ACCCF / 应用知识图书馆

11

卷

控制、通知、保全与恢复

西班牙语版 · 2026

公众数字欺诈应对手册：网络钓鱼、勒索与账户遭入侵

WhatsApp、银行、虚假网页、贷款、投资、勒索及为他人提供支持

帮助尽早行动，不再向欺诈者提供信息，也不破坏举报、恢复账户和防止出现新受害者所需的证据。

面向公众、家庭、学校、小型企业、支持团队以及陪伴受影响者的人员。紧急求助、银行和举报渠道应在当地核实；不得以消息中收到的电话号码替代这些渠道。

编辑统筹：Jocsan Laguna · 美洲网络安全与计算机取证委员会

通用技术指南与开放教育材料。不构成法律意见、专家鉴定意见，也不提供未经授权访问系统的指导。示例和数据均为虚构；图示为编辑重构。

目录

所示页码对应 PDF 版。Word 可在打开文档时更新本目录；标题保留内部导航。

前言：仓促正是骗局的一部分 3

第1章 最初几分钟 3

- **1.1 停止下一步操作** 3
- **1.2 在避免继续暴露的同时保存关键证据** 3
- **1.3 通知适当人员** 4

第2章 WhatsApp 与遭入侵账户 5

- **2.1 从可信环境恢复** 5
- **2.2 检查应用程序与远程访问** 5
- **2.3 将身份验证与恢复作为整体系统处理** 5

第3章 欺诈迹象 6

- **3.1 先看行为，而非表象** 6
- **3.2 常见情景** 6
- **3.3 当消息来自真实账户时** 7

第4章 勒索与私密内容 7

- **4.1 不谈判，不传播** 7
- **4.2 降低后续暴露风险** 8
- **4.3 陪伴而不造成二次伤害** 8

第5章 账户恢复 8

- **5.1 恢复顺序** 8
- **5.2 银行与交易** 9
- **5.3 报告与跟进** 9

第6章 证据保存与为他人提供支持 10

- **6.1 最低限度证据材料包** 10
- **6.2 如何帮助年长者或经验不足者** 10
- **6.3 可实际使用的当地通讯录** 11

附录A 应急卡片 11

- **A.1 WhatsApp 账户遭入侵** 11
- **A.2 已付款或转账** 11
- **A.3 勒索或私密内容** 12
- **A.4 来自亲友或银行的可疑消息** 12

附录B 时间线、通讯录与最终检查 12

- **B.1 最简时间线** 12
- **B.2 危机发生前填写的个人通讯录** 13
- **B.3 法律框架与复核** 13

前言：仓促正是骗局的一部分

欺诈通常在你来得及思考之前，要求你完成一个看似微小却不可逆的操作：分享验证码、安装应用、支付佣金、打开链接或确认数据。其外观可能很有说服力，消息也可能来自某个已知但已遭入侵的账户。第一道防线是明确暂停操作：不付款、不分享验证码、不安装远程访问软件，并通过你原先就知晓的渠道核实。

本手册不要求你调查诈骗者，也不要求你与其周旋。它建议你制止损失、通过官方渠道发出通知、保存必要材料并恢复环境。致电银行或举报账户之前，你无需证明一切。等到案卷完美无缺再行动，可能会扩大损害。保存证据时，不应让其他人面临风险。

如存在人身威胁、未成年人面临危险或紧急情况，应优先保障人身安全，并联系当地紧急服务机构。如果内容涉及隐私，不要为了求助而转发，也不要上传到分析服务。你可以保存消息、账户、URL 和日期，而无须传播相关文件。为一个人提供支持，并不意味着可以毫无必要地查看其私密内容。

> **应急规则**
> 不要使用随优惠信息或威胁消息发来的电话号码、链接或 QR 码。请打开官方应用，拨打银行卡或合同上的电话号码，或自行输入你已知的机构网址。

第1章 最初几分钟

1.1 停止下一步操作

如果你尚未付款或提供数据，不要为了核实真伪而继续操作。关闭链接，挂断电话，不要回复。如果你已经分享验证码、密码或远程访问权限，应立即改变做法：使用另一台安全设备登录账户，联系相关机构并检查登录会话。不要执行所谓支持人员为“撤销”第一步操作而发出的第二项指令。

