यह बदल जाता है तो ATM या भुगतान मशीन का उपयोग न करें।
- यदि ATM का उपयोग करने में परेशानी हो, तो अजनबियों की मदद स्वीकार न करें।
- संदिग्ध गतिविधि को देखने के लिए नियमित रूप से बैंक स्टेटमेंट की जांच करें।

सिम स्वैप फ्रॉड क्या है?

स्टेप 1



जालसाज ग्राहक की निजी जानकारी फिशिंग, विशिंग, स्मिशिंग या किसी अन्य माध्यम से इकट्ठा करते हैं।

स्टेप 2



वे फिर मोबाइल ऑपरेटर से संपर्क करते हैं और सिम को ब्लॉक करवाते हैं। इसके बाद मोबाइल ऑपरेटर के रिटेल आउटलेट पर ग्राहक के रूप में फेक आईडी प्रूफ लेकर जाते हैं।

स्टेप 4



धोखेबाज़ तब चोरी की गई बैंकिंग जानकारी का उपयोग करके लेनदेन को सुविदजनक बनाने के लिए आवश्यक OTP उत्पन्न करता है। यह OTP जालसाज द्वारा रखे गए नए सिम पर प्राप्त होता है।

स्टेप 3



मोबाइल ऑपरेटर वास्तविक सिम कार्ड को निष्क्रिय कर देता है और धोखाधड़ी करने वाले के लिए एक नया सिम जारी करता है।



रोमांस धोखाधड़ी के शिकार होने से बचें।



- ऑनलाइन चैटिंग में शामिल न हों, डेटिंग करें या ग्राहकों की सत्यता की पुष्टि किये बिना लोगों से भावनात्मक रूप से न जुड़ें।
- ऑनलाइन अजनबियों / सोशल मीडिया दोस्तों को पैसे या अपना विवरण कभी न दें।
- ऑनलाइन फॉलोअर कुछ संपर्कों या बातचीत के बाद ही डेटिंग वेबसाइट/प्लेटफॉर्म के बाहर संवाद करने के लिए कहता है।
- अपने प्रशंसक को www.tineye.com पर या गूगल रिवर्स इमेज चेक करें, यह निर्धारित करने में मदद करें की क्या वे वास्तव में वही है जो वे कहते हैं।
- ऑनलाइन अंतरंग चित्रों या वीडियो को साझा न करें। स्कैमर्स को पिछले साझा चित्रों या वीडियो का उपयोग करके उन लक्ष्यों को ब्लैकमेल करने के लिए जाना जाता है जो आप दूसरों को नहीं दिखाना चाहते।





वैवाहिक धोखाधड़ी रोकें

खुद को वैवाहिक धोखाधड़ी का शिकार होने से कैसे रोकें ।



- गहरी प्रोफाइल चेक करें।
- विवाह पोर्टल पर हमेशा सत्यापित प्रोफाइल मिलान के लिए देखें।
- कभी किसी को पैसे न दें।
- अपने पोर्टल खाते की जानकारी कभी भी प्रकट न करें। व्यक्ति से मिलते समय सूचित रहें।
- किसी भी दस्तावेज़ पर हस्ताक्षर करते समय सूचित करें।





ऋण धोखाधड़ी से सावधान रहें।

चेतावनी के संकेत

- कोई क्रेडिट जांच की आवश्यकता नहीं है।
- कानूनी रूप से सरकार के साथ ऋणदाता पंजीकृत नहीं है।
- कोई भौतिक पता नहीं है।
- अग्रिम भुगतान।
- ऑफर कुछ दिनों में समाप्त हो गई है।

सुरक्षा टिप्स

- एक सुरक्षित भुगतान (<https://URL> के साथ पैड लॉक प्रतीक के लिए देखें)।
- खरीददार या विक्रेता को कभी भी OTP या PIN नंबर साझा न करें।
- जब आप कॉल पर हों तो कभी भी भुगतान न करें।
- खरीददार या विक्रेता द्वारा प्रदान किये गए किसी भी शॉर्ट लिंक पर क्लिक न करें और न भरें।
- खरीददार या विक्रेता द्वारा उपलब्ध कराये गए लिंक से कोई गूगल न करें।
- QR कोड को स्कैन न करें।
- किसी भी ऋण के लिए अग्रिम शुल्क का भुगतान कभी न करें।





