ACCCF / Applied knowledge library

11

VOLUME

Contain, warn, preserve and recover

Spanish edition · 2026

A Citizen's Guide to Responding to Digital Fraud: Phishing, Extortion, and Compromised Accounts

WhatsApp, banking, fake pages, loans, investments, extortion and support for others

Help readers act quickly without giving fraudsters more information or destroying the evidence needed to report incidents, recover accounts, and prevent further victimization.

For citizens, families, schools, small businesses, support teams, and people assisting someone affected. Emergency, banking, and reporting channels must be verified locally; a phone number received in a message is not a substitute.

Editorial coordinator: Jocsan Laguna · American Council on Cybersecurity and Forensic Computing

General technical guide and open educational material. It does not constitute legal advice, an expert opinion, or instructions for accessing systems without authorization. Examples and data are fictitious; figures are editorial reconstructions.

Content

The visible page numbering corresponds to the PDF edition. Word can update this table of contents when the document is opened; headings retain internal navigation.

Presentation: Haste Is Part of the Deception ... 3
Chapter 1. The First Minutes ... 3
- **1.1 Stop the Next Action** ... 3
- **1.2 Preserve the Essentials Without Further Exposure** ... 3
- **1.3 Notify the Right People** ... 4

Chapter 2. WhatsApp and compromised accounts ... 4
- **2.1 Recovery from a Trusted Environment** ... 4
- **2.2 Review of applications and remote access** ... 5
- **2.3 Authentication and Recovery as a System** ... 5

Chapter 3 Signs of Deception ... 6
- **3.1 Behaviour before appearance** ... 6
- **3.2 Frequent scenarios** ... 6
- **3.3 When the message comes from a real account** ... 6

Chapter 4. Extortion and intimate content ... 7
- **4.1 Do Not Negotiate or Disseminate** ... 7
- **4.2 Reduce subsequent exposure** ... 7
- **4.3 Provide Support Without Revictimizing** ... 8

Chapter 5. Recovery of accounts ... 8
- **5.1 Recovery order** ... 8
- **5.2 Banking and operations** ... 8
- **5.3 Reporting and monitoring** ... 8

Chapter 6. Preservation and support for others ... 9
- **6.1 Minimum package of evidence** ... 9
- **6.2 How to help an older or less experienced person** ... 10
- **6.3 Local directory that you can use** ... 10

Appendix A. Emergency Cards ... 10
- **A.1 Compromised WhatsApp Account** ... 10
- **A.2 Payment or transfer made** ... 11
- **A.3 Extortion or intimate content** ... 11
- **A.4 Suspicious Message from a Family Member or Bank** ... 11

Appendix B. Timeline, Directory, and Final Check ... 11
- **B.1 Minimum timeline** ... 11
- **B.2 Personal directory to complete before a crisis** ... 12
- **B.3 Legal framework and review** ... 12

Presentation: Haste Is Part of the Deception

Fraud often demands a small, irreversible action before you have time to think: sharing a code, installing an app, paying a fee, opening a link, or confirming data. The appearance may be convincing, and the message may come from a known account that has been compromised. The first line of defense is a deliberate pause: do not pay, share codes, or install remote access software, and verify through a channel you already knew.

This manual does not ask you to investigate the scammer or play along. Instead, it helps you stop the loss, notify others through official channels, preserve what is necessary, and recover your environment. You do not need to prove everything before calling the bank or reporting an account. Waiting until you have a perfect case file can increase the damage. Preserve evidence without putting anyone else at risk.

If there is a physical threat, a risk to minors, or an emergency, prioritize safety and your local emergency services. If the content is intimate, do not forward it to seek help or upload it to analysis services. You can preserve the message, account, URL, and date without distributing the file. Supporting someone does not include unnecessarily intruding on their privacy.

> **Emergency rule**
> Do not use the number, link, or QR code included with the offer or threat. Open the official app, call the number on your card or contract, or type the institution's known address yourself.

