ACCCF / अनुप्रयुक्त ज्ञान पुस्तकालय

खंड 11

रोकना, सूचित करना, संरक्षित करना और पुनर्प्राप्त करना।

स्पेनिश संस्करण · 2026

डिजिटल धोखाधड़ी पर नागरिक प्रतिक्रिया मैनुअल: फ़िशिंग, जबरदस्ती और समझौता किए गए खाते

WhatsApp, बैंकिंग, फ़र्ज़ी पेज, ऋण, निवेश, जबरदस्ती और अन्य लोगों की सहायता

धोखाधड़ी को और जानकारी दिए बिना तथा रिपोर्ट करने, खाते पुनर्प्राप्त करने और नए पीड़ितों को रोकने के लिए आवश्यक साक्ष्य नष्ट किए बिना शीघ्र कार्रवाई करने में सहायता करना।

नागरिकों, परिवारों, स्कूलों, छोटे व्यवसायों, सहायता टीमों और किसी प्रभावित व्यक्ति के साथ रहने वाले लोगों के लिए। आपातकाल, बैंकिंग और शिकायत के चैनल स्थानीय स्तर पर सत्यापित किए जाते हैं; किसी संदेश में मिले फ़ोन नंबर से उनका स्थान नहीं लिया जाता।

संपादकीय समन्वय: Jocsan Laguna · अमेरिकन साइबर सुरक्षा और कंप्यूटर फोरेंसिक परिषद

सामान्य तकनीकी मार्गदर्शिका और खुली शैक्षिक सामग्री। यह कानूनी सलाह, फोरेंसिक विशेषज्ञ की राय या बिना अधिकार के सिस्टम तक पहुँचने का निर्देश नहीं है। उदाहरण और डेटा काल्पनिक हैं; आकृतियाँ संपादकीय पुनर्निर्माण हैं।

विषय-सूची

दिखाई देने वाली पृष्ठ संख्या PDF संस्करण से संबंधित है। Word दस्तावेज़ खुलने पर इस अनुक्रमणिका को अद्यतन कर सकता है; शीर्षक आंतरिक नेविगेशन बनाए रखते हैं।

प्रस्तावना: जल्दबाजी धोखे का हिस्सा है 3

अध्याय 1. पहले मिनट 3

- **1.1 अगली कार्रवाई को रोकना** 3
- **1.2 जोखिम में रहे बिना आवश्यक साक्ष्य संरक्षित करना** 3
- **1.3 उपयुक्त लोगों को सूचित करना** 4

अध्याय 2. WhatsApp और समझौता किए गए खाते 4

- **2.1 विश्वसनीय वातावरण से पुनर्प्राप्ति** 4
- **2.2 अनुप्रयोगों की समीक्षा और दूरस्थ पहुंच** 5
- **2.3 प्रणाली के रूप में प्रमाणीकरण और पुनर्प्राप्ति** 5

अध्याय 3. धोखे के संकेत 6

- **3.1 दिखावे से पहले व्यवहार** 6
- **3.2 सामान्य परिदृश्य** 6
- **3.3 जब संदेश एक वास्तविक खाते से आता है** 6

अध्याय 4. जबरदस्ती और अंतरंग सामग्री 7

- **4.1 मोलभाव या प्रसार न करना** 7
- **4.2 आगे का खुलाव कम करना** 7
- **4.3 बिना पुनः पीड़ित बनाए सहयोग करना** 8

अध्याय 5. खातों की पुनर्प्राप्ति 8

- **5.1 पुनर्प्राप्ति का क्रम** 8
- **5.2 बैंकिंग और लेनदेन** 8
- **5.3 रिपोर्ट और अनुवर्ती कार्रवाई** 8

अध्याय 6. संरक्षण और अन्य लोगों की सहायता 9

- **6.1 न्यूनतम साक्ष्य पैकेज** 9
- **6.2 किसी बुजुर्ग या अनुभवहीन व्यक्ति की मदद कैसे करें** 9
- **6.3 स्थानीय निर्देशिका जो आप उपयोग कर सकते हैं** 10

अनुलग्नक A. आपातकालीन कार्ड 10

- **A.1 समझौता किया गया WhatsApp खाता** 10
- **A.2 भुगतान या स्थानांतरण किया गया** 10
- **A.3 जबरदस्ती या अंतरंग सामग्री** 11
- **A.4 परिजन या बैंक का संदिग्ध संदेश** 11

अनुलग्नक B. कालक्रम, निर्देशिका और अंतिम जाँच 11

- **B.1 न्यूनतम कालक्रम** 11
- **B.2 संकट से पहले भरने के लिए व्यक्तिगत निर्देशिका** 11
- **B.3 कानूनी ढांचा और समीक्षा** 12

प्रस्तावना: जल्दबाजी धोखे का हिस्सा है

धोखाधड़ी में प्रायः सोचने से पहले कोई छोटा लेकिन अपरिवर्तनीय काम कराया जाता है: कोड साझा करना, ऐप इंस्टॉल करना, कमीशन देना, लिंक खोलना या डेटा की पुष्टि करना। दिखावा विश्वसनीय हो सकता है और संदेश किसी ज्ञात लेकिन समझौता किए गए खाते से भी आ सकता है। पहली सुरक्षा एक स्पष्ट विराम है: भुगतान न करें, कोड साझा न करें, दूरस्थ पहुँच इंस्टॉल न करें और किसी ऐसे चैनल से सत्यापित करें जिसे आप पहले से जानते हैं।