लॉटरी धोखाधड़ी के खिलाफ खुद को सुरक्षित रखें।

कुछ धोखाधड़ी

- कौन बनेगा करोड़पति।
- स्कैच कार्ड उपहार।
- RBI की लॉटरी।
- युरोपियन लॉटरी।

सुरक्षा टिप्स

- ई-मेल या एसएमएस (SMS) के माध्यम से भेजे गए शोर्टलिंक पर क्लिक न करें।
- https:// के साथ शुरू होने वाले वेबसाइट पर क्लिक करें।
- एक ऐसा लगाव है जिसकी आपको उम्मीद नहीं थी।
- प्रेषक आपको नाम से नहीं बुलाता।
- लॉटरी पुरस्कार जीतने के लिए अग्रिम भुगतान करने की आवश्यकता नहीं है।
- जब तक हम व्यक्तिगत रूप से खरीदें या भाग न लें, हम लॉटरी में पैसा नहीं जीत सकते।
- प्रतियोगिताओं और लॉटरी में जीता इनाम हासिल करने के लिए आपको अग्रिम शुल्क का भुगतान करने की आवश्यकता नहीं।
- उच्च रिटर्न की प्रतीक्षा में अज्ञात व्यक्ति या संस्थाओं को धन हस्तांतरित न करें।





पहचान धोखाधड़ी से सुरक्षित रहें।

अपनेआप को पहचान के शिकार होने से कैसे सुरक्षित रखें।

- ई-मेल या एसएमएस के माध्यम से भेजे गए छोटे लिंक न खोले।
- पीसी और मोबाइल फ़ोन दोनों पर एंटीवायरस सॉफ्टवेयर अपडेट करें।
- ई-मेल या एसएमएस पर वित्तीय / पासवर्ड जानकारी के बारे में संवाद न करें।
- सोशल मीडिया प्लेटफ़ॉर्म पर DOB जन्मस्थल या मेलिंग पता पोस्ट न करें।
- समय समय पर पासवर्ड बदले।
- सभी ऐप्लिकेशन्स के लिए एक ही पासवर्ड का प्रारूप न रखें।
- समय समय पर बैंक स्टेटमेंट और क्रेडिट कार्ड स्टेटमेंट की जांच करें।
- पैन कार्ड/आधार कार्ड की जानकारी की ज़ेरोक्स कॉपी देते समय उद्देश्य का उल्लेख करें।



साइबर सुरक्षा



कैसे ऑनलाइन सुरक्षित रहें।



हमेशा अपनी जानकारी और पासवर्ड निजी रखें।



आप जो ऑनलाइन पोस्ट कर रहे हैं उससे सावधान रहें।



हमेशा अपनी गोपनीयता सेटिंग की जांच करें।



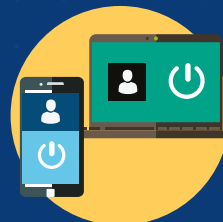
विश्वसनीय वेबसाइट पर सुरक्षित रूप से खरीददारी करें।



मज़बूत पासवर्ड चुनें।



एंटीवायरस के साथ अपने सभी उपकरणों को सुरक्षित रखें।



लॉग-ऑफ़ करना याद रखें।



वेबसाइट (URL) की जांच करें।



ई-मेल खोलने से पहले हमेशा उनकी जांच करें।



फिशिंग और अन्य घोटालों से बचें।



अपने बच्चों को ऑनलाइन सुरक्षित रखें।



अपना और दूसरों का ऑनलाइन सम्मान करें।



स्मार्टफोन और टैबलेट को सुरक्षित रखें।



स्मार्टफोन और टैबलेट को आपके डेस्कटॉप उपकरण की तुलना में अधिक सुरक्षा की आवश्यकता है।



ऑटोमैटिक अपडेट का उपयोग करें और अपने उपकरणों (और सभी इनस्टॉल किये गए एप्लीकेशन) को अप-टू-डेट रखें।



पिन/पासवर्ड या मोबाइल उपकरणों के लिए सुरक्षा/फिंगरप्रिंट पहचान पर स्विच करें।



सार्वजनिक वाई-फाई से कनेक्ट न करें, 3G या 4G कनेक्शन का उपयोग करें या VPNs का उपयोग करें।



कॉन्फ़िगर किया जा सकता है, जिसे दूर से मिटाया जा सकता है या रिमोट से लॉक किया जा सकता है।