如果你已经付款，请立即通过官方渠道联系银行或支付服务提供商，询问举报、冻结或审查交易的选项。不要承诺资金一定能够追回：结果取决于渠道、时间、规定和具体情况。保存参考号、日期、金额、收款账户、付款凭证和通信记录，不要因羞愧而隐瞒信息。

1.2 在避免继续暴露的同时保存关键证据

对象	应保存的内容	应避免的做法
消息	完整文本、发件人、日期、时区和上下文。	为获取更多证据而编辑或回复消息。

对象	应保存的内容	应避免的做法
链接	完整 URL 和页面，不做进一步交互。	在你的主要设备上打开链接。
账户	用户名、个人资料、标识符和平台。	只相信名称或照片。
付款	付款凭证、参考号、金额、收款方和渠道。	将其发送给所谓的追款人员。
电子邮件	含邮件头和附件的 EML。	仅保存正文截图。
操作记录	安装内容、提供过的验证码、变更和时间。	隐瞒可能解释访问过程的操作步骤。

截图必须包含发件人、日期和足够的内容，而不能只有令人警觉的那句话。如果消息通过电子邮件收到，应导出含邮件头和附件的 EML。如有链接，只记录，不再访问。如已安装应用，在出于安全需要而卸载之前，先记录名称、来源、权限和日期；不要在个人手机上保留样本以供分析。

1.3 通知适当人员

如果你的账户遭入侵，请通过其他渠道通知联系人：拨打电话、使用恢复邮箱，或从已确认安全的账户发送消息。请他们不要向受影响的号码汇款或发送验证码。简短的通知可以阻止出现新的受害者。不要为了示警而转发欺诈链接：描述消息内容，只分享必要的信息。

> **可向联系人发送的实用消息**
>
> “我已失去对此账户的控制。不要向这个号码汇款、发送验证码或文件，也不要打开它发出的链接。我正在通过官方渠道核实恢复事宜。如果你收到请求，请拨打你原先就知道的号码联系我。”



图1. 紧急处置不应造成另一笔损失。控制损害并保存证据的简要流程。编辑重构；不构成真实证据。

第2章 WhatsApp 与遭入侵账户

2.1 从可信环境恢复

使用未被篡改的设备，更新系统，并通过官方恢复机制登录。先更改可用于恢复其他账户的邮箱密码，并检查其转发规则、过滤器、委托人和恢复方式。随后使用可靠的密码管理器更改密码，并注销会话和解除已关联设备。新密码不会清除持续有效的会话，也不会删除攻击者创建的过滤器。

检查注册号码、邮箱、PIN、已关联设备、登录会话、备份和恢复联系人。如果运营商更换了你的 SIM 卡或服务停止运作，请通过官方渠道联系运营商，询问保护程序。不要把平台刚刚发给你、用于恢复自己账户的验证码分享给陌生人。

2.2 检查应用程序与远程访问

如果你安装了陌生的支持类应用，请记录其名称和权限，并根据安全需要断开设备网络。寻求可信的技术帮助，检查持久化机制、配置文件和具有特权的应用。仅关闭远程访问程序窗口并不足够。可能有必要卸载，但如果不增加风险，应先保存软件包信息和观察到的变更。

如果攻击者看到过屏幕、文件或验证码，应视相关凭据已遭泄露，并从另一台设备更改。不要让同一个所谓“支持人员”卸载其工具或检查你的账户。不要运行欺诈联系人推荐的清理工具：这可能是骗局的第二阶段。

2.3 将身份验证与恢复作为整体系统处理

NIST SP 800-63B-4 涉及身份验证、保证级别和抗网络钓鱼身份验证。在实践中，如果用户交出密钥或第二因素，或者攻击者控制了恢复流程，它们仍可能存在脆弱性。检查验证码是否送达预期渠道；服务提供抗网络钓鱼方法时，应优先采用。不要为了方便所谓技术人员访问而关闭保护措施。[1]

检查项	安全操作	避免的错误
主邮箱	设置新密码、注销会话，并检查过滤器和转发规则。	使用已遭入侵的邮箱恢复其他账户。
设备	注销已关联设备，并删除无法识别的访问权限。	只更改密码。
恢复方式	核实电话、邮箱、安全问题和联系人。	留下由攻击者控制的渠道。