यह मैनुअल आपको धोखेबाज़ की जाँच या उसके खेल में शामिल होने को नहीं कहता। इसका उद्देश्य हानि रोकना, आधिकारिक चैनलों से सूचित करना, आवश्यक साक्ष्य संरक्षित करना और अपना डिजिटल वातावरण पुनर्प्राप्त करना है। बैंक को कॉल करने या खाते की रिपोर्ट करने से पहले सब कुछ सिद्ध करना आवश्यक नहीं है। आदर्श केस फ़ाइल तैयार करने की प्रतीक्षा हानि बढ़ा सकती है। संरक्षण करते समय अन्य लोगों को जोखिम में नहीं डालना चाहिए।

यदि शारीरिक खतरा, नाबालिगों के लिए खतरा या कोई आपात स्थिति हो, तो सुरक्षा और अपने स्थान की आपातकालीन सेवाओं को प्राथमिकता दें। यदि सामग्री अंतरंग है, तो सहायता माँगने के लिए उसे अग्रेषित या विश्लेषण सेवाओं पर अपलोड न करें। फ़ाइल का प्रसार किए बिना संदेश, खाता, URL और तिथि संरक्षित की जा सकती है। किसी व्यक्ति की सहायता करने के लिए बिना आवश्यकता के उसकी निजी जानकारी देखना शामिल नहीं है।

> **आपातकालीन नियम**
> ऑफर या धमकी के साथ आने वाले नंबर, लिंक या क्यूआर का उपयोग न करें। आधिकारिक एप्लिकेशन खोलें, अपने कार्ड या अनुबंध नंबर पर कॉल करें, या संस्थान का ज्ञात पता स्वयं लिखें।

अध्याय 1. पहले मिनट

1.1 अगली कार्रवाई को रोकना

यदि आपने अब तक भुगतान या डेटा नहीं दिया है, तो यह जाँचने के लिए आगे न बढ़ें कि बात सच थी या नहीं। लिंक बंद करें, कॉल समाप्त करें और उत्तर न दें। यदि आप कोड, पासवर्ड या दूरस्थ पहुँच साझा कर चुके हैं, तो तुरंत दिशा बदलें: अपने खातों में प्रवेश करने के लिए दूसरे सुरक्षित डिवाइस का उपयोग करें, संस्थान से संपर्क करें और सत्रों की जाँच करें। पहली कार्रवाई को "पूर्ववत" करने के लिए कथित सहायता के दूसरे निर्देश पर अमल न करें।

यदि भुगतान कर चुके हैं, तो तुरंत आधिकारिक चैनल से बैंक या भुगतान प्रदाता से संपर्क करें और लेनदेन की रिपोर्ट, रोक या समीक्षा के विकल्प पूछें। यह वादा न करें कि धन वापस मिलेगा: परिणाम चैनल, समय, नियम और मामले पर निर्भर करता है। संदर्भ, तिथि, राशि, प्राप्तकर्ता खाता, प्रमाण-पत्र और संचार संरक्षित रखें; शर्म के कारण जानकारी न छिपाएँ।

1.2 जोखिम में रहे बिना आवश्यक साक्ष्य संरक्षित करना

वस्तु	क्या रखना है	क्या न करें
संदेश	पूरा पाठ, प्रेषक, तिथि, समय क्षेत्र और संदर्भ।	इसे संपादित करना या आपके साक्ष्य पाने के लिए उत्तर देना।
लिंक	पूरा URL और बिना किसी अतिरिक्त बातचीत के पृष्ठ।	इसे अपने मुख्य डिवाइस पर खोलना।
खाता	उपयोगकर्ता, प्रोफ़ाइल, आईडी और प्लेटफ़ॉर्म।	केवल नाम या तस्वीर पर भरोसा करना।
भुगतान	प्रमाण-पत्र, संदर्भ, राशि, प्राप्तकर्ता और चैनल।	उस एक कथित वसूली एजेंट के पास भेजा।

वस्तु	क्या रखना है	क्या न करें
ईमेल	हेडर और संलग्नक वाले ईएमएल।	केवल संदेश के मुख्य भाग का स्क्रीनशॉट रखना।
फोरेंसिक	क्या इंस्टॉल किया, कौन से कोड दिए, क्या बदलाव किए और किस समय।	उन चरणों को छिपाना जो प्रेषक को चेतावनी दे सकते हैं।

स्क्रीनशॉट में प्रेषक, तिथि और पर्याप्त सामग्री होनी चाहिए, केवल चिंताजनक वाक्यांश नहीं। संदेश ईमेल से आया हो तो उसे हेडर और संलग्नकों सहित EML में निर्यात करें। लिंक हो तो उसे दोबारा खोले बिना दर्ज करें। कोई ऐप इंस्टॉल हो तो सुरक्षा के लिए उसे हटाने से पहले उसका नाम, स्रोत, अनुमतियाँ और तिथि दर्ज करें; विश्लेषण के लिए उसका नमूना व्यक्तिगत फ़ोन में न रखें।

1.3 उपयुक्त लोगों को सूचित करना

यदि आपके खाते से समझौता हुआ है, तो किसी दूसरे चैनल—कॉल, पुनर्प्राप्ति ईमेल या सत्यापित खाते के संदेश—से अपने संपर्कों को सूचित करें। उन्हें प्रभावित नंबर पर धन या कोड न भेजने को कहें। एक संक्षिप्त चेतावनी नए पीड़ितों को रोक सकती है। चेतावनी देने के लिए धोखे का लिंक अग्रेषित न करें: संदेश का वर्णन करें और केवल आवश्यक जानकारी साझा करें।

> **संपर्क के लिए उपयोगी संदेश**
> “मैंने इस खाते का नियंत्रण खो दिया है। इस नंबर पर धन, कोड या दस्तावेज़ न भेजें और इसके लिंक न खोलें। मैं आधिकारिक चैनलों से पुनर्प्राप्ति की पुष्टि कर रहा/रही हूँ। यदि आपको कोई अनुरोध मिला हो, तो मुझे उसी नंबर पर कॉल करें जिसे आप पहले से जानते हैं।”



