ACCCF / BIBLIOTHEK FÜR ANGEWANDTES WISSEN

11

BAND

Eindämmen, benachrichtigen, sichern und wiederherstellen

Spanische Ausgabe · 2026

Handbuch für die Reaktion von Bürgerinnen und Bürgern auf digitalen Betrug: Phishing, Erpressung und kompromittierte Konten

WhatsApp, Bankgeschäfte, gefälschte Seiten, Kredite, Investitionen, Erpressung und Unterstützung anderer Personen

Hilfe beim raschen Handeln, ohne den Betrügern weitere Informationen zu geben und ohne die Beweise zu vernichten, die für Meldungen, die Wiederherstellung von Konten und den Schutz weiterer möglicher Opfer erforderlich sind.

Für Bürgerinnen und Bürger, Familien, Schulen, kleine Unternehmen, Unterstützungsteams und Personen, die Betroffene begleiten. Notruf-, Bank- und Anzeigekanäle werden vor Ort überprüft; eine in einer Nachricht erhaltene Telefonnummer ersetzt sie nicht.

Redaktionelle Koordination: Jocsan Laguna · Amerikanischer Rat für Cybersicherheit und digitale Forensik

Allgemeiner technischer Leitfaden und offenes Bildungsmaterial. Er stellt keine Rechtsberatung oder forensisches Gutachten dar und enthält keine Anleitung zum unbefugten Zugriff auf Systeme. Beispiele und Daten sind fiktiv; die Abbildungen sind redaktionelle Rekonstruktionen.

Inhalt

Die sichtbare Seitennummerierung entspricht der PDF-Ausgabe. Word kann dieses Inhaltsverzeichnis beim Öffnen des Dokuments aktualisieren; die Überschriften ermöglichen weiterhin die interne Navigation.

Einleitung: Zeitdruck ist Teil der Täuschung ... 3
Kapitel 1. Die ersten Minuten ... 3
1.1 Die nächste Handlung unterbrechen ... 3
1.2 Das Wesentliche sichern, ohne weiterhin gefährdet zu sein ... 3
1.3 Die richtigen Personen benachrichtigen ... 4
Kapitel 2. WhatsApp und kompromittierte Konten ... 5
2.1 Wiederherstellung in einer vertrauenswürdigen Umgebung ... 5
2.2 Anwendungen und Fernzugriff überprüfen ... 5
2.3 Authentifizierung und Wiederherstellung als Gesamtsystem ... 5
Kapitel 3. Anzeichen von Täuschung ... 6
3.1 Verhalten zählt mehr als der äußere Anschein ... 6
3.2 Häufige Szenarien ... 6
3.3 Wenn die Nachricht von einem echten Konto stammt ... 7
Kapitel 4. Erpressung und intime Inhalte ... 7
4.1 Nicht verhandeln und nichts verbreiten ... 7
4.2 Spätere Gefährdungen verringern ... 8
4.3 Begleiten, ohne erneut zu victimisieren ... 8
Kapitel 5. Wiederherstellung von Konten ... 8
5.1 Reihenfolge der Wiederherstellung ... 8
5.2 Bank und Transaktionen ... 9
5.3 Meldung und Nachverfolgung ... 9
Kapitel 6. Beweissicherung und Unterstützung anderer Personen ... 10
6.1 Mindestumfang des Beweispakets ... 10
6.2 Älteren oder wenig erfahrenen Personen helfen ... 10
6.3 Lokale Kontaktstellen, die du tatsächlich nutzen kannst ... 11
Anhang A. Notfallkarten ... 11
A.1 WhatsApp-Konto kompromittiert ... 11
A.2 Zahlung oder Überweisung bereits erfolgt ... 11
A.3 Erpressung oder intime Inhalte ... 11
A.4 Verdächtige Nachricht von einem Angehörigen oder einer Bank ... 12
Anhang B. Chronologie, Kontaktverzeichnis und Abschlusskontrolle ... 12
B.1 Minimale Chronologie ... 12
B.2 Persönliches Kontaktverzeichnis zur Vorbereitung auf eine Krise ... 12
B.3 Rechtsrahmen und Überprüfung ... 13

Einleitung: Zeitdruck ist Teil der Täuschung

Betrüger verlangen häufig eine kleine, unumkehrbare Handlung, bevor du nachdenken kannst: einen Code weitergeben, eine Anwendung installieren, eine Gebühr zahlen, einen Link öffnen oder Daten bestätigen. Der äußere Anschein kann überzeugend sein, und die Nachricht kann von einem bekannten, kompromittierten Konto stammen. Die erste Abwehr ist eine bewusste Pause: Nichts zahlen, keine Codes weitergeben, keinen Fernzugriff installieren und alles über einen dir bereits bekannten Kanal überprüfen.