Chapter 1. The First Minutes

1.1 Stop the Next Action

If you have not yet paid or provided data, do not continue just to check whether it was genuine. Close the link, end the call, and do not respond. If you have already shared a code, password, or remote access, change course: use another secure device to sign in to your accounts, contact the institution, and review active sessions. Do not follow a second instruction from the supposed support agent to ‘undo’ the first.

If you have already paid, contact the bank or payment provider immediately through an official channel and ask about options for reporting, blocking, or reviewing the transaction. Do not promise that the money will be recovered: the outcome depends on the channel, timing, applicable rules, and circumstances. Preserve the reference, date, amount, receiving account, receipt, and communications; do not withhold information out of embarrassment.

1.2 Preserve the Essentials Without Further Exposure

Item	What to Keep	What to Avoid
Message	Full text, sender, date, time zone, and context.	Editing it or replying to obtain more evidence.
Link	Full URL and page without additional interaction.	Opening it on your primary device.
Account	Username, profile, identifier, and platform.	Relying solely on the name or photograph.
Payment	Receipt, reference, amount, recipient, and channel.	Sending it to a supposed recovery agent.
Email	EML with headers and attachments.	Saving only a screenshot of the body.

Item	What to Keep	What to Avoid
Actions	What you installed, codes provided, changes made, and times.	Concealing steps that could explain the access.

The screenshot must include the sender, date, and enough content to provide context, not just the alarming phrase. If the message arrived by email, export an EML file with headers and attachments. If there is a link, record it without visiting it again. If an application was installed, record its name, source, permissions, and date before uninstalling it when required for security; do not keep a sample on a personal phone for analysis.

1.3 Notify the Right People

If your account was compromised, notify your contacts through another channel: a call, recovery email, or message from a verified account. Ask them not to send money or codes to the affected number. A brief warning can prevent further victimization. Do not forward the fraudulent link as a warning: describe the message and share only the necessary information.

> **Suggested Message for Contacts**
> "I have lost control of this account. Do not send money, codes, or documents to this number or open its links. I am verifying the recovery process through official channels. If you received a request, call me at the number you already knew."