आकृति 1. जल्दबाज़ी से एक और हानि नहीं होनी चाहिए। हानि को सीमित करने और साक्ष्य सुरक्षित करने का संक्षिप्त क्रम। संपादकीय पुनर्संरेखण; यह वास्तविक साक्ष्य नहीं है।

अध्याय 2. WhatsApp और समझौता किए गए खाते

2.1 विश्वसनीय वातावरण से पुनर्प्राप्ति

ऐसे डिवाइस का उपयोग करें जिसमें छेड़छाड़ नहीं हुई हो, सिस्टम अद्यतन करें और आधिकारिक पुनर्प्राप्ति व्यवस्था से प्रवेश करें। पहले उस ईमेल को सुरक्षित करें जिससे अन्य खाते पुनर्प्राप्त होते हैं और उसके अग्रेषण नियम, फ़िल्टर, प्रतिनिधि तथा पुनर्प्राप्ति के तरीके जाँचें। इसके बाद सुरक्षित पासवर्ड प्रबंधक की मदद से पासवर्ड बदलें और सत्र तथा लिंक किए गए डिवाइस बंद करें। नया पासवर्ड किसी स्थायी सत्र या हमलावर द्वारा बनाए गए फ़िल्टर को नहीं हटाता।

पंजीकृत नंबर, ईमेल, PIN, लिंक किए गए डिवाइस, सत्र, बैकअप और पुनर्प्राप्ति संपर्क जाँचें। यदि ऑपरेटर ने आपका SIM बदल दिया है या सेवा बंद हो गई है, तो आधिकारिक चैनलों से ऑपरेटर से संपर्क करके सुरक्षा प्रक्रिया पूछें। अपने खाते की पुनर्प्राप्ति के लिए प्लेटफ़ॉर्म द्वारा अभी भेजा गया कोड किसी अजनबी के साथ साझा न करें।

2.2 अनुप्रयोगों की समीक्षा और दूरस्थ पहुंच

यदि आपने किसी अज्ञात सहायता ऐप को इंस्टॉल किया है, तो उसका नाम और अनुमतियाँ दर्ज करें और सुरक्षा की आवश्यकता के अनुसार डिवाइस को नेटवर्क से अलग करें। स्थायी पहुँच, प्रोफ़ाइल और विशेषाधिकार वाले ऐप की जाँच के लिए विश्वसनीय तकनीकी सहायता लें। केवल दूरस्थ पहुँच वाले प्रोग्राम की विंडो बंद करना पर्याप्त नहीं है। ऐप हटाना आवश्यक हो सकता है, लेकिन यदि जोखिम न बढ़े तो पहले पैकेज की जानकारी और देखे गए बदलाव संरक्षित करें।

यदि हमलावर ने स्क्रीन, फ़ाइलें या कोड देखे हैं, तो संबंधित क्रेडेंशियल समझौता किए गए मानें और उन्हें दूसरे डिवाइस से बदलें। उसी कथित "सहायता" से उसका टूल हटाने या अपने खातों की जाँच करने को न कहें। धोखेबाज़ संपर्क द्वारा सुझाए गए क्लीनर न चलाएँ: वे धोखे का दूसरा चरण हो सकते हैं।

2.3 प्रणाली के रूप में प्रमाणीकरण और पुनर्प्राप्ति

NIST SP 800-63B-4 प्रमाणीकरण, आश्वासन स्तर और फ़िशिंग-प्रतिरोधी प्रमाणीकरण से संबंधित है। व्यवहार में, यदि उपयोगकर्ता स्वयं कुंजी या दूसरा कारक दे दे या हमलावर पुनर्प्राप्ति को नियंत्रित करे, तो वह अब भी असुरक्षित हो सकता है। जाँचें कि कोड अपेक्षित चैनल पर आएँ और सेवा उपलब्ध कराए तो फ़िशिंग-प्रतिरोधी तरीकों को प्राथमिकता दें। कथित तकनीशियन की पहुँच आसान बनाने के लिए सुरक्षा अक्षम न करें।[1]

समीक्षा	सुरक्षित कार्रवाई	गलत से बचना
मुख्य ईमेल	नया पासवर्ड, बैकअप कोड और सत्र बदलें।	संदिग्ध मेल के साथ जुड़े खाते को पुनर्प्राप्त करना।
उपकरण	लिंक किए गए डिवाइस और सत्र बंद करें।	केवल पासवर्ड बदलना।
पुनर्प्राप्ति	फ़ोन, मेल, प्रश्न और संपर्क की जाँच करें।	हमलावर को नियंत्रण में एक चैनल छोड़ देना।
अनुप्रयोग	सूची, अनुमति और प्रोफ़ाइल की जाँच करें।	एक संदिग्ध ऐप को नाम पर भरोसा करना।
संपर्क	दूसरे चैनल से सूचित करें और चेतावनी साझा करें।	धोखेबाज़ को जल्दी लागू करने और रखने की अनुमति दें।

काल्पनिक मामला

एक व्यक्ति किसी कथित एजेंट के साथ WhatsApp का कोड साझा करता है। वह दूसरे फ़ोन से खाता पुनर्प्राप्त करता है, लिंक किए गए डिवाइस जाँचता है और पुनर्प्राप्ति ईमेल बदलता है। बाद में उसे एक ऐसा नियम मिलता है जो संदेशों को दूसरे पते पर अग्रेषित कर रहा था। यदि उसने केवल पासवर्ड बदला होता, तो वह नियम जानकारी का खुलाव करता रहता।