[1]NIST SP 800-63B-4（2025年7月）。身份验证与验证器管理指南，包括保证级别和抗网络钓鱼身份验证。账户恢复是风险的一部分，不应将其简化为密码问题。 官方在线来源

检查项	安全操作	避免的错误
应用程序	检查来源、权限和配置文件。	仅凭支持类应用的名称就相信它。
联系人	通过另一渠道通知，并分享警示。	让欺诈继续危害他人。

虚构案例

某人向所谓的客服人员分享了 WhatsApp 验证码。他从另一部手机恢复账户，检查已关联设备，并更改恢复邮箱。随后发现一条将消息转发到另一地址的规则。如果只更改密码，该规则仍会继续泄露信息。

第3章 欺诈迹象

3.1 先看行为，而非表象

标志、照片、相似域名和流畅的措辞都不能证明身份。应检查消息提出了什么要求：保密、紧急处理、安装软件、转账、更换渠道或威胁。真正的亲友也可能遇到紧急情况，但你可以拨打已知号码联系本人。银行也可能要求你采取某项操作，但你不应通过短信中显示的号码核实。

链接显示的地址可能与实际打开的地址不同。不要依据可见文字作判断；避免打开链接，应从应用进入，或手动输入已知的官方域名。域名使用 HTTPS 仅表示连接经过加密，并不表示该网站属于相关机构，也不表示网站诚实可信。证书不会评估网页的意图。

3.2 常见情景

情景	风险迹象	立即应对
使用新号码的亲友	紧急索要钱财或数据，并回避通话。	拨打原号码或联系其他亲友。
银行或客服	索要验证码、密码或远程访问权限。	挂断电话，通过官方渠道联系。
中奖或遗产	要求支付佣金或提交文件才能领取。	不付款，也不发送身份证件。
投资	承诺回报，并施压要求增加存款。	不再投入资金；保存证据并举报。
贷款	要求获取通讯录、权限和预付款。	不安装，也不授权访问通讯录。
快递包裹	通过链接收取小额费用以放行包裹。	通过官方渠道查询运单号。
招聘	要求支付押金、设备费，或完成需要预付款的任务。	通过独立联系方式核实企业。
追回资金	承诺再收一笔佣金即可追回资金。	不再次付款；向官方渠道举报。

3.3 当消息来自真实账户时

熟悉的账户也可能遭入侵。信任不能建立在认出照片上，而应通过其他途径核实请求。可以询问对方能在电话中回答的问题；最重要的是，在与本人通话之前不要转账。语音留言或视频也可能被重复使用或合成，因此仍有必要核实渠道。

> **实用的家庭规则**
>
> 家人之间约定一句用于核实汇款请求的暗语可能有帮助，但不能替代拨打已知号码。如果请求方回避一切核实，安全的应对方式就是停止操作。

应根据行为而非外观评估消息

ACCCF · 编辑重建 · 虚构数据

标志和规范措辞不能验证身份

迹象	有用的问题	安全应对
紧迫	是否阻止你在行动前核实?	暂停并通过官方渠道。
代码或链接	是否要求提供秘密信息或安装远程访问工具?	不共享，也不安装。
不可逆付款	是否要求银行卡、加密货币或新账户?	不转账；保留参考信息。
亲友联系	是否更换号码并要求立即帮助?	拨打已知的原号码。
收益保证	是否承诺无风险回报?	不提供资金或文件。

本图说明决策与关系；不代表真实案例的证据。

图2. 应根据行为而非表象评估消息。标志和流畅措辞不能验证身份。编辑重构；不构成真实证据。

第4章 勒索与私密内容

4.1 不谈判，不传播

如果有人威胁传播私密内容或私人信息，不要付款，也不要继续发送材料。付款不能保证内容会被删除，也不能保证勒索结束。保存用户名、消息、URL、日期、收款账户和任何参考信息，不要将私密内容下载或分享给更多人。寻求可信人员的支持，并联系专业渠道或当地主管机构。