उन उपकरणों को बदले जो अब अप-टू-डेट विकल्प के साथ निर्माताओं द्वारा समर्थित नहीं हैं।



डाटा बैकअप

एक बेहतर तरीका ।



अपने महत्वपूर्ण डाटा का नियमित बैकअप लें और परिक्षण करें कि उन्हें पुनर्स्थापित किया जा सकता है।



एक वैकल्पिक डिवाइस पर नियमित अंतराल पर डाटा की बहाली का परिक्षण करें।



पहचानें कि क्या बैकअप की आवश्यकता है। यानि दस्तावेज़, फोटो, ई-मेल, संपर्क और कैलेंडर।



क्लाउड पर बैकअप लेने पर विचार करें और आप इसे किसी स्थान से एक्सेस कर पाएंगे।



सुनिश्चित करें कि आपके बैकअप वाले डिवाइस को स्थायी रूप से किसी भी नेटवर्क से नहीं जोड़ा गया है।



मालवेयर क्षति रोके।

अप्रत्याशित पॉप-अप, अजीब ई-मेल और .exe एक्सटेंशन फाइल से बचें।



सभी उपकरणों पर एंटीवायरस सॉफ्टवेयर का उपयोग करें। केवल अनुमोदित सॉफ्टवेयर स्थापित करें।



हटाने योग्य मीडिया को नियंत्रित करें। इसके बजाय ई-मेल या क्लाउड स्टोरेज के ज़रिये फाइल ट्रांसफर करने के लिए प्रोत्साहित करें।



अज्ञात स्रोतों से तृतीय पक्ष एप्लीकेशन डाउनलोड करने से रोके।



अपने नेटवर्क और इंटरनेट के बीच बफर जोन बनाने के लिए अपने फ़ायरवॉल पर स्विच करें।



स्वचलित तिथि विकल्प का उपयोग करके सभी सॉफ्टवेयर और फर्मवेयर को पैच करें।



पासवर्ड का उपयोग करना

अपने डाटा को सुरक्षित करना ।



एक ऐसे एन्क्रिप्शन उत्पाद का उपयोग करें जिसे बूट करने के लिए पासवर्ड की आवश्यकता हो।



आवधिक अंतराल पर पासवर्ड परिवर्तन लागू करें।



पासवर्ड/पिन सुरक्षा या सभी उपकरणों के लिए फिंगरप्रिंट पहचान पर स्विच करें।



डिवाइस पर मैनुफैक्चर्ड डिफ़ॉल्ट पासवर्ड बदलें।



बैंकिंग, ई-मेल और सोशल मीडिया साइट के लिए दो कारक प्रमाणीकरण (2FA) का उपयोग करें।



सुरक्षित भण्डारण प्रदान को और उपयोगकर्ता अपने पासवर्ड बनाती है।



आसानी से प्रेडिक्टेबल पासवर्ड (यानि परिवार, पालतू जानवर, पहला नाम, आदि) का उपयोग करने से बचें।



पासवर्ड मैनेजर टूल "मास्टर पासवर्ड" का उपयोग करें (जो अन्य सभी पासवर्ड तक पहुँच प्रदान करता है)।

कैरीमिनाटी का यूट्यूब चैनल (कैरीइज़लाइव) हैक किया गया

टू-फैक्टर ऑथेंटिकेशन सक्षम करें

यदि इनके खाते हैक किये जा चुके हैं, तो आपका खाता भी आसानी से हैक किया जा सकता है।



टू-फैक्टर ऑथेंटिकेशन के लिए इन चरणों का पालन करें।



सेटिंग → सुरक्षा → टू फैक्टर
ऑथेंटिकेशन



सेटिंग → सुरक्षा और लॉगिन →
टू फैक्टर ऑथेंटिकेशन



सेटिंग और गोपनीयता → खाते →
सुरक्षा → पाठ सन्देश



सेटिंग और गोपनीयता → लॉगिन
और सुरक्षा → टू फैक्टर
ऑथेंटिकेशन



गूगल खाता → सुरक्षा →
टू फैक्टर ऑथेंटिकेशन

10 इंटरनेट सुरक्षा

माता-पिता के लिए टिप्स

डिजिटल नागरिकता और इंटरनेट सुरक्षा।

प्रौद्योगिकी तक सभी पहुँच को अवरुद्ध न करें। अपने बच्चे को तकनीक उपयोग करना सीखने में मदद करें।