Dieses Handbuch verlangt nicht, dass du den Betrüger selbst ermittelst oder auf sein Spiel eingehst. Es hilft dir, den Schaden zu begrenzen, offizielle Stellen zu benachrichtigen, das Erforderliche aufzubewahren und die Kontrolle über deine Umgebung zurückzugewinnen. Du musst nicht alles beweisen, bevor du die Bank anrufst oder ein Konto meldest. Auf ein perfektes Dossier zu warten, kann den Schaden vergrößern. Die Beweissicherung erfolgt, ohne weitere Personen zu gefährden.

Bei körperlicher Bedrohung, Gefahr für Minderjährige oder einem Notfall haben deine Sicherheit und die örtlichen Notdienste Vorrang. Verschicke intime Inhalte nicht erneut, um Hilfe zu erhalten, und lade sie nicht zu Analysediensten hoch. Du kannst Nachricht, Konto, URL und Datum aufbewahren, ohne die Datei zu verbreiten. Eine Person zu unterstützen bedeutet nicht, ohne Not ihre Privatsphäre zu durchsuchen.

> **Notfallregel**
> Verwende nicht die Telefonnummer, den Link oder den QR-Code, der mit dem Angebot oder der Drohung eingegangen ist. Öffne die offizielle Anwendung, rufe die Nummer auf deiner Karte oder in deinem Vertrag an oder gib die bekannte Adresse der Einrichtung selbst ein.

Kapitel 1. Die ersten Minuten

1.1 Die nächste Handlung unterbrechen

Wenn du noch nicht gezahlt und keine Daten übermittelt hast, setze den Kontakt nicht fort, nur um zu prüfen, ob alles stimmt. Schließe den Link, beende das Gespräch und antworte nicht. Wenn du bereits einen Code, ein Passwort oder Fernzugriff preisgegeben hast, ändere sofort dein Vorgehen: Nutze ein anderes sicheres Gerät für den Zugriff auf deine Konten, kontaktiere die Einrichtung und überprüfe die Sitzungen. Führe keine zweite Anweisung des angeblichen Supports aus, um die erste angeblich rückgängig zu machen.

Wenn du bereits gezahlt hast, kontaktiere sofort die Bank oder den Zahlungsdienstleister über den offiziellen Kanal und frage nach Möglichkeiten, den Vorgang zu melden, zu sperren oder zu überprüfen. Versprich niemandem, dass das Geld zurückerstattet wird: Das Ergebnis hängt vom Zahlungsweg, dem Zeitpunkt, den Vorschriften und dem Einzelfall ab. Bewahre Referenz, Datum, Betrag, Empfängerkonto, Zahlungsbeleg und Kommunikation auf und verschweige aus Scham keine Informationen.

1.2 Das Wesentliche sichern, ohne weiterhin gefährdet zu sein

Gegenstand	Was aufzubewahren ist	Was zu vermeiden ist
Nachricht	Vollständiger Text, Absender, Datum, Zeitzone und Kontext.	Sie zu bearbeiten oder zu antworten, um weitere Beweise zu erhalten.
Link	Vollständige URL und Seitenansicht, ohne weitere Interaktion.	Ihn auf deinem Hauptgerät zu öffnen.

Gegenstand	Was aufzubewahren ist	Was zu vermeiden ist
Konto	Benutzername, Profil, Kennung und Plattform.	Sich allein auf Namen oder Fotos zu verlassen.
Zahlung	Beleg, Referenz, Betrag, Empfänger und Zahlungsweg.	Ihn an einen angeblichen Rückholungsbeauftragten zu senden.
E-Mail	EML-Datei mit Kopfzeilen und Anhängen.	Nur einen Screenshot des Nachrichtentexts aufzubewahren.
Handlungen	Was installiert wurde, welche Codes preisgegeben wurden, welche Änderungen erfolgten und zu welchen Uhrzeiten.	Schritte zu verschweigen, die den Zugriff erklären könnten.

Der Screenshot muss Absender, Datum und ausreichend Inhalt zeigen, nicht nur den alarmierenden Satz. Bei einer E-Mail wird eine EML-Datei mit Kopfzeilen und Anhängen exportiert. Ein Link wird notiert, ohne ihn erneut aufzurufen. Bei einer installierten Anwendung werden Name, Quelle, Berechtigungen und Datum notiert, bevor sie aus Sicherheitsgründen deinstalliert wird; zu Analysezwecken wird keine Kopie auf dem privaten Telefon behalten.

1.3 Die richtigen Personen benachrichtigen

Wenn dein Konto kompromittiert wurde, warne deine Kontakte über einen anderen Kanal: telefonisch, über dein Wiederherstellungs-E-Mail-Konto oder mit einer Nachricht von einem bestätigten Konto. Bitte sie, weder Geld noch Codes an die betroffene Nummer zu senden. Eine kurze Warnung kann weitere Opfer verhindern. Leite den betrügerischen Link nicht als Warnung weiter: Beschreibe die Nachricht und teile nur die erforderlichen Angaben.