[1] NIST SP 800-63B-4 (जुलाई 2025)। प्रमाणीकरण और प्रमाणकों के प्रबंधन के दिशानिर्देश, जिनमें आश्वासन स्तर और फ़िशिंग-प्रतिरोधी प्रमाणीकरण शामिल हैं। खाते की पुनर्प्राप्ति भी जोखिम का हिस्सा है और इसे केवल पासवर्ड तक सीमित नहीं करना चाहिए। आधिकारिक ऑनलाइन स्रोत

अध्याय 3. धोखे के संकेत

3.1 दिखावे से पहले व्यवहार

लोगो, तस्वीर, मिलता-जुलता डोमेन और अच्छा लेखन पहचान का प्रमाण नहीं है। देखें कि संदेश क्या माँगता है: गोपनीयता, जल्दबाजी, इंस्टॉलेशन, स्थानांतरण, चैनल बदलना या धमकी। किसी वास्तविक परिजन को वाकई आपात स्थिति हो सकती है, लेकिन आप उसे ज्ञात नंबर पर कॉल कर सकते हैं। बैंक भी कोई कार्रवाई माँग सकता है, लेकिन उसे संदेश में दिए नंबर से सत्यापित न करें।

एक लिंक एक पते को दिखा सकता है और दूसरा खोल सकता है। दृश्यमान पाठ का उपयोग निर्णय लेने के लिए न करें; इसे खोलने से बचें और एप्लिकेशन से प्रवेश करें या ज्ञात आधिकारिक डोमेन लिखें। HTTPS वाला डोमेन केवल एक एन्क्रिप्टेड कनेक्शन को इंगित करता है, न कि साइट संस्था से संबंधित है या ईमानदार है। प्रमाणपत्र पृष्ठ के इरादे का आकलन नहीं करता है।

3.2 सामान्य परिदृश्य

परिदृश्य	जोखिम संकेत	तत्काल कार्रवाई
नए नंबर वाला परिजन	जल्दबाजी में धन या डेटा माँगना और कॉल से बचना।	पुराने नंबर या किसी अन्य परिजन को कॉल करें।
बैंक या सेवाएँ	कोड, पासवर्ड या दूरस्थ पहुँच माँगना।	कॉल समाप्त करें और आधिकारिक चैनल से संपर्क करें।
पुरस्कार या विरासत	पुरस्कार या विरासत जारी करने के लिए कमीशन या दस्तावेज़ माँगना।	भुगतान न करें और न ही पहचान पत्र भेजें।
निवेश	रिटर्न की गारंटी देना और जल्दी राशि बढ़ाने के लिए दबाव डालना।	जोखिम समझें, संदेश सहेजें और रिपोर्ट करें।
ऋण	संपर्क, जमानतियों और अग्रिम भुगतान की माँग।	ऐप इंस्टॉल न करें और संपर्क-सूची तक पहुँच की अनुमति न दें।
पार्सल या कूरियर सेवा	रिपोर्ट जारी करने के लिए लिंक पर छोटी राशि माँगना।	आधिकारिक चैनल पर रिपोर्ट ट्रैकिंग नंबर जाँचें।
रोजगार	जमा राशि, उपकरण या अग्रिम भुगतान वाले कार्य माँगना।	स्थानीय संपर्क द्वारा कंपनी की जाँच करें।
धन की वसूली	अतिरिक्त कमीशन देने पर धन पुनर्प्राप्त करने का वादा।	दूसरा बार भुगतान न करें, आधिकारिक चैनल पर रिपोर्ट करें।

3.3 जब संदेश एक वास्तविक खाते से आता है

किसी ज्ञात खाते से समझौता हो सकता है। विश्वास का आधार तस्वीर पहचानना नहीं, बल्कि अनुरोध को दूसरे माध्यम से सत्यापित करना है। कॉल पर ऐसा प्रश्न पूछें जिसका उत्तर वह व्यक्ति दे सके और, सबसे महत्वपूर्ण, उससे बात किए बिना स्थानांतरण न करें। वॉइस नोट या वीडियो का पुनः उपयोग या संश्लेषण भी हो सकता है; चैनल का सत्यापन फिर भी आवश्यक है।

> **उपयोगी घरेलू नियम**
> धन के अनुरोधों के लिए परिवार में सत्यापन वाक्यांश तय करना सहायक हो सकता है, लेकिन यह ज्ञात नंबर पर कॉल का विकल्प नहीं है। यदि अनुरोध हर तरह के सत्यापन से बचे, तो सुरक्षित उत्तर है कि कार्रवाई रोक दी जाए।



चित्र 2. संदेश व्यवहार से मूल्यांकन किया जाता है, न कि उपस्थिति से। लोगो और अच्छी भाषा पहचान सत्यापित नहीं करते हैं संपादकीय पुनर्संरेखण; यह वास्तविक सबूत नहीं है।

अध्याय 4. जबरदस्ती और अंतरंग सामग्री

4.1 मोलभाव या प्रसार न करना

यदि कोई अंतरंग सामग्री या निजी जानकारी प्रसारित करने की धमकी दे, तो भुगतान न करें और और सामग्री न भेजें। भुगतान से सामग्री हटने या जबरदस्ती समाप्त होने की गारंटी नहीं होती। अंतरंग सामग्री डाउनलोड किए या अधिक लोगों के साथ साझा किए बिना उपयोगकर्ता नाम, संदेश, URL, तिथि, प्राप्तकर्ता खाता और हर संबंधित संदर्भ संरक्षित करें। विश्वसनीय सहायता तथा विशेषज्ञ चैनलों या स्थानीय अधिकारियों से संपर्क करें।

यदि नाबालिग शामिल हों या तत्काल खतरा हो, तो सुरक्षा और विशेषज्ञ शिकायत को प्राथमिकता दें। ऐसी सामग्री न रखें और न पुनः वितरित करें जो अवैध हो सकती हो। उसे कॉपी किए बिना उसका स्वरूप बताएँ और सक्षम चैनल से निर्देश माँगें। सहायता इस शर्त पर नहीं होनी चाहिए कि व्यक्ति तस्वीरें दे या ऐसे विवरण बताए जिनकी कार्रवाई के लिए आवश्यकता नहीं है।