如涉及未成年人或迫在眉睫的危险，应优先保护人员安全，并通过专业渠道举报。不要存储或重新分发可能违法的材料。描述相关对象但不要复制，并向主管渠道询问处理指引。提供帮助不应以当事人交出图片或讲述你采取行动并不需要知道的细节为条件。

4.2 降低后续暴露风险

检查隐私设置、联系人列表、照片、链接、恢复方式和已连接账户。从安全设备更改密码并注销会话。通知联系人时不要描述相关材料。如果勒索者从另一账户联系你，应保存不同个人资料之间的关联；如果这样做不会增加风险，在保存证据前不要屏蔽对方。

在墨西哥，《联邦刑法典》第199 Octies条和第199 Nonies条涵盖某些未经同意处理性私密内容的行为，即使材料并不对应被识别的人。在其他国家，罪名和处理途径会有所不同；应查询当地法规，不能假定所有行为都具有相同名称或法律效果。[2]

4.3 陪伴而不造成二次伤害

不要追问当事人为什么发送材料，也不要要求其展示。提供具体帮助：陪伴在旁、只记录必要信息、致电主管渠道、检查账户并避免新的接触。自责可能使当事人接受侵害者更多要求。不带评判地倾听，可以防止勒索因孤立无援而继续。

> **帮助原则**
> 保护当事人比完善案卷更重要。如果某项证据保存操作可能扩大传播或增加危险，应先咨询专业渠道，只记录必要信息。

第5章 账户恢复

5.1 恢复顺序

先保护设备和主邮箱，然后处理身份验证与恢复方式，再检查会话、应用程序、银行业务和联系人。将重复使用的密码改为互不相同的密码，并使用可靠的密码管理器。不要把新密码记在敞开的笔记本上，也不要发送到同一个已遭入侵的邮箱。如果服务提供通行密钥或抗网络钓鱼方法，应在确保安全恢复的前提下评估是否采用。

检查邮件规则、过滤器、委托设置、自动回复、已授权应用、第三方访问和管理配置文件。即使更改密码，攻击者仍可能通过过滤器或应用保持访问。如果不会增加风险，应在修改前保存配置截图。

[2]墨西哥。《联邦刑法典》（Código Penal Federal），第199 Octies条和第199 Nonies条，含13-03-2026改革的汇编版本：某些未经同意处理性私密内容的行为，即使材料并不对应被识别的人。 官方在线来源

5.2 银行与交易

联系银行并提供参考信息，如实描述发生的事情，不要编造细节。询问冻结、审查、警报和所需文件。如果存在无法确认的交易，请索取凭证和可用的渠道记录。已接受的身份验证本身并不能证明获得授权：验证因素变更、注册记录和警报可能具有决定性作用。

在墨西哥，信贷机构在其制度下，对凭证、异常事件、日志和无法确认交易的处理有具体规则。在其他国家，条件和期限会有所不同。银行不会仅因收到报告就保证退款，但及时通知可能很重要。保存受理编号、日期、渠道名称和答复。[3][4][5]

5.3 报告与跟进

记录对象	有用内容	重要性
银行	受理编号、日期、交易、渠道和答复。	便于跟进并核实已发出通知。
平台	举报记录、URL、账户和答复。	关联相关内容及日后出现的副本。
当地主管机构	渠道、案卷、文件和日期。	不要以公开发帖替代正式举报。
运营商	SIM 卡、变更、保护措施和受理编号。	控制通过手机号码进行恢复的渠道。
联系人	通知、渠道和日期。	防止出现新的受害者。
复核	后续变更和警报。	发现持续访问或第二次尝试。

完成恢复

不要仅因屏幕显示又能登录账户就结束处置。只有检查完恢复方式、会话、过滤器、设备和联系人，并保存各项报告的记录后，才能结束恢复工作。

[3]适用于信贷机构的一般性规定，第316 Bis、316 Bis 1、316 Bis 10至17条：凭证、加密、访问、事件、异常事项、日志和审查。 官方在线来源