> **Hilfreiche Nachricht an Kontakte**
> „Ich habe die Kontrolle über dieses Konto verloren. Sende kein Geld, keine Codes und keine Dokumente an diese Nummer und öffne keine ihrer Links. Ich kümmere mich über offizielle Kanäle um die Wiederherstellung. Wenn du eine Aufforderung erhalten hast, ruf mich unter der dir bereits bekannten Nummer an.“



Abbildung 1. Dringlichkeit darf keinen weiteren Schaden verursachen. Kurze Abfolge zur Schadensbegrenzung und Beweissicherung. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

Kapitel 2. WhatsApp und kompromittierte Konten

2.1 Wiederherstellung in einer vertrauenswürdigen Umgebung

Verwende ein Gerät, das nicht manipuliert wurde, aktualisiere das System und nutze die offiziellen Wiederherstellungsverfahren. Ändere zuerst das Passwort des E-Mail-Kontos, über das andere Konten wiederhergestellt werden können, und überprüfe Weiterleitungsregeln, Filter, delegierte Zugriffe und Wiederherstellungsmethoden. Ändere anschließend die übrigen Passwörter mit einem sicheren Passwortmanager und melde alle Sitzungen und verknüpften Geräte ab. Ein neues Passwort beendet weder eine bestehende Sitzung noch entfernt es einen vom Angreifer eingerichteten Filter.

Überprüfe hinterlegte Rufnummer, E-Mail-Adresse, PIN, verknüpfte Geräte, Sitzungen, Sicherungskopien und Wiederherstellungskontakte. Wenn der Anbieter deine SIM-Karte ausgetauscht hat oder der Dienst nicht mehr funktioniert, kontaktiere ihn über offizielle Kanäle und frage nach dem Schutzverfahren. Gib den Code, den die Plattform dir gerade zur Wiederherstellung deines eigenen Kontos gesendet hat, niemals an Unbekannte weiter.

2.2 Anwendungen und Fernzugriff überprüfen

Wenn du eine unbekannte Support-Anwendung installiert hast, notiere ihren Namen und ihre Berechtigungen und trenne das Gerät bei Bedarf zum Schutz vor weiteren Zugriffen vom Netzwerk. Hole vertrauenswürdige technische Hilfe, um Persistenzmechanismen, Profile und Anwendungen mit erweiterten Rechten zu überprüfen. Es genügt nicht, das Fenster des Fernzugriffsprogramms zu schließen. Eine Deinstallation kann erforderlich sein; sichere jedoch zuerst die Paketinformationen und beobachteten Änderungen, sofern dies das Risiko nicht erhöht.

Wenn der Angreifer deinen Bildschirm, Dateien oder Codes sehen konnte, betrachte die betreffenden Zugangsdaten als kompromittiert und ändere sie von einem anderen Gerät aus. Bitte nicht denselben angeblichen Support, sein Werkzeug zu deinstallieren oder deine Konten zu überprüfen. Führe keine Reinigungsprogramme aus, die der betrügerische Kontakt empfiehlt: Sie können die nächste Stufe der Täuschung sein.

2.3 Authentifizierung und Wiederherstellung als Gesamtsystem

NIST SP 800-63B-4 behandelt Authentifizierung, Vertrauensniveaus und phishing-resistente Authentifizierung. In der Praxis kann selbst ein Schlüssel oder zweiter Faktor verwundbar bleiben, wenn die nutzende Person ihn weitergibt oder der Angreifer die Wiederherstellung kontrolliert. Prüfe, ob Codes über den erwarteten Kanal ankommen, und bevorzuge phishing-resistente Verfahren, sofern der Dienst sie anbietet. Deaktiviere keine Schutzfunktionen, um dem angeblichen Techniker den Zugriff zu erleichtern.[1]

Prüfpunkt	Sicheres Vorgehen	Vermiedener Fehler
Haupt-E-Mail-Konto	Neues Passwort, alle Sitzungen abgemeldet, Filter und Weiterleitungen überprüft.	Andere Konten über das kompromittierte E-Mail-Konto wiederherstellen.
Geräte	Verknüpfte Geräte abmelden und unbekannte Zugriffe entfernen.	Nur das Passwort ändern.

[1] NIST SP 800-63B-4 (Juli 2025). Richtlinien zur Authentifizierung und Verwaltung von Authentikatoren, einschließlich Vertrauensniveaus und phishing-resistenter Authentifizierung. Die Kontowiederherstellung ist Teil des Risikos und darf nicht auf Passwörter reduziert werden. Offizielle Online-Quelle

Prüfpunkt	Sicheres Vorgehen	Vermiedener Fehler
Wiederherstellung	Rufnummer, E-Mail-Adresse, Sicherheitsfragen und Kontakte überprüfen.	Einen vom Angreifer kontrollierten Wiederherstellungskanal bestehen lassen.
Anwendungen	Herkunft, Berechtigungen und Profile überprüfen.	Dem Namen einer Support-App vertrauen.
Kontakte	Über einen anderen Kanal benachrichtigen und eine Warnung teilen.	Zulassen, dass der Betrug bei anderen Personen fortgesetzt wird.