4.2 आगे का खुलाव कम करना

गोपनीयता, संपर्क-सूचियाँ, तस्वीरें, लिंक, पुनर्प्राप्ति और जुड़े खाते जाँचें। सुरक्षित डिवाइस से पासवर्ड बदलें और सत्र बंद करें। सामग्री का वर्णन किए बिना संपर्कों को सूचित करें। यदि जबरदस्ती करने वाला किसी दूसरे खाते से संपर्क करे, तो प्रोफ़ाइल के बीच संबंध का साक्ष्य रखें और, यदि जोखिम न बढ़े, संरक्षण से पहले उसे ब्लॉक करने से बचें।

मेक्सिको में Código Penal Federal के अनुच्छेद 199 Octies और 199 Nonies बिना सहमति वाली कुछ यौन अंतरंग सामग्री से जुड़े व्यवहारों को शामिल करते हैं, भले सामग्री पहचाने गए व्यक्ति की न हो। अन्य देशों में अपराधों के प्रकार और उपाय अलग होते हैं; स्थानीय कानून देखें और यह न मानें कि हर व्यवहार का नाम या प्रभाव एक जैसा है।[2]

[2] मेक्सिको। Código Penal Federal, अनुच्छेद 199 Octies और 199 Nonies, 13-03-2026 के संशोधन सहित संकलन: बिना सहमति वाली कुछ यौन अंतरंग सामग्री से जुड़े व्यवहार, भले सामग्री पहचाने गए व्यक्ति की न हो। आधिकारिक ऑनलाइन स्रोत

4.3 बिना पुनः पीड़ित बनाए सहयोग करना

यह न पूछें कि उसने सामग्री क्यों भेजी और न उसे दिखाने को कहें। ठोस सहायता दें: साथ रहें, न्यूनतम जानकारी दर्ज करें, सक्षम चैनल को कॉल करें, खाते जाँचें और नए संपर्क से बचें। दोषारोपण से व्यक्ति हमलावर की और माँगें मान सकता है। बिना निर्णय किए उसकी बात सुनने से अकेलेपन के कारण जबरदस्ती जारी रहने का जोखिम घट सकता है।

> **सहायता का मानदंड**
> केस फ़ाइल से पहले व्यक्ति की सुरक्षा करें। यदि संरक्षण की कोई कार्रवाई प्रसार या खतरा बढ़ा सकती हो, तो पहले विशेषज्ञ चैनल से परामर्श करें और केवल आवश्यक जानकारी दर्ज करें।

अध्याय 5. खातों की पुनर्प्राप्ति

5.1 पुनर्प्राप्ति का क्रम

पहले डिवाइस और मुख्य ईमेल सुरक्षित करें, फिर प्रमाणीकरण और पुनर्प्राप्ति के तरीके, उसके बाद सत्र, ऐप, बैंकिंग और संपर्क जाँचें। दोहराए गए पासवर्ड को अद्वितीय पासवर्ड से बदलें और विश्वसनीय पासवर्ड प्रबंधक का उपयोग करें। नई कुंजियाँ खुली कॉपी में न लिखें या समझौता किए गए उसी ईमेल पर न भेजें। यदि कोई सेवा पासकी या फ़िशिंग-प्रतिरोधी तरीके दे, तो सुरक्षित पुनर्प्राप्ति की व्यवस्था सुनिश्चित करके उनके उपयोग पर विचार करें।

ईमेल नियम, फ़िल्टर, प्रतिनिधित्व, स्वचालित उत्तर, अधिकृत ऐप, तीसरे पक्ष की पहुँच और प्रशासन प्रोफ़ाइल जाँचें। पासवर्ड बदलने के बाद भी हमलावर किसी फ़िल्टर या ऐप के ज़रिए पहुँच बनाए रख सकता है। यदि जोखिम न बढ़े तो बदलाव से पहले सेटिंग के स्क्रीनशॉट संरक्षित करें।

5.2 बैंकिंग और लेनदेन

संदर्भों के साथ बैंक से संपर्क करें और बिना विवरण बनाए बताएँ कि क्या हुआ। रोक, समीक्षा, अलर्ट और आवश्यक दस्तावेज़ों के बारे में पूछें। यदि कोई अपरिचित लेनदेन हो, तो प्रमाण-पत्र और उपलब्ध चैनल रिकॉर्ड माँगें। स्वीकृत प्रमाणीकरण अपने आप में अधिकार का प्रमाण नहीं है: कारक में बदलाव, नामांकन और अलर्ट निर्णायक हो सकते हैं।

मेक्सिको में क्रेडिट संस्थानों के लिए उनके नियामक ढाँचे के भीतर प्रमाण-पत्र, विसंगतियाँ, लॉग और अपरिचित लेनदेन के निपटान से संबंधित विशेष नियम हैं। अन्य देशों में शर्तें और समय-सीमाएँ बदलती हैं। केवल रिपोर्ट करने से बैंक धन वापसी की गारंटी नहीं देता, लेकिन समय पर सूचना महत्वपूर्ण हो सकती है। फ़ोलियो, तिथि, चैनल का नाम और उत्तर सुरक्षित रखें।[3][4][5]

5.3 रिपोर्ट और अनुवर्ती कार्रवाई

रिकॉर्ड	उपयोगी सामग्री	क्या साबित रखता है
बैंक	फ़ोलियो, तिथि, लेनदेन, चैनल और उत्तर।	जानकारी कार्रवाई और सूचना की पुष्टि।
प्लेटफ़ॉर्म	रिपोर्ट, पूर्जारएल, खाता और प्रतिक्रिया।	सामग्री और नीचे की प्रतियों के साथ संबंध।
स्थानीय प्राधिकरण	पनल, केस फ़ाइल, दस्तावेज़ और तिथि।	एक प्रकरण के साथ प्रतिस्थापन नहीं करना।