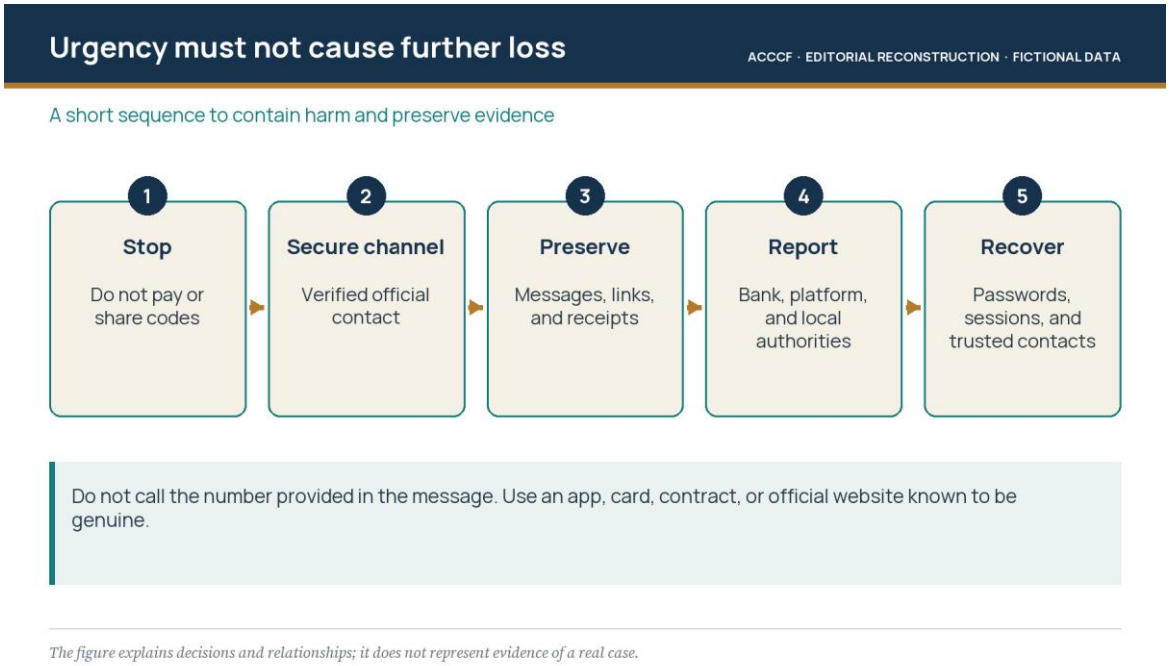


Figure 1. Urgency must not cause another loss. A brief sequence for containing the damage and preserving evidence. Editorial reconstruction; not actual evidence.

Chapter 2. WhatsApp and compromised accounts

2.1 Recovery from a Trusted Environment

Use a device that has not been altered, update the system, and sign in through the official recovery mechanisms. First secure the email account used to recover other accounts, and review its forwarding rules, filters, delegates, and recovery methods. Then use a secure password manager to change passwords, and sign out of sessions and linked devices. A new password does not remove a persistent session or a filter created by an attacker.

Check the registered number, email address, PIN, linked devices, sessions, backups, and recovery contacts. If the carrier changed your SIM or the service stopped working, contact the carrier through its official channels and ask about its protection procedure. Never share with a stranger the code the platform has just sent you to recover your own account.

2.2 Review of applications and remote access

If you installed an unknown support application, record its name and permissions and disconnect the device from networks as needed for security. Seek reliable technical assistance to check for persistence, profiles, and privileged applications. Simply closing the remote access program window is not enough. Uninstalling may be necessary, but first preserve the package information and observed changes if doing so does not increase the risk.

If the attacker saw your screen, files, or codes, consider the related credentials compromised and change them from another device. Do not ask the same 'support' agent to uninstall their tool or review your accounts. Do not run cleaners recommended by the fraudulent contact: they may be a second stage of the deception.

2.3 Authentication and Recovery as a System

NIST SP 800-63B-4 addresses authentication, assurance levels, and phishing-resistant authentication. In practice, a key or second factor can remain vulnerable if the user discloses it or if an attacker controls account recovery. Check that codes arrive through the expected channel and prefer phishing-resistant methods when the service offers them. Do not disable protections to make access easier for a supposed technician.[1]

Review	Safe action	Error avoided
Primary email	New password, sessions signed out, and filters and forwarding rules reviewed.	Recovering other accounts using the compromised email account.
Devices	Sign out of linked devices and remove unrecognized access.	Changing only the password.
Recovering	Verify the phone number, email address, security questions, and contacts.	Leaving a channel controlled by the attacker.
Applications	Review the source, permissions, and profiles.	Trusting the name of a support app.
Contacts	Notify others through another channel and share a warning.	Allowing the fraud to victimize others.

Fictitious case

A person shares a WhatsApp code with a supposed agent. From another phone, they recover the account, review linked devices, and change the recovery email address. They then discover a rule that was forwarding messages to another address. If they had only changed the password, the rule would have continued exposing information.

[1] NIST SP 800-63B-4 (July 2025). Guidelines on authentication and authenticator management, including assurance levels and phishing-resistant authentication. Account recovery is part of the risk and must not be reduced to passwords. Official online source

Chapter 3 Signs of Deception

3.1 Behaviour before appearance

A logo, photograph, similar-looking domain, and polished writing do not establish identity. Check what the message requests: secrecy, urgency, installation, a transfer, a change of channel, or a threat. A real family member may be experiencing an emergency, but you can still call them at their known number. A bank may request an action, but you should not validate it using the number shown in the text.