Fiktiver Fall

Eine Person gibt ihren WhatsApp-Code an einen angeblichen Mitarbeiter weiter. Von einem anderen Telefon aus stellt sie das Konto wieder her, überprüft verknüpfte Geräte und ändert die Wiederherstellungs-E-Mail-Adresse. Anschließend entdeckt sie eine Regel, die Nachrichten an eine andere Adresse weitergeleitet hat. Hätte sie nur das Passwort geändert, wären durch diese Regel weiterhin Informationen offengelegt worden.

Kapitel 3. Anzeichen von Täuschung

3.1 Verhalten zählt mehr als der äußere Anschein

Logo, Foto, eine ähnlich aussehende Domain und fehlerfreie Sprache belegen keine Identität. Prüfe, was die Nachricht verlangt: Geheimhaltung, Dringlichkeit, eine Installation, eine Überweisung, einen Kanalwechsel oder eine Drohung. Ein Angehöriger kann tatsächlich einen Notfall haben, aber du kannst ihn unter der bekannten Nummer anrufen. Auch eine Bank kann eine Handlung verlangen; überprüfe sie jedoch nicht über die im Text genannte Nummer.

Ein Link kann eine Adresse anzeigen und eine andere öffnen. Verlasse dich nicht auf den sichtbaren Text; öffne ihn nicht, sondern nutze die Anwendung oder gib die bekannte offizielle Domain selbst ein. HTTPS bei einer Domain bedeutet nur, dass die Verbindung verschlüsselt ist, nicht dass die Seite zur Einrichtung gehört oder vertrauenswürdig ist. Das Zertifikat beurteilt nicht die Absicht der Seite.

3.2 Häufige Szenarien

Szenario	Warnsignal	Sofortige Reaktion
Angehöriger mit neuer Rufnummer	Verlangt dringend Geld oder Daten und vermeidet ein Telefonat.	Die frühere Nummer oder einen anderen Angehörigen anrufen.
Bank oder Support	Verlangt Code, Passwort oder Fernzugriff.	Auflegen und über den offiziellen Kanal Kontakt aufnehmen.
Gewinn oder Erbschaft	Verlangt eine Gebühr oder Dokumente für die Auszahlung.	Nichts zahlen und keinen Ausweis senden.
Investition	Garantiert Erträge und drängt zu höheren Einzahlungen.	Nichts weiter einzahlen; Beweise sichern und den Vorfall melden.
Kredit	Verlangt Kontakte, Berechtigungen und Vorauszahlungen.	Nichts installieren und keinen Zugriff auf das Adressbuch erlauben.
Paketdienst	Kleine Gebühr über einen Link, um eine Sendung freizugeben.	Die Sendungsnummer über den offiziellen Kanal überprüfen.
Stellenangebot	Verlangt eine Kaution, Arbeitsmaterial oder Aufgaben gegen Vorauszahlung.	Das Unternehmen über einen unabhängig ermittelten Kontakt überprüfen.

Szenario	Warnsignal	Sofortige Reaktion
Rückholung von Geld	Verspricht die Rückholung gegen eine weitere Gebühr.	Kein zweites Mal zahlen; den Vorfall über den offiziellen Kanal melden.

3.3 Wenn die Nachricht von einem echten Konto stammt

Ein bekanntes Konto kann kompromittiert sein. Vertrauen beruht nicht auf einem wiedererkannten Foto, sondern auf der Überprüfung der Bitte über einen anderen Weg. Stelle eine Frage, die die Person am Telefon beantworten kann, und überweise vor allem nichts, bevor du mit ihr gesprochen hast. Auch eine Sprachnachricht oder ein Video kann wiederverwendet oder synthetisch erzeugt werden; die Überprüfung über einen anderen Kanal bleibt erforderlich.

> **Hilfreiche Regel für den Alltag**
> Ein in der Familie vereinbarter Prüfsatz für Geldbitten kann helfen, ersetzt aber nicht den Anruf unter einer bekannten Nummer. Wenn jede Überprüfung abgelehnt wird, ist Abbruch die sichere Antwort.



Abbildung 2. Eine Nachricht wird anhand des Verhaltens beurteilt, nicht anhand ihres äußeren Anscheins. Logos und fehlerfreie Sprache bestätigen keine Identität. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

Kapitel 4. Erpressung und intime Inhalte

4.1 Nicht verhandeln und nichts verbreiten

Wenn jemand damit droht, intime Inhalte oder private Informationen zu verbreiten, zahle nicht und sende kein weiteres Material. Eine Zahlung garantiert weder die Löschung noch das Ende der Erpressung. Bewahre Benutzername, Nachrichten, URL, Datum, Empfängerkonto und alle Referenzen auf, ohne die intimen Inhalte herunterzuladen oder an weitere Personen weiterzugeben. Suche vertrauenswürdige Unterstützung sowie spezialisierte Stellen oder örtliche Behörden auf.

Sind Minderjährige betroffen oder besteht unmittelbare Gefahr, haben Schutz und eine Meldung an spezialisierte Stellen Vorrang. Material, das rechtswidrig sein könnte, wird weder gespeichert noch weiterverbreitet. Beschreibe den Gegenstand, ohne ihn zu kopieren, und bitte die zuständige Stelle um

Anweisungen. Hilfe darf nicht davon abhängig gemacht werden, dass die betroffene Person Bilder aushändigt oder Details schildert, die für das Handeln nicht erforderlich sind.