[3] Disposiciones de carácter general aplicables a las instituciones de crédito, अनुच्छेद 316 Bis, 316 Bis 1, 316 Bis 10 से 17: प्रमाण-पत्र, एन्क्रिप्शन, पहुँच, घटनाएँ, विसंगतियाँ, लॉग और समीक्षाएँ। आधिकारिक ऑनलाइन स्रोत

[4] पेरू। SBS 2286-2024: अनुच्छेद 20.3 में संशोधन, जो कुछ अपरिचित लेनदेन और उत्तरदायित्व से संबंधित है, जब तक उपयोगकर्ता का उत्तरदायित्व सिद्ध न हो। आधिकारिक ऑनलाइन स्रोत

[5] स्पेन। Real Decreto-ley 19/2018, अनुच्छेद 45, 66 और 67: अनधिकृत लेनदेन के लिए धन वापसी, जोखिम प्रबंधन और गंभीर घटनाओं की तत्काल सूचना। आधिकारिक ऑनलाइन स्रोत

रिकॉर्ड	उपयोगी सामग्री	क्या नोट रखता है
जोपरटर	Stivi, बदलाव, सुरक्षा और फ़ालोवा।	लाइन पर पुनर्प्राप्ति नियंत्रण।
सेवक	चेतावनी, पैनल और तारीख।	नए पीड़ितों को रोकना।
समाधा।	पारदर्शन और बाद के जलट।	स्वाथा पहुच पा दूसर प्रयास का पता लगाना।

पुनर्प्राप्ति का समापन

केवल इसलिए प्रक्रिया समाप्त न करें कि स्क्रीन पर आपका खाता फिर खुल गया है। पुनर्प्राप्ति, सत्र, फ़िल्टर, डिवाइस और संपर्कों की जाँच होने तथा रिपोर्टों का रिकॉर्ड मिलने के बाद ही इसे समाप्त करें।



चित्र 3। एक्सेस पुनर्प्राप्त करने का मतलब पर्यावरण की जाँच करना भी है। नया पासवर्ड हमलावर सत्र या नियम को नहीं हटाता। संपादकीय पुनर्निर्माण; यह वास्तविक सबूत नहीं है।

अध्याय 6. संरक्षण और अन्य लोगों की सहायता

6.1 न्यूनतम साक्ष्य पैकेज

पैकेज में कालक्रम, संदेश, यदि हो तो EML, URL, खाते, प्रमाण-पत्र, संदर्भ, रिपोर्ट और देखे गए बदलाव शामिल हैं। इसमें पासवर्ड, कोड, निजी कुंजियाँ या अनावश्यक व्यक्तिगत डेटा शामिल नहीं हैं। फ़ाइलें बिना संपादन के संरक्षित रखें और कार्यकारी प्रतियाँ अलग रखें। व्यक्ति को बड़ा संग्रह नहीं, बल्कि ऐसी वस्तुएँ चाहिए जिन्हें उसके वर्णन से जोड़ा जा सके।

कालक्रम में शामिल करें कि संदेश कब आया, व्यक्ति ने क्या किया, कब भुगतान किया, कब कॉल किया, क्या बदला और क्या रिपोर्ट किया। समय के साथ समय क्षेत्र लिखें और बताए गए समय तथा सत्यापित समय में अंतर करें। समय याद न हो तो उसे अनुमानित बताएँ; मनगढ़ंत सटीकता न जोड़ें।

6.2 किसी बुजुर्ग या अनुभवहीन व्यक्ति की मदद कैसे करें

उसके फ़ोन की जाँच से पहले अनुमति लें और हर कार्रवाई समझाएँ। उसका कार्ड न लें या पासवर्ड न माँगें। यदि उसे कुंजियाँ बदलनी हों, तो वह उन्हें निजी रूप से लिखे जबकि आप उसे बताएँ कि स्क्रीन पर क्या दिख रहा है। एक सरल नियम का अभ्यास करें: कोड

साझा न करें, दूरस्थ सहायता इंस्टॉल न करें और भुगतान से पहले कॉल करें। धैर्य रखें ताकि धोखे का दबाव सहायता करने वाले के दबाव में न बदले।

यदि व्यक्ति धन भेज चुका है, तो उसे न डाँटें। बैंक से संपर्क करने और संदर्भ इकट्ठा करने में सहायता करें। धोखाधड़ी बुद्धि की कमी का नहीं, विश्वास, डर और जल्दबाजी का फ़ायदा उठाती है। दूसरा धोखा प्रायः धन पुनर्प्राप्ति का वादा करता है: स्पष्ट करें कि संस्थागत सत्यापन के बिना कथित रूप से निधि जारी करने के लिए कोई अतिरिक्त कमीशन नहीं देना चाहिए।

6.3 स्थानीय निर्देशिका जो आप उपयोग कर सकते हैं

इंटरनेट से बिना सत्यापित नंबर कॉपी करने के बजाय, अपने ज्ञात चैनलों की निर्देशिका तैयार करें: कार्ड या अनुबंध पर दिया बैंक का आधिकारिक नंबर, ऑपरेटर, प्लेटफ़ॉर्म, स्थानीय पुलिस या लोक अभियोजक कार्यालय, उपभोक्ता संरक्षण, स्थानीय आपातकाल, पारिवारिक संपर्क और सहायता करने वाला व्यक्ति। संकट से पहले ये विवरण जाँचें और उन्हें कागज़ पर तथा सुलभ स्थान पर रखें।