A link can show one address and open another. Do not use visible text to decide; avoid opening it and enter from the app or type in the known official domain. A domain with HTTPS only indicates an encrypted connection, not that the site belongs to the institution or that it is honest. The certificate does not evaluate the intent of the page.

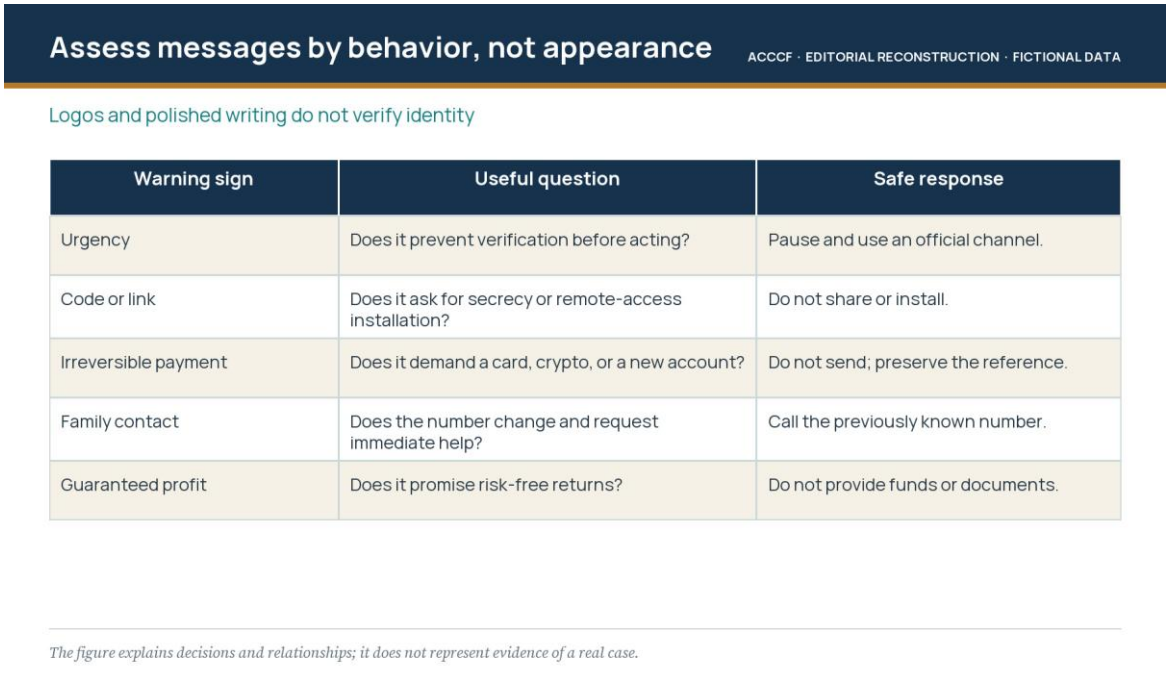
3.2 Frequent scenarios

Scenario	Risk Indicator	Immediate response
Family member with a new number	Requests money or data urgently and avoids calls.	Call the previous number or another family member.
Bank or support	Request a code, password or remote access.	Hang up and make contact through an official channel.
Prize or inheritance	Demands a fee or documents to release it.	Do not pay or send identification.
Investment	Guarantees returns and pressures you to increase the deposit.	Do not contribute more; preserve evidence and report.
Loan	Requests contacts, permissions, and upfront payments.	Do not install it or authorize access to your contacts.
Parcel delivery	Demands a small fee via a link to release a shipment.	Check the tracking number through an official channel.
Employment	Requests a deposit, equipment, or tasks with advance payment.	Verify the company through independently obtained contact details.
Recovery of money	Promises recovery in exchange for another fee.	Do not pay a second time; report through an official channel.

3.3 When the message comes from a real account

A known account may be compromised. Trust should be based not on recognizing the photo, but on verifying the request through another channel. Ask something the person can answer during a call and, above all, do not make the transfer until you have spoken with them. A voice note or video can also be reused or synthesized; channel verification remains necessary.