[4]秘鲁。SBS 2286-2024：修改第20.3条，涉及某些无法确认的交易及责任，但经证明由用户负责的除外。 官方在线来源

[5]西班牙。Real Decreto-ley 19/2018，第45、66和67条：未经授权交易的退款、风险管理和严重事件的立即通报。 官方在线来源



图3. 恢复访问权限还包括检查系统环境。新密码不会清除攻击者建立的会话或规则。编辑重构；不构成真实证据。

第6章 证据保存与为他人提供支持

6.1 最低限度证据材料包

材料包包含时间线、消息、EML（如有）、URL、账户、凭证、参考信息、报告和观察到的变更。不包含密码、验证码、私钥或不必要的个人数据。文件应原样保存，不做编辑，并与工作版本分开。当事人不需要数量庞大的材料，而需要能够与其陈述相互关联的对象。

时间线包括消息何时到达、当事人做了什么、何时付款、何时致电、发生了什么变更以及举报了什么。记录时间时应注明时区，并区分当事人陈述的时间与经核实的时间。如果记不得某一时间，应标明为约略时间，不要虚构精确度。

6.2 如何帮助年长者或经验不足者

查看其手机前应征得许可，并解释每项操作。不要拿走其银行卡，也不要索要密码。如果需要更改密码，让当事人在你解释当前屏幕内容时私下输入。练习一条简单规则：不分享验证码、不安装远程支持软件、付款前先致电核实。保持耐心，避免以帮助者的压力取代欺诈者施加的压力。

如果当事人已经汇款，不要斥责。帮助其联系银行并汇集参考信息。欺诈利用的是信任、恐惧和仓促，而不是智力不足。第二次诈骗通常承诺追回资金：要提醒当事人，未经机构核实，任何人都不应以所谓解冻资金为由再收一笔佣金。

6.3 可实际使用的当地通讯录

不要从不经核实的互联网页面复制电话号码，而应准备一份通讯录，列入你已知的渠道：银行卡或合同上的银行官方号码、运营商、平台、当地警察或检察机关、消费者保护机构、当地紧急服务、亲友联系人和可提供支持的人。在危机发生前核实这些信息，并以纸质形式及在易于取用的位置保存。

需求	应核实的渠道	不要使用
银行交易	银行卡、合同或官方应用上的号码。	所谓银行发来的电话号码。
账户或帖子	平台内的帮助中心。	陌生评论中的链接。
SIM 卡或手机号码	通过官方应用、合同或营业厅联系运营商。	第三方发来的验证码。
人身紧急情况	当地紧急求助号码。	等待社交媒体回复。
举报	检察机关或所属司法辖区的官方渠道。	仅将公开发帖作为举报。
情感支持	可信赖的人或当地服务机构。	要求查看私密内容的联系人。

结语

最好的准备，是事先约定暂停操作的规则并备好经过核实的通讯录。要避免下一笔损失，你无需成为调查人员。

附录A 应急卡片

A.1 WhatsApp 账户遭入侵

简要步骤

1. 不要再分享其他验证码，也不要点击新链接。
2. 从安全设备通过官方机制恢复账户。
3. 检查邮箱、恢复方式、已关联设备和登录会话。
4. 更改密码，并关闭无法识别的访问。
5. 检查规则、过滤器、备份和已授权应用。
6. 通过另一渠道通知联系人。
7. 保存消息、变更记录和举报受理编号。
8. 留意新的尝试；不要联系攻击者。

A.2 已付款或转账

简要步骤

1. 不再汇款，也不支付追款佣金。
2. 拨打银行卡、合同或官方应用上的号码联系银行。
3. 提供参考号、日期、金额、收款方，并如实说明经过，不要编造。
4. 保存凭证、消息、URL 和账户信息。
5. 询问冻结、审查和案件所需文件。

6. 保存受理编号和答复。
7. 向平台和当地主管机构举报。
8. 不要听从所谓收款方的指示。

A.3 勒索或私密内容

安全步骤

1. 不要付款，也不要再发送内容。
2. 不要为了求助而转发或上传相关材料。
3. 保存账户、消息、URL、日期和必要的最低限度参考信息。
4. 寻找可信赖的人，并联系当地专业渠道。
5. 如存在危险或涉及未成年人，优先联系紧急服务并通过专业渠道举报。
6. 从安全设备恢复账户并检查登录会话。
7. 通过官方渠道举报相关帖子。
8. 不要自行调查或谈判。