4.2 Spätere Gefährdungen verringern

Überprüfe Datenschutzeinstellungen, Kontaktlisten, Fotos, Links, Wiederherstellungsoptionen und verbundene Konten. Ändere Passwörter von einem sicheren Gerät aus und melde alle Sitzungen ab. Informiere Kontakte, ohne das Material zu beschreiben. Wenn sich der Erpresser über ein anderes Konto meldet, dokumentiere die Verbindung zwischen den Profilen und blocke ihn nicht vor der Beweissicherung, sofern dadurch kein zusätzliches Risiko entsteht.

In Mexiko erfassen Artikel 199 Octies und Artikel 199 Nonies im Código Penal Federal bestimmte Handlungen im Zusammenhang mit sexuell intimen Inhalten ohne Einwilligung, auch wenn das Material nicht die identifizierte Person zeigt. In anderen Ländern unterscheiden sich Straftatbestände und Rechtswege; die örtliche Rechtslage ist zu prüfen, ohne anzunehmen, dass jede Handlung überall denselben Namen oder dieselben Rechtsfolgen hat.[2]

4.3 Begleiten, ohne erneut zu victimisieren

Frage nicht, warum die Person das Material gesendet hat, und bitte sie nicht, es zu zeigen. Biete konkrete Hilfe an: Sei für sie da, dokumentiere das Nötigste, rufe die zuständige Stelle an, überprüfe Konten und verhindere weitere Kontaktaufnahmen. Schuldgefühle können dazu führen, dass die Person weitere Forderungen des Täters erfüllt. Urteilsfreies Zuhören kann verhindern, dass die Erpressung durch Isolation fortgesetzt wird.

> **Grundsatz für Hilfeleistungen**
> Schütze die Person vor der Akte. Wenn eine Maßnahme zur Beweissicherung die Verbreitung oder Gefahr erhöhen könnte, konsultiere zuerst die spezialisierte Stelle und dokumentiere nur das unbedingt Erforderliche.

Kapitel 5. Wiederherstellung von Konten

5.1 Reihenfolge der Wiederherstellung

Sichere zuerst Gerät und Haupt-E-Mail-Konto, danach Authentifizierung und Wiederherstellungsmethoden und anschließend Sitzungen, Anwendungen, Bankzugänge und Kontakte. Ersetze mehrfach verwendete Passwörter durch einzigartige Passwörter und nutze einen vertrauenswürdigen Passwortmanager. Notiere neue Zugangsdaten nicht in einer offen herumliegenden Liste und sende sie nicht an dasselbe kompromittierte E-Mail-Konto. Wenn ein Dienst Passkeys oder phishing-resistente Verfahren anbietet, prüfe deren Einsatz zusammen mit einer sicheren Wiederherstellungsmöglichkeit.

Überprüfe E-Mail-Regeln, Filter, delegierte Zugriffe, automatische Antworten, autorisierte Anwendungen, Drittanbieterzugriffe und Verwaltungsprofile. Ein Angreifer kann trotz eines neuen Passworts über einen Filter oder eine Anwendung Zugriff behalten. Fertige vor Änderungen Screenshots der Konfiguration an, sofern dies das Risiko nicht erhöht.

[2] Mexiko. Código Penal Federal, Artikel 199 Octies und 199 Nonies, Textfassung mit der Reform vom 13-03-2026: bestimmte Handlungen im Zusammenhang mit sexuell intimen Inhalten ohne Einwilligung, auch wenn das Material nicht die identifizierte Person zeigt. Offizielle Online-Quelle

5.2 Bank und Transaktionen

Kontaktiere die Bank mit den Referenzen und beschreibe den Vorfall, ohne Einzelheiten zu erfinden. Frage nach Sperrung, Überprüfung, Warnmeldungen und erforderlichen Dokumenten. Bei einer nicht anerkannten Transaktion fordere den Beleg und die verfügbaren Aufzeichnungen des verwendeten Kanals an. Eine erfolgreiche Authentifizierung beweist für sich allein keine Autorisierung: Änderungen am Faktor, die Registrierung neuer Verfahren und Warnmeldungen können entscheidend sein.