अभिभावक बनें, आप प्रभारी हैं। फ़िल्टरिंग सॉफ्टवेयर का उपयोग कर सीमाएं निर्धारित करें।



हमेशा अपने बच्चों को सिखाएं की उन्हें कौनसी व्यक्तिगत चीज़ें ऑनलाइन प्रकट नहीं करनी चाहिए (yappy संक्षिप्त)।



अपने बच्चे के साथ डिजिटल दुविधाओं को नेविगेट करें। पुरस्कार या दंड के रूप में उपकरण का उपयोग करने से बचें।



यदि वे कम उम्र के हैं तो अपने बच्चे को आयु प्रतिबन्ध (उदाहरण - 15+) वाली साइट के लिए साइन अप करने का समर्थन न दें।



अपने बच्चे के पसंदीदा ऐप्लिकेशन्स या साइट में रूचि लें। सह-दृश्य या सह-समय पर बनायें।



कार, बैडरूम और भोजन जैसे तकनीकी मुक्त क्षेत्रों के साथ पारिवारिक मीडिया समझौता करें।



अपने बच्चे को ऑनलाइन जानकारी फ़िल्टर करने में मदद करें, कल्पना और तथ्य में फर्क बताएं।



ग्रीन समय और स्क्रीन समय को संतुलित करें। बुनियादी विकासात्मक ज़रूरतों पर ध्यान दें।



माता-पिता के लिए और अधिक खोजपूर्ण विश्वसनीय संसाधन लाएं ताकि आप खुद को शिक्षित कर सकें।

10 इंटरनेट सुरक्षा

बच्चों के लिए टिप्स

डिजिटल नागरिकता और इंटरनेट सुरक्षा।

कानून : कई साइट और वेब उपकरण 13 + हैं। अधिकांश चित्र और कार्य ऑनलाइन कॉपीराइट द्वारा संरक्षित हैं।



फ्रेंड्स : माता-पिता की अनुमति के बिना ऑनलाइन दोस्तों को न जोड़े या न मिलाएं / दोस्तों की बताई हर बात पर भरोसा न करें।



प्रतिष्ठा : कुछ भी ऐसा पोस्ट न करें जिसे आप शिक्षक, परिवार, दोस्तों और भविष्य के नियोक्ताओं को नहीं दिखाना चाहेंगे।



बदमाशी : किसी को बताएं अगर आप सोचते हैं या देखते हैं कि आपके साथ या आपके जानने वाले के साथ साइबर बदमाशी हो रही है।



शिष्टाचार : हर समय विनम्र और सम्मानित रहे। दूसरों से ऑनलाइन ऐसे व्यवहार करें जैसा आप अपने लिए चाहते हैं।



बात करें : अपने माता-पिता को बताएं कि आप ऑनलाइन क्या कर रहे हैं। यदि आप किसी भी चीज़ के बारे में सुनिश्चित नहीं हैं, तो हमेशा एक विश्वसनीय वयस्क से पूछें।



गोपनीयता : अपनी व्यक्तिगत जानकारी को निजी रखें, आपका पूरा नाम, पता, फ़ोन नंबर, योजना, पासवर्ड और जन्मदिन।



प्रश्न : आप विश्वास नहीं कर सकते हैं कि आप जो भी पढ़ते हैं और ऑनलाइन देखते हैं क्योंकि वहां बहुत सी गलत और पक्षपाती जानकारी भी दी होती है।



खाता : कुछ समझदार ई-मेल पते और उपयोगकर्ता नाम चुनें और मज़बूत पासवर्ड का उपयोग करें और उन्हें दूसरों के साथ साझा न करें।