> **Useful household rule**
> Agreeing on a family verification phrase for money requests can help, but it does not replace a call to a known number. If the request avoids all verification, the safe response is to stop.



Assess messages by behavior, not appearance

ACCCF · EDITORIAL RECONSTRUCTION · FICTIONAL DATA

Logos and polished writing do not verify identity

Warning sign	Useful question	Safe response
Urgency	Does it prevent verification before acting?	Pause and use an official channel.
Code or link	Does it ask for secrecy or remote-access installation?	Do not share or install.
Irreversible payment	Does it demand a card, crypto, or a new account?	Do not send; preserve the reference.
Family contact	Does the number change and request immediate help?	Call the previously known number.
Guaranteed profit	Does it promise risk-free returns?	Do not provide funds or documents.

The figure explains decisions and relationships; it does not represent evidence of a real case.

Figure 2. Assess the message by its behavior, not its appearance. Logos and polished writing do not verify an identity. Editorial reconstruction; not actual evidence.

Chapter 4. Extortion and intimate content

4.1 Do Not Negotiate or Disseminate

If someone threatens to distribute intimate content or private information, do not pay or continue sending material. Payment guarantees neither deletion nor an end to the extortion. Preserve the username, messages, URL, date, receiving account, and any references without downloading or sharing the intimate content with anyone else. Seek support from trusted people and specialized channels or local authorities.

If minors are involved or there is immediate danger, prioritize protection and specialized reporting. Do not store or redistribute material that may be illegal. Describe the item without copying it and request instructions from the appropriate channel. Help must not be conditional on the person providing images or recounting details you do not need in order to act.

4.2 Reduce subsequent exposure

Review privacy settings, contact lists, photos, links, recovery options, and connected accounts. Change passwords from a secure device and sign out of sessions. Notify contacts without describing the material. If the extortionist makes contact from another account, preserve the relationship between the profiles and avoid blocking before preservation if doing so does not increase the risk.

In Mexico, articles 199 Octies and 199 Nonies of the Federal Penal Code cover certain conduct involving intimate sexual content without consent, even when the material does not depict the identified person. Offenses and procedures differ in other countries; consult local law without assuming that every type of conduct has the same name or legal effect.[2]

[2]Mexico. Federal Penal Code, articles 199 Octies and 199 Nonies, compilation including the amendment of 13-03-2026: certain conduct involving intimate sexual content without consent, even if the material does not depict the identified person. Official online source

4.3 Provide Support Without Revictimizing

Do not ask why the person sent the material or ask them to show it to you. Offer concrete help: be present, record the minimum, call the appropriate channel, review accounts, and avoid further contact. Guilt can make the person comply with more of the aggressor's demands. Listening without judgment can prevent the extortion from continuing through isolation.

> **Support Criterion**
> Protect the person before the case file. If a preservation action could increase distribution or danger, consult the specialized channel first and record only what is necessary.

Chapter 5. Recovery of accounts

5.1 Recovery order

First secure the device and primary email account, then address authentication and recovery methods, followed by sessions, applications, banking, and contacts. Replace reused passwords with unique values using a reliable password manager. Do not write new passwords in an openly accessible notebook or send them to the same compromised email account. If a service offers passkeys or phishing-resistant methods, evaluate their use together with secure account recovery.

Review email rules, filters, delegation, automatic replies, authorized applications, third-party access, and administrator profiles. An attacker can retain access through a filter or application even after you change the password. Preserve screenshots of the configuration before making changes when doing so does not increase the risk.

5.2 Banking and operations

Contact the bank with the relevant references and describe what happened without inventing details. Ask about blocking, review, alerts, and required documents. If there is an unrecognized transaction, request the receipt and available channel records. Accepted authentication does not by itself prove authorization: factor changes, enrollment, and alerts can be decisive.