In Mexiko gelten für Kreditinstitute besondere Vorschriften zu Belegen, Vorfällen, Protokollen und der Bearbeitung nicht anerkannter Transaktionen im Rahmen ihres jeweiligen Regimes. In anderen Ländern unterscheiden sich Bedingungen und Fristen. Eine Bank garantiert nicht allein aufgrund einer Meldung die Rückerstattung, aber eine rechtzeitige Benachrichtigung kann erheblich sein. Bewahre Vorgangsnummer, Datum, Bezeichnung des Kanals und Antwort auf.[3][4][5]

5.3 Meldung und Nachverfolgung

Aufzeichnung	Nützlicher Inhalt	Warum das wichtig ist
Bank	Vorgangsnummer, Datum, Transaktion, Kanal und Antwort.	Nachverfolgung und Bestätigung der Meldung.
Plattform	Meldung, URL, Konto und Antwort.	Zuordnung zu Inhalten und künftigen Kopien.
Örtliche Behörde	Kanal, Aktenzeichen, Dokumente und Datum.	Die Meldung nicht durch eine Veröffentlichung ersetzen.
Mobilfunkanbieter	SIM-Karte, Änderungen, Schutz und Vorgangsnummer.	Die Wiederherstellung über die Rufnummer kontrollieren.
Kontakte	Benachrichtigung, Kanal und Datum.	Weitere Opfer verhindern.
Überprüfung	Spätere Änderungen und Warnmeldungen.	Persistenz oder einen zweiten Versuch erkennen.

Abschluss der Wiederherstellung

Schließe den Vorgang nicht ab, nur weil du dein Konto wieder öffnen kannst. Schließe ihn ab, wenn Wiederherstellungsoptionen, Sitzungen, Filter, Geräte und Kontakte überprüft wurden und du Aufzeichnungen über alle Meldungen hast.

[3] Disposiciones de carácter general aplicables a las instituciones de crédito, Artikel 316 Bis, 316 Bis 1, 316 Bis 10 a 17: Belege, Verschlüsselung, Zugriff, Vorfälle, Störfälle, Protokolle und Überprüfungen. Offizielle Online-Quelle

[4] Peru. SBS 2286-2024: Änderung von Artikel 20.3 zu bestimmten nicht anerkannten Transaktionen und zur Haftung, sofern keine Verantwortung der nutzenden Person nachgewiesen wird. Offizielle Online-Quelle

[5] Spanien. Real Decreto-ley 19/2018, Artikel 45, 66 und 67: Rückerstattung bei nicht autorisierten Transaktionen, Risikomanagement und unverzügliche Meldung schwerer Vorfälle. Offizielle Online-Quelle



Abbildung 3. Zur Wiederherstellung des Zugriffs gehört auch die Überprüfung der Umgebung. Ein neues Passwort beseitigt weder Sitzungen noch Regeln des Angreifers. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

Kapitel 6. Beweissicherung und Unterstützung anderer Personen

6.1 Mindestumfang des Beweispakets

Das Paket enthält die Chronologie, Nachrichten, gegebenenfalls EML-Dateien, URLs, Konten, Belege, Referenzen, Meldungen und beobachtete Änderungen. Es enthält keine Passwörter, Codes, privaten Schlüssel oder unnötigen personenbezogenen Daten. Dateien werden unverändert aufbewahrt; Arbeitskopien werden getrennt davon abgelegt. Die Person braucht keine riesige Sammlung, sondern Gegenstände, die mit ihrer Schilderung in Verbindung gebracht werden können.

Die Chronologie enthält den Eingang der Nachricht, die Handlungen der Person, den Zeitpunkt der Zahlung und des Anrufs sowie Änderungen und Meldungen. Uhrzeiten werden mit Zeitzone notiert; angegebene und überprüfte Zeiten werden unterschieden. Wenn sich die Person nicht genau erinnert, wird die Uhrzeit als ungefähr gekennzeichnet und keine scheinbare Genauigkeit erfunden.

6.2 Älteren oder wenig erfahrenen Personen helfen

Bitte um Erlaubnis, bevor du das Telefon einer Person überprüfst, und erkläre jeden Schritt. Nimm nicht ihre Karte an dich und frage nicht nach ihren Passwörtern. Wenn sie Zugangsdaten ändern muss, soll sie diese unbeobachtet eingeben, während du erklärst, welche Anzeige zu sehen ist. Übe eine einfache Regel: keine Codes weitergeben, keinen Fernsupport installieren und vor jeder Zahlung anrufen. Geduld verhindert, dass der Druck der Betrüger durch Druck der helfenden Person ersetzt wird.

Wenn die Person bereits Geld gesendet hat, schimpfe nicht mit ihr. Hilf ihr, die Bank zu kontaktieren und Referenzen zusammenzustellen. Betrug nutzt Vertrauen, Angst und Zeitdruck aus, nicht mangelnde Intelligenz. Ein zweiter Betrug verspricht häufig die Rückholung: Warne davor, dass niemand ohne institutionelle Überprüfung eine weitere Gebühr für die angebliche Freigabe von Guthaben verlangen sollte.

6.3 Lokale Kontaktstellen, die du tatsächlich nutzen kannst

Anstatt ungeprüfte Telefonnummern aus dem Internet zu kopieren, lege ein Verzeichnis mit den dir bereits bekannten Kanälen an: die offizielle Nummer deiner Bank auf Karte oder Vertrag, Mobilfunkanbieter, Plattform, örtliche Polizei oder Staatsanwaltschaft, Verbraucherschutz, örtlicher Notruf, ein Angehöriger und eine Vertrauensperson. Überprüfe die Angaben vor einer Krise und bewahre sie auf Papier sowie an einem leicht zugänglichen Ort auf.