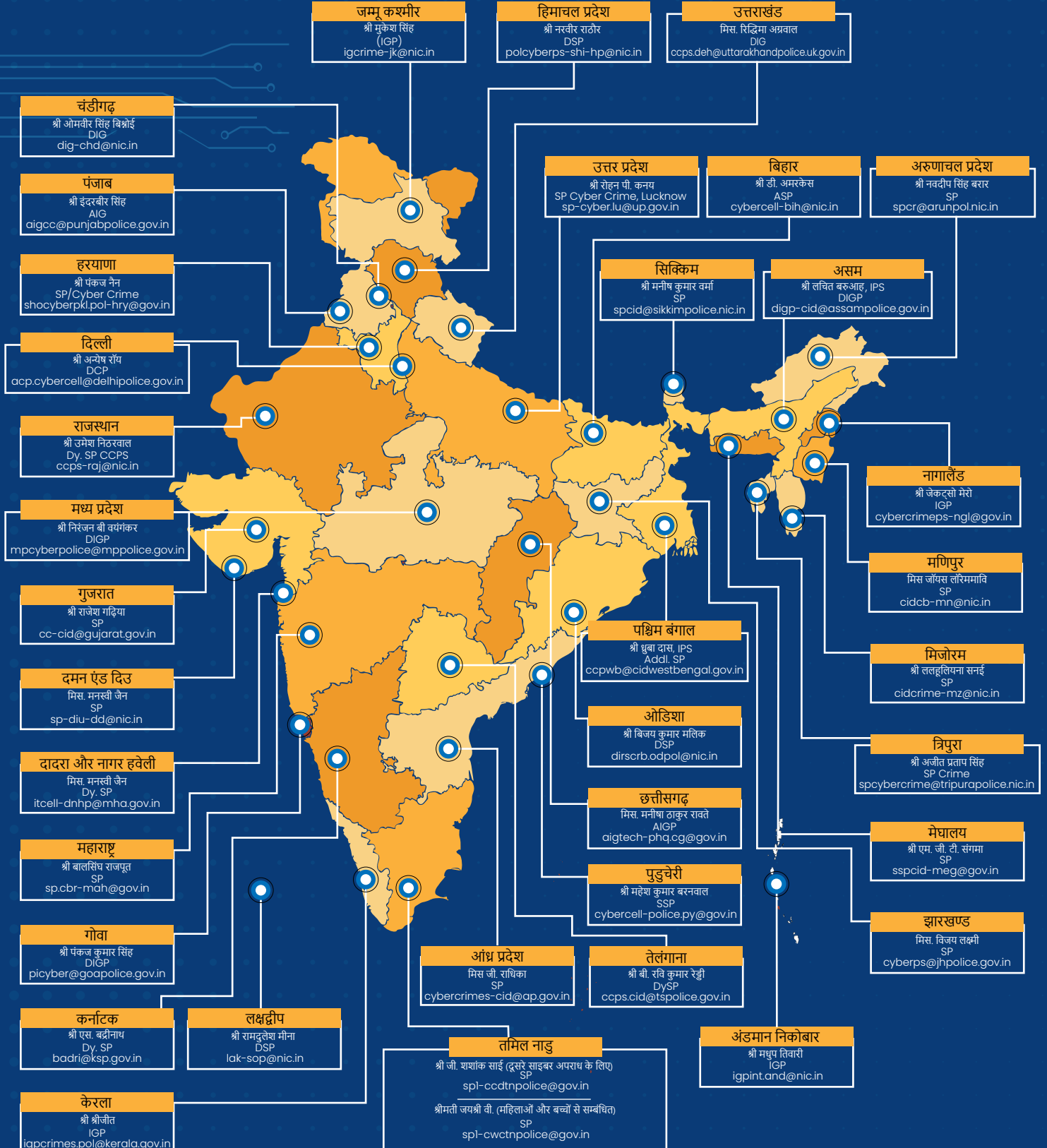


अनप्लग करें : अपना स्क्रीन समय और ग्रीन समय संतुलित करें। दरवाज़े से बहार निकलें, हिलें, डुलें, खेलें और आमने-सामने बातचीत करें।