In Mexico, credit institutions have specific rules under their regulatory regime for receipts, incident reports, logs, and the handling of unrecognized transactions. Conditions and deadlines differ in other countries. Reporting alone does not guarantee that the bank will provide restitution, but timely notification may be relevant. Keep the reference number, date, channel name, and response.[3][4][5]

5.3 Reporting and monitoring

Record	Useful content	Why It Matters
Bank	Reference number, date, transaction, channel, and response.	Follow-up and verification of the notification.
Platform	Report, URL, account and reply.	Connection to the content and future copies.

[3] General provisions applicable to credit institutions, articles 316 Bis, 316 Bis 1, 316 Bis 10 to 17: receipts, encryption, access, incidents, case reports, logs, and reviews. Official online source

[4] Peru. SBS 2286-2024: amendment to article 20.3 on certain unrecognized transactions and liability, except where user liability is established. Official online source

[5] Spain. Royal Decree-Law 19/2018, articles 45, 66, and 67: restitution for unauthorized transactions, risk management, and immediate notification of serious incidents. Official online source

Record	Useful content	Why It Matters
Local authority	Channel, case file, documents, and date.	Replacing it with a social media post.
Operator	SIM, changes, protection, and reference number.	Control over account recovery through the phone line.
Contacts	Notification, channel, and date.	Prevent further victimization.
Review	Changes and subsequent alerts.	Detect persistence or a second attempt.

Completing Recovery

Do not consider the process complete merely because you can open your account again. It is complete when recovery options, sessions, filters, devices, and contacts have been reviewed and you have records of the reports.

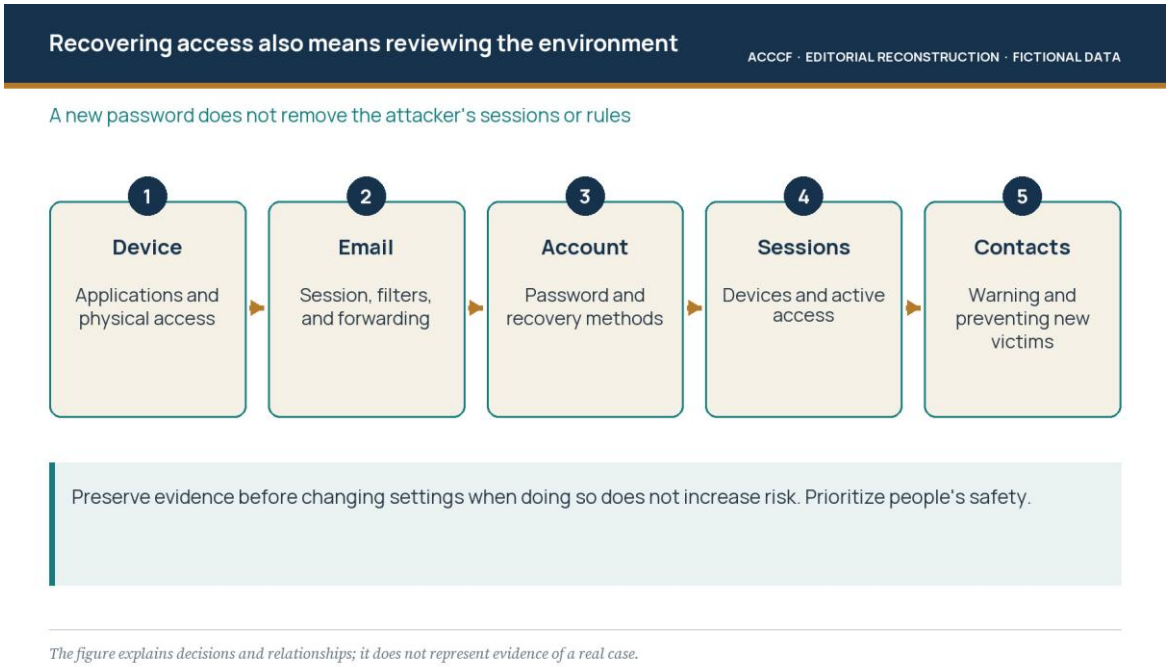


Figure 3. Regaining access also means reviewing the environment. A new password does not remove the attacker's sessions or rules. Editorial reconstruction; not actual evidence.