Bedarf	Zu überprüfender Kanal	Nicht verwenden
Banktransaktion	Nummer auf der Karte, im Vertrag oder in der offiziellen App.	Die von der angeblichen Bank gesendete Telefonnummer.
Konto oder Beitrag	Hilfebereich innerhalb der Plattform.	Link aus einem unbekannten Kommentar.
SIM-Karte oder Rufnummer	Anbieter über App, Vertrag oder offizielle Filiale.	Von Dritten gesendeter Code.
Körperlicher Notfall	Notrufnummer deines Ortes.	Auf eine Antwort in sozialen Netzwerken warten.
Anzeige	Staatsanwaltschaft oder offizieller Kanal deiner Gerichtsbarkeit.	Eine Veröffentlichung als einzige Anzeige.
Emotionale Unterstützung	Vertrauensperson oder örtlicher Dienst.	Kontakte, die die intimen Inhalte sehen wollen.

Abschluss

Die beste Vorbereitung ist eine gemeinsam vereinbarte Pause und ein überprüftes Kontaktverzeichnis. Du musst nicht selbst ermitteln, um den nächsten Verlust zu verhindern.

Anhang A. Notfallkarten

A.1 WhatsApp-Konto kompromittiert

Kurze Abfolge

1. Gib keinen weiteren Code weiter und öffne keine neuen Links.
2. Stelle das Konto von einem sicheren Gerät aus über das offizielle Verfahren wieder her.
3. Überprüfe E-Mail-Konto, Wiederherstellungsoptionen, verknüpfte Geräte und Sitzungen.
4. Ändere Passwörter und entferne unbekannte Zugriffe.
5. Überprüfe Regeln, Filter, Sicherungskopien und autorisierte Apps.
6. Benachrichtige deine Kontakte über einen anderen Kanal.
7. Bewahre Nachrichten, Änderungen und Vorgangsnummern der Meldungen auf.
8. Achte auf neue Versuche; kontaktiere nicht den Angreifer.

A.2 Zahlung oder Überweisung bereits erfolgt

Kurze Abfolge

1. Sende kein weiteres Geld und zahle keine Gebühren für eine angebliche Rückholung.
2. Rufe die Bank unter der Nummer auf deiner Karte, in deinem Vertrag oder in der offiziellen App an.
3. Gib Referenz, Datum, Betrag und Empfänger an und schildere den Vorfall ohne erfundene Angaben.
4. Bewahre Belege, Nachrichten, URLs und Kontoinformationen auf.
5. Frage nach Sperrung, Überprüfung und Dokumenten zum Fall.
6. Bewahre Vorgangsnummer und Antwort auf.
7. Melde den Vorfall der Plattform und der örtlichen Behörde.
8. Befolge keine Anweisungen des angeblichen Empfängers.

A.3 Erpressung oder intime Inhalte

Sichere Abfolge

```
1. Zahle nicht und sende keine weiteren Inhalte.
2. Leite das Material nicht weiter und lade es nicht hoch, um Hilfe zu erhalten.
3. Bewahre Konto, Nachrichten, URL, Datumsangaben und die wichtigsten Referenzen auf.
4. Suche eine Vertrauensperson und die örtliche Fachstelle auf.
5. Bei Gefahr oder betroffenen Minderjährigen haben Notruf und Meldung an eine Fachstelle Vorrang.
6. Stelle Konten und Sitzungen von einem sicheren Gerät aus wieder her.
7. Melde Veröffentlichungen über offizielle Kanäle.
8. Ermittle und verhandle nicht auf eigene Faust.
```

A.4 Verdächtige Nachricht von einem Angehörigen oder einer Bank

Überprüfung vor dem Handeln

```
1. Unterbrich die Handlung, auch wenn sie dringend erscheint.
2. Gib weder Codes noch Passwörter oder Fernzugriff weiter.
3. Rufe die dir bereits bekannte Nummer an, nicht die aus der Nachricht.
4. Überprüfe Anliegen und Identität über einen anderen Weg.
5. Zahle erst nach der Überprüfung.
6. Bewahre Nachricht, URL, Konto und Datum auf.
7. Warne deine Kontakte, wenn das echte Konto kompromittiert wurde.
```

Anhang B. Chronologie, Kontaktverzeichnis und Abschlusskontrolle

B.1 Minimale Chronologie

Datum / Zeitzone	Ereignis und Quelle	Durchgeführte Handlung	Vorgangsnummer / Beweismaterial
[Ungefähr oder genau]	Nachricht erhalten und Gegenstand aufbewahrt.	Keine weitere Interaktion.	[ID]
[ ]	Code, Installation, Zahlung oder Änderung.	Was tatsächlich geschehen ist.	[Beleg]
[ ]	Kontakt mit Bank / Plattform.	Sperrung, Überprüfung oder Meldung.	[Vorgangsnummer]
[ ]	Wiederherstellung des Kontos.	Passwort, Sitzungen, Filter und Apps.	[Aufzeichnung]
[ ]	Benachrichtigung der Kontakte.	Verhinderung weiterer Opfer.	[Kanal]
[ ]	Spätere Überprüfung.	Persistenz oder neuer Versuch.	[Offen]