आवश्यकता	वहाँ क्या जोड़ा जाना चाहिए	उपयोग न करें
बैंक संपर्क	कार्ड, अनुबंध या आधिकारिक ऐप में दिया नंबर।	कथित बैंक द्वारा भेजा गया फोन।
खाता या प्रकरण	ऑपरेटर के अंदर सहायता केंद्र।	ऐप अज्ञात टिप्पणी का लिंक।
SIM या लाइन	आधिकारिक ऐप, अनुबंध या शाखा में ऑपरेटर का संपर्क।	एक तीसरे पक्ष द्वारा भेजा गया कोड।
स्थानीय आपातकाल	आपके स्थान का आपातकालीन नंबर।	सामाजिक मीडिया पर उत्तर का इंतज़ार करना।
शिकायत	आपके क्षेत्राधिकार का लोक अभियोजक कार्यालय या आधिकारिक चैनल।	एकमात्र शिकायत के रूप में प्रकाशन।
भावनात्मक सहायता	विश्वसनीय व्यक्ति या स्थानीय सेवा।	सपने जो जल्दी सलाह देखने के लिए पूछते हैं।

समापन

सबसे अच्छी तैयारी पहले से तय किया गया विराम और सत्यापित निर्देशिका है। अगली हानि रोकने के लिए आपको अन्वेषक बनने की आवश्यकता नहीं है।

अनुलग्नक A. आपातकालीन कार्ड

A.1 समझौता किया गया WhatsApp खाता

संक्षिप्त क्रम

1. कोई और कोड साझा न करें और नए लिंक न खोलें।
2. सुरक्षित डिवाइस से आधिकारिक व्यवस्था के माध्यम से खाता पुनर्प्राप्त करें।
3. ईमेल, पुनर्प्राप्ति, लिंक किए गए डिवाइस और सत्र जाँचें।
4. पासवर्ड बदलें और अनजान एक्सेस बंद करें।
5. नियमों, फ़िल्टर, बैकअप और अधिकृत ऐप्स की समीक्षा करें।
6. किसी अन्य चैनल से संपर्क को सूचित करें।
7. संदेश, बदलाव और रिपोर्ट के फ़ोलियो संरक्षित करें।
8. नए प्रयासों की निगरानी करें; हमलावर से संपर्क न करें।

A.2 भुगतान या स्थानांतरण किया गया

संक्षिप्त क्रम

1. और धन या पुनर्प्राप्ति के नाम पर कमीशन न भेजें।
2. कार्ड, अनुबंध या आधिकारिक ऐप में दिए नंबर पर बैंक को कॉल करें।
3. संदर्भ, तिथि, राशि और प्राप्तकर्ता बताएँ तथा बिना कुछ बनाए घटना का वर्णन करें।
4. प्रमाण-पत्र, संदेश, URL और खाते संरक्षित करें।
5. रोक, समीक्षा और मामले के दस्तावेज़ों के बारे में पूछें।

8. फ़ाइलें और उपकरण सुरक्षित रखें।
7. मंच और स्थानीय प्राधिकरण को रिपोर्ट करें।
8. कथित प्राप्तकर्ता के निर्देशों का पालन न करें।

A.3 जबरदस्ती या अंतरंग सामग्री

सुरक्षित अनुक्रम

1. भुगतान न करें और अधिक सामग्री न भेजें।
2. मदद के लिए सामग्री को न फिर से भेजें और न ही अपलोड करें।
3. खाता, संदेश, यूआरएल, तिथियां और न्यूनतम संदर्भ बनाए रखें।
4. एक विश्वसनीय व्यक्ति और स्थानीय विशेषज्ञ चैनल खोजें।
5. खतरा या नाबालिगों के शामिल होने पर आपातकाल और विशेषज्ञ शिकायत को प्राथमिकता दें।
6. एक सुरक्षित डिवाइस से खाते और सत्र पुनर्प्राप्त करें।
7. आधिकारिक चैनलों के माध्यम से पोस्ट की रिपोर्ट करें।
8. अपने दम पर न तो जांच करें और न ही बातचीत करें।

A.4 परिजन या बैंक का संदिग्ध संदेश

कार्य करने से पहले सत्यापन

1. कार्रवाई को रोकें, भले ही यह तत्काल लगे।
2. कोड, पासवर्ड या रिमोट एक्सेस साझा न करें।
3. उस नंबर पर कॉल करें जिसे आप पहले से जानते थे, न कि संदेश पर।
4. दूसरे माध्यम से अनुरोध और पहचान सत्यापित करें।
5. पुष्टि किए बिना भुगतान न करें।
6. संदेश, यूआरएल, खाता और तिथि को सहेजें।
7. यदि वास्तविक खाते से समझौता हुआ है तो अपने संपर्कों को चेतावनी दें।

अनुलग्नक B. कालक्रम, निर्देशिका और अंतिम जाँच

B.1 न्यूनतम कालक्रम

तारीख / समय क्षेत्र	घटना और स्रोत	किया गया कार्य	फ़ाइलें / साक्ष्य
[लगभग या सटीक]	संपर्क प्राप्त और वस्तु खरीदार।	कोई अतिरिक्त बातचीत नहीं।	[ID]
[ ]	फोन, इंस्टालेशन, भुगतान या अपलोड।	जो वास्तव में हुआ।	[प्रमाण-पत्र]
[ ]	बैंक / प्लेटफ़ॉर्म से संपर्क।	रोक, समीक्षा या रिपोर्ट।	[फ़ाइलें]
[ ]	खाते की पुनर्प्राप्ति।	पासवर्ड, सत्र, डिवाइस और ऐप।	[पंजीकरण]
[ ]	संपर्कों को सूचना।	नए पीड़ितों को रोकथाम।	[पत्र]
[ ]	कार्य की समीक्षा।	स्वीकृत पहुंच या नया प्रमाण।	[लॉक्ड]