Chapter 6. Preservation and support for others

6.1 Minimum package of evidence

The package contains a timeline, messages, EML files if available, URLs, accounts, receipts, references, reports, and observed changes. It does not include passwords, codes, private keys, or unnecessary personal data. Keep files unedited and separate working copies. The person does not need a huge collection: they need items that can be connected to their account of events.

The timeline includes when the message arrived, what the person did, when they paid, when they called, what they changed, and what they reported. Record times with their time zones and distinguish reported times from verified times. If the person does not remember a time, mark it as approximate; do not invent precision.

6.2 How to help an older or less experienced person

Ask permission before checking the person's phone and explain every action. Do not take their card or ask for passwords. If they need to change passwords, have them enter the new values privately while you explain what is on the screen. Practice a simple rule: do not share codes, do not install remote support software, and call before paying. Patience prevents the pressure of fraud from being replaced by pressure from the helper.

If the person has already sent money, do not scold them. Help them contact the bank and gather references. Fraud exploits trust, fear, and haste, not a lack of intelligence. A second scam often promises recovery: warn that no one should charge another fee to supposedly release funds without institutional verification.

6.3 Local directory that you can use

Instead of copying unverified numbers from the internet, prepare a directory of channels you already know: your bank's official number from your card or contract, carrier, platform, local police or prosecutor's office, consumer protection agency, local emergency service, family contact, and support person. Verify the details before a crisis and keep them on paper and in an accessible place.

Need	Channel to Verify	Do Not Use
Bank Transaction	Number shown on the card or contract, or in the official app.	Phone number supplied by the supposed bank.
Account or publication	Account or post	Link in a comment from an unknown source.
SIM or line	Carrier through its official app, contract, or branch.	Code sent by a third party.
Physical emergency	Your local emergency number.	Waiting for a response on social media.
Report	Prosecutor's office or official channel in your jurisdiction.	A social media post as the only report.
Emotional support	Trusted person or local service.	Contacts asking to see intimate content.

Conclusion

The best preparation is an agreed pause and a verified directory. You do not need to become an investigator to prevent the next loss.

Appendix A. Emergency Cards

A.1 Compromised WhatsApp Account

Short sequence

```
1. Do not share another code or click any new links.
2. From a secure device, recover the account through the official mechanism.
3. Review email, recovery options, linked devices, and sessions.
4. Change passwords and close unrecognized access.
5. Review rules, filters, backups and authorized apps.
6. Notify contacts via another channel.
7. Preserve messages, changes, and report reference numbers.
8. Watch for new attempts; do not contact the attacker.
```

A.2 Payment or transfer made

Short sequence

1. Do not send more money or recovery fees.
2. Call the bank using the number on your card or contract, or in the official app.
3. Provide the reference, date, amount, recipient, and what happened without inventing details.
4. Preserve receipts, messages, URLs, and accounts.
5. Ask about blocking, review, and documents for the case.
6. Keep the reference number and response.
7. Report to the platform and local authorities.
8. Do not follow instructions from the alleged recipient.

A.3 Extortion or intimate content

Safe Sequence

1. Do not pay or send any more content.
2. Do not forward or upload the material to ask for help.
3. Preserve account details, messages, URLs, dates, and the minimum necessary references.
4. Seek a trusted person and the local specialized channel.
5. If there is danger or minors are involved, prioritize emergency services and specialized reporting.
6. Recover accounts and sessions from a secure device.
7. Report posts through official channels.
8. Do not investigate or negotiate on your own.