A.4 来自亲友或银行的可疑消息

行动前先核实

1. 即使看似紧急，也要停止操作。
2. 不要分享验证码、密码或远程访问权限。
3. 拨打你原先就知道的号码，而不是消息中的号码。
4. 通过另一途径核实请求和身份。
5. 核实之前不要付款。
6. 保存消息、URL、账户和日期。
7. 如果真实账户遭入侵，提醒你的联系人。

附录B 时间线、通讯录与最终检查

B.1 最简时间线

日期 / 时区	事件和来源	已采取的操作	受理编号 / 证据
[约略或准确]	收到消息并保存相关对象。	不做进一步交互。	[ID]
[ ]	验证码、安装、付款或变更。	实际发生的情况。	[凭证]
[ ]	联系银行 / 平台。	冻结、审查或举报。	[受理编号]
[ ]	恢复账户。	密码、会话、过滤器和应用。	[记录]
[ ]	通知联系人。	防止出现新的受害者。	[渠道]
[ ]	后续复核。	持续访问或新的尝试。	[待处理]

B.2 危机发生前填写的个人通讯录

服务	经核实的官方渠道	替代方式
主要银行	[银行卡、合同或应用上的号码]	[营业厅或官方应用]
移动运营商	[应用、合同或营业厅]	[恢复渠道]
主要平台	[平台内帮助中心]	[已知的官方邮箱]
当地主管机构	[官方网站或电话]	[检察机关或主管部门]
当地紧急服务	[所在地的官方号码]	[医疗服务或安全部门]
支持人员	[已知姓名和电话号码]	[第二联系人]

B.3 法律框架与复核

电子交易应依据所在国家和行业有关数据电文、记录及无法确认交易的规则分析。在墨西哥，应查阅 CCom 89–94 和1205以及适用的 CNBV 规定；秘鲁有 SBS 规则；阿根廷有 BCRA 规则；西班牙有 RD-ley 19/2018。哥伦比亚和厄瓜多尔要求保存带有上下文的消息；智利区分不同签名的法律效力。出示凭证并不产生普遍适用的退款权利。[6][7][8][9][10][11][12][13]

最终检查	预期结果
损害是否已制止?	不再付款、提供验证码、安装软件或传播内容。
是否已发出通知?	视情况通知银行、平台、运营商、主管机构和联系人。
是否已保存证据?	消息、URL、EML、凭证、变更和时间线。
是否已恢复?	设备、邮箱、密码、会话、过滤器和应用。
是否已保护当事人?	避免暴露、责备和第二次诈骗。
接下来做什么?	受理编号、待办事项、警报和后续复核。

[6]墨西哥《商法典》，第89–94条和第1205条：数据电文的中立性、归属、书面形式、原件、完整性、可访问性和采信。官方汇编版本。 官方在线来源

[7]适用于信贷机构的一般性规定，第316 Bis、316 Bis 1、316 Bis 10至17条：凭证、加密、访问、事件、异常事项、日志和审查。 官方在线来源

[8]秘鲁。SBS 2286-2024：修改第20.3条，涉及某些无法确认的交易及责任，但经证明由用户负责的除外。 官方在线来源

[9]阿根廷。BCRA Comunicación A 7783：数字交易记录至少保存90天，并监测安全事件。 官方在线来源

[10]西班牙。Real Decreto-ley 19/2018，第45、66和67条：未经授权交易的退款、风险管理和严重事件的立即通报。 官方在线来源

[11]哥伦比亚。Ley 527 de 1999，第5–13、16–25和28条：数据电文、书面形式、原件、完整性、可采性、保存、发送、接收和数字签名。 官方在线来源

[12]厄瓜多尔。《电子商务、电子签名和数据电文法》（Ley 67），第2、6–8、10–16条：等效性、书面形式、原件、保存、来源、发送、接收和电子签名。 官方在线来源

[13]智利。Ley 19.799（关于电子文件和电子签名），第1–5条：等效性、书面形式、简单 / 高级签名、日期和证明力。 官方在线来源

结语

尽早行动并不意味着盲目行动。暂停一下、使用官方渠道并维护好时间线，可以防止第一次骗局演变成接连多次骗局。