B.2 संकट से पहले भरने के लिए व्यक्तिगत निर्देशिका

सेवा	सत्यापित आधिकारिक चैनल	विकल्प
मुख्य बैंक	[फोन, जनादेश या ऐप पर नंबर]	[शाखा या आधिकारिक ऐप]
मोबाइल ऑपरेटर	[ऐप, जनादेश या शाखा]	[पुनर्प्राप्ति चैनल]
मुख्य प्लेटफ़ॉर्म	[आंतरिक सहायता फ़ॉर्म]	[शांत आधिकारिक ईमेल]
स्थानीय प्राधिकरण	[आधिकारिक साइट या फोन]	[लॉक्ड जानपदिक कार्यालय या सहायता पंक्ति]

समय	संस्थागत आधिकारिक चैनल	विकल्प
स्थानीय आपातकाल	[आपके स्थान का आधिकारिक नंबर]	[स्वास्थ्य सेवा या सुरक्षा]
संदेहास्पद व्यक्ति	[शांत नाम और ब्रांच]	[दूसरा संपर्क]

B.3 कानूनी ढांचा और समीक्षा

इलेक्ट्रॉनिक लेनदेन का विश्लेषण देश और क्षेत्र के डेटा संदेश, रिकॉर्ड और अपरिचित लेनदेन के नियमों के अनुसार किया जाता है। मेक्सिको में CCom 89–94 और 1205 तथा लागू CNBV प्रावधान देखे जाते हैं; पेरू में SBS नियम हैं; अर्जेंटीना में BCRA; स्पेन में RD-ley 19/2018। कोलंबिया और इक्वाडोर संदर्भ सहित संदेशों के संरक्षण की अपेक्षा करते हैं; चिली हस्ताक्षर के प्रभावों में अंतर करता है। केवल प्रमाण-पत्र प्रस्तुत करने से धन वापसी की कोई सार्वभौमिक गारंटी नहीं है।[6][7][8][9][10][11][12][13]

जांचने योग्य	अपेक्षित उत्तर
क्या नुकसान रोक गया है?	जब कोई नुकसान, फीस, इंस्टालेशन या प्रसार नहीं।
क्या सूचना दी गई?	बैंक, एटीएम, जीपरटेट, प्रोविकरण और संपर्क, जहां आवश्यक हो।
क्या साक्ष्य संरक्षित किए गए?	संपर्क, वॉउचरऐप, इंस्पेक्ट, प्रमाण पत्र, पारपत्र और फोलियम।
क्या पुनर्प्राप्ति हो गई?	डिवाइस, मेल, पासवर्ड, सेव, फ़ाइलें और ऐप।
क्या व्यक्ति को सुरक्षा है?	बिना खुलासे, दोषारोपण या दूसरे पीड़ित के।
आगे क्या है?	फ़ॉलोअप, लिखित कार्य, जर्नल और बाद की समीक्षा।

समापन

शीघ्र कार्रवाई का अर्थ आँख बंद करके कार्रवाई करना नहीं है। एक विराम, आधिकारिक चैनल और अच्छा कालक्रम पहले धोखे को कई धोखों में बदलने से रोक सकते हैं।

[6] Código de Comercio de México, अनुच्छेद 89–94 और 1205: डेटा संदेशों की तटस्थता, प्रेषक-संबंध, लिखित रूप, मूलता, अखंडता, पहुँच और स्वीकार्यता। आधिकारिक संकलन। आधिकारिक ऑनलाइन स्रोत

[7] Disposiciones de carácter general aplicables a las instituciones de crédito, अनुच्छेद 316 Bis, 316 Bis 1, 316 Bis 10 से 17: प्रमाण-पत्र, एन्क्रिप्शन, पहुँच, घटनाएँ, विसंगतियाँ, लॉग और समीक्षाएँ। आधिकारिक ऑनलाइन स्रोत

[8] पेरू। SBS 2286-2024: अनुच्छेद 20.3 में संशोधन, जो कुछ अपरिचित लेनदेन और उत्तरदायित्व से संबंधित है, जब तक उपयोगकर्ता का उत्तरदायित्व सिद्ध न हो। आधिकारिक ऑनलाइन स्रोत

[9] अर्जेंटीना. BCRA सूचना A 7783: कम से कम 90 दिनों के लिए उपलब्ध डिजिटल लेनदेन रिकॉर्ड और सुरक्षा घटनाओं की निगरानी। आधिकारिक ऑनलाइन स्रोत

[10] स्पेन। Real Decreto-ley 19/2018, अनुच्छेद 45, 66 और 67: अनधिकृत लेनदेन के लिए धन वापसी, जोखिम प्रबंधन और गंभीर घटनाओं की तत्काल सूचना। आधिकारिक ऑनलाइन स्रोत

[11] कोलंबिया। Ley 527 de 1999, अनुच्छेद 5–13, 16–25 और 28: डेटा संदेश, लिखित रूप, मूलता, अखंडता, स्वीकार्यता, संरक्षण, प्रेषण, प्राप्ति और डिजिटल हस्ताक्षर। आधिकारिक ऑनलाइन स्रोत

[12] इक्वाडोर। Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, अनुच्छेद 2, 6–8, 10–16: समतुल्यता, लिखित रूप, मूलता, संरक्षण, उत्पत्ति, प्रेषण, प्राप्ति और इलेक्ट्रॉनिक हस्ताक्षर। आधिकारिक ऑनलाइन स्रोत

[13] चिली। Ley 19.799 sobre documentos electrónicos y firma electrónica, अनुच्छेद 1–5: समतुल्यता, लिखित रूप, सरल/उन्नत हस्ताक्षर, तिथि और साक्ष्य मूल्य। आधिकारिक ऑनलाइन स्रोत