B.2 Persönliches Kontaktverzeichnis zur Vorbereitung auf eine Krise

Dienst	Überprüfter offizieller Kanal	Alternative
Hauptbank	[Nummer auf der Karte, im Vertrag oder in der App]	[Filiale oder offizielle App]
Mobilfunkanbieter	[App, Vertrag oder Filiale]	[Wiederherstellungskanal]
Hauptplattform	[Interner Hilfebereich]	[Bekannte offizielle E-Mail-Adresse]
Örtliche Behörde	[Offizielle Website oder Telefonnummer]	[Staatsanwaltschaft oder zuständige Behörde]
Örtlicher Notruf	[Offizielle Nummer deines Standorts]	[Medizinischer Dienst oder Sicherheitsdienst]

Dienst	Überprüfter offizieller Kanal	Alternative
Unterstützende Person	[Name und bekannte Telefonnummer]	[Zweite Kontaktperson]

B.3 Rechtsrahmen und Überprüfung

Elektronische Transaktionen werden nach den Regeln des jeweiligen Landes und Sektors zu Datennachrichten, Aufzeichnungen und nicht anerkannten Transaktionen beurteilt. In Mexiko sind CCom 89–94 und 1205 sowie die anwendbaren CNBV-Bestimmungen zu prüfen; für Peru gelten SBS-Regeln, für Argentinien BCRA-Regeln und für Spanien RD-ley 19/2018. Kolumbien und Ecuador verlangen die Aufbewahrung von Nachrichten mit ihrem Kontext; Chile unterscheidet die Wirkungen der Signaturarten. Die Vorlage eines Belegs führt nicht zu einer allgemein gültigen Rückerstattungspflicht.[6][7][8][9][10][11][12][13]

Abschlusskontrolle	Erwartetes Ergebnis
Wurde der Schaden gestoppt?	Keine weiteren Zahlungen, Codes, Installationen oder Verbreitungen.
Wurden die erforderlichen Stellen benachrichtigt?	Bank, Plattform, Anbieter, Behörde und Kontakte, je nach Fall.
Wurde Beweismaterial gesichert?	Nachrichten, URLs, EML-Dateien, Belege, Änderungen und Chronologie.
Wurde die Kontrolle wiederhergestellt?	Gerät, E-Mail-Konto, Passwörter, Sitzungen, Filter und Apps.
Wurde die Person geschützt?	Ohne zusätzliche Offenlegung, Schuldzuweisung oder zweiten Betrug.
Was folgt?	Vorgangsnummer, offene Schritte, Warnmeldungen und spätere Überprüfung.

Abschluss

Rasches Handeln bedeutet nicht blindes Handeln. Eine Pause, ein offizieller Kanal und eine sorgfältige Chronologie können verhindern, dass aus dem ersten Betrug mehrere Schäden entstehen.

[6] Código de Comercio de México, Artikel 89–94 und 1205: Neutralität, Zurechnung, Schriftform, Original, Integrität, Zugänglichkeit und Zulassung von Datennachrichten. Offizielle Textfassung. Offizielle Online-Quelle

[7] Disposiciones de carácter general aplicables a las instituciones de crédito, Artikel 316 Bis, 316 Bis 1, 316 Bis 10 a 17: Belege, Verschlüsselung, Zugriff, Vorfälle, Störfälle, Protokolle und Überprüfungen. Offizielle Online-Quelle

[8] Peru. SBS 2286-2024: Änderung von Artikel 20.3 zu bestimmten nicht anerkannten Transaktionen und zur Haftung, sofern keine Verantwortung der nutzenden Person nachgewiesen wird. Offizielle Online-Quelle

[9] Argentinien. BCRA Comunicación A 7783: Aufzeichnungen digitaler Transaktionen, die mindestens 90 Tage verfügbar sein müssen, und Überwachung von Sicherheitsereignissen. Offizielle Online-Quelle

[10] Spanien. Real Decreto-ley 19/2018, Artikel 45, 66 und 67: Rückerstattung bei nicht autorisierten Transaktionen, Risikomanagement und unverzügliche Meldung schwerer Vorfälle. Offizielle Online-Quelle

[11] Kolumbien. Ley 527 de 1999, Artikel 5–13, 16–25 und 28: Datennachrichten, Schriftform, Original, Integrität, Zulässigkeit, Aufbewahrung, Versand, Empfang und digitale Signatur. Offizielle Online-Quelle

[12] Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, Artikel 2, 6–8, 10–16: Gleichwertigkeit, Schriftform, Original, Aufbewahrung, Herkunft, Versand, Empfang und elektronische Signatur. Offizielle Online-Quelle

[13] Chile. Ley 19.799 über elektronische Dokumente und elektronische Signatur, Artikel 1–5: Gleichwertigkeit, Schriftform, einfache/fortgeschrittene Signatur, Datum und Beweiswert. Offizielle Online-Quelle