A.4 Suspicious Message from a Family Member or Bank

Verification before taking action

1. Stop the action, even if it seems urgent.
2. Do not share codes, passwords or remote access.
3. Call the number you already knew, not the one in the message.
4. Verify the request and the person's identity through another channel.
5. Do not pay until you have verified it.
6. Save message, URL, account and date.
7. Warn your contacts if the real account was compromised.

Appendix B. Timeline, Directory, and Final Check

B.1 Minimum timeline

Date / time zone	Event and source	Action carried out	Reference number / evidence
[Approximate or exact]	Message received and item preserved.	No further interaction.	[ID]
[ ]	Code, installation, payment, or change.	What really happened.	[Receipt]
[ ]	Contact with bank/platform.	Blocking, reviewing or reporting.	[Reference number]
[ ]	Account recovery.	Password, sessions, filters and apps.	[Record]
[ ]	Notification to contacts.	Prevention of further victimization.	[Channel]
[ ]	Follow-up review.	Persistence or a new attempt.	[Pending]

B.2 Personal directory to complete before a crisis

Service	Verified official channel	Alternative
Main bank	[Number on card, contract, or app]	[Official branch or app]
Mobile operator	[App, contract or branch]	[Recovery channel]
Main platform	[Internal help center]	[Known official email address]
Local authority	[Official website or telephone]	[Prosecutor's office or agency]
Local emergency	[Official number for your location]	[Medical or security service]
Support person	[Known name and phone number]	[Second contact]

B.3 Legal framework and review

Electronic transactions are analyzed under the data-message, recordkeeping, and unrecognized-transaction rules of the relevant country and sector. In Mexico, review CCom 89–94 and 1205 and the applicable CNBV provisions; Peru has SBS rules; Argentina, BCRA; Spain, RD-ley 19/2018. Colombia and Ecuador require preservation of messages with context; Chile distinguishes the effects of signatures. Presenting a receipt does not create a universal right to restitution.[6][7][8][9][10][11][12][13]

Final Check	Expected response
Has the damage stopped?	No more payments, codes, installations, or distribution.
Were notifications sent?	Bank, platform, carrier, authorities, and contacts, as applicable.
Was evidence preserved?	Messages, URLs, EML files, receipts, changes, and timeline.
Was access recovered?	Device, email, passwords, sessions, filters and apps.
Did you protect the person?	Without exposure, blame, or a second scam.
What's next?	Reference number, pending actions, alerts, and follow-up review.

Conclusion

Acting quickly does not require acting blindly. A pause, an official channel, and a good timeline can prevent the first deception from leading to several more.

[6] Mexico's Commercial Code, articles 89–94 and 1205: neutrality, attribution, written form, originals, integrity, accessibility, and admission of data messages. Official compilation. Official online source

[7] General provisions applicable to credit institutions, articles 316 Bis, 316 Bis 1, 316 Bis 10 to 17: receipts, encryption, access, incidents, case reports, logs, and reviews. Official online source

[8] Peru. SBS 2286-2024: amendment to article 20.3 on certain unrecognized transactions and liability, except where user liability is established. Official online source

[9] Argentina. BCRA Communication A 7783: digital transaction records available for at least 90 days and monitoring of security events. Official online source

[10] Spain. Royal Decree-Law 19/2018, articles 45, 66, and 67: restitution for unauthorized transactions, risk management, and immediate notification of serious incidents. Official online source

[11] Colombia. Law 527 of 1999, articles 5–13, 16–25, and 28: data messages, written form, originals, integrity, admissibility, preservation, sending, receipt, and digital signatures. Official online source

[12] Ecuador. Law on Electronic Commerce, Electronic Signatures, and Data Messages, Law 67, articles 2, 6–8, 10–16: equivalence, written form, originals, preservation, origin, sending, receipt, and electronic signatures. Official online source

[13] Chile. Law 19.799 on electronic documents and electronic signatures, articles 1–5: equivalence, written form, simple/advanced signatures, date, and evidentiary value. Official online source