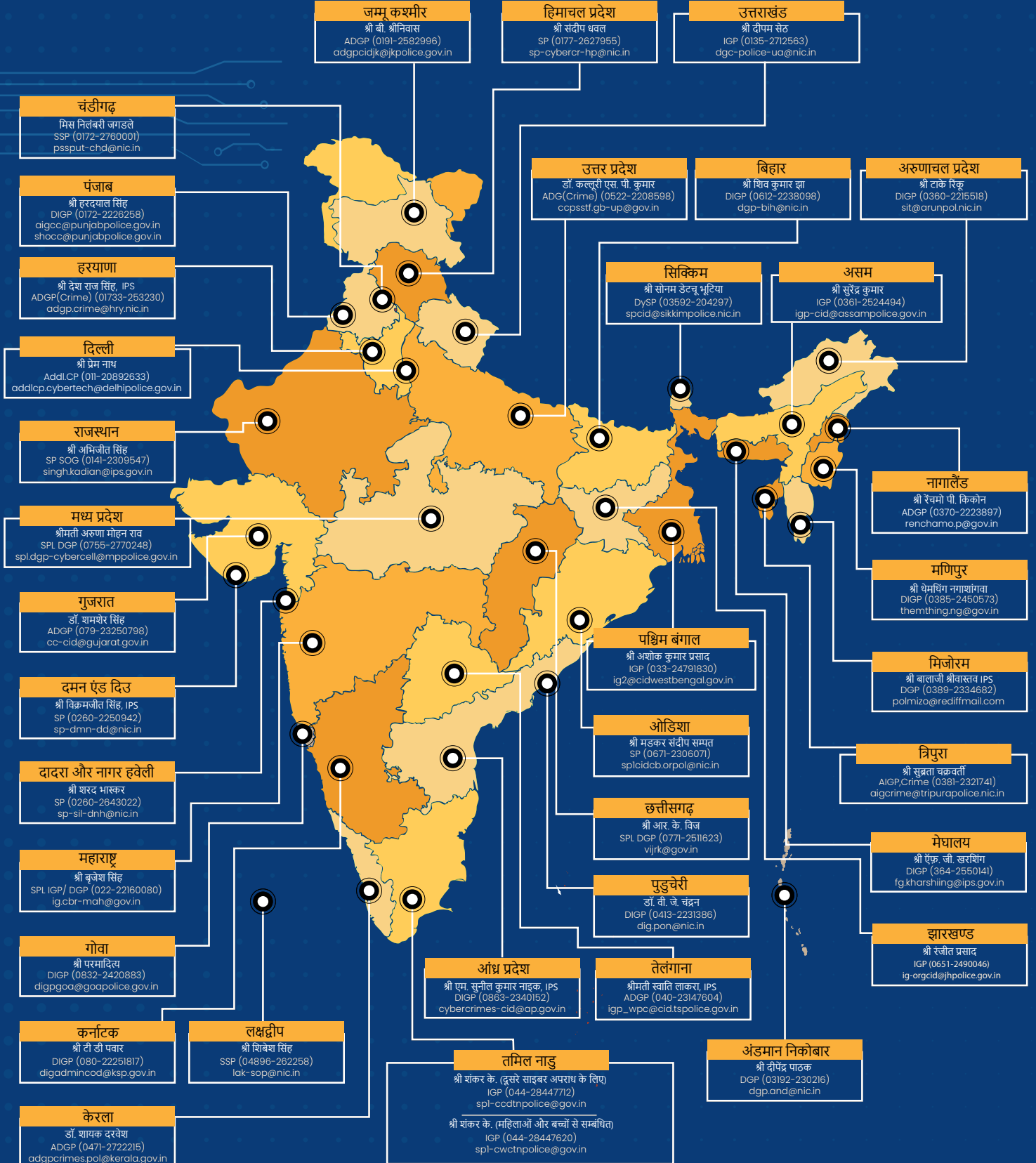
नोडल साइबर सेल अधिकारी

साइबर क्राइम रिपोर्टिंग पोर्टल
www.cybercrime.gov.in



शिकायत अधिकारी साइबर सेल

साइबर क्राइम रिपोर्टिंग पोर्टल
www.cybercrime.gov.in



आभार :

मिस. मितुशी बैरागी
उत्तर प्रदेश इंस्टिट्यूट ऑफ़ डिज़ाइन, नॉएडा।

मिस. श्रुति सिंह
उत्तर प्रदेश इंस्टिट्यूट ऑफ़ डिज़ाइन, नॉएडा।

श्रीमती. सूर्यमल्ला शालिनी
हिंदी पंडित



<https://www.canva.com/>



<https://slidesgo.com/>



<https://linktr.ee/>



<https://www.freepik.com/>



<https://internshala.com/>



ADVOCACY ON DIGITAL SAFETY

www.endnowfoundation.org

हैदराबाद - 500018

तेलंगाना, भारत (रेज. नंबर : 86/IV/2017)



Advocacy by
News Paper



Research &
Development



Advocacy by
Digital Safety Advocates



Advocacy by
FM Radio



Advocacy by
Student Ambassadors



Advocacy By
Organisations