DIGITAL DEMOCRACY INSTITUTE OF THE AMERICAS

WhatsApp Weaponized: How Scammers Target U.S. Latinos Through Public Groups

Part 2 (of 3): Scams Targeting Migrants

Table of Contents:

1. **Executive Summary** 2
2. **Methodology** 2
3. **Preying on Pathways to Legal Status** 3
4. **Employment and Financial Scams** 5
    a. Job Offers 5
    b. Housing and Healthcare Offers 7
5. **Weaponizing Victimhood** 8
6. **Extracting Insights from Fact-Checks** 10
7. **Final Takeaways and Recommendations** 12

The Digital Democracy Institute of the Americas

www.ddia.org | info@ddia.org

December 2025

1. EXECUTIVE SUMMARY

WhatsApp Weaponized, a series of three investigations, looks at how scammers target U.S. Latinos through public Spanish-language WhatsApp groups. In November 2025, the Digital Democracy Institute of the Americas (DDIA) released the first investigation – a report on commercial and product scams (available here). In this installment, the DDIA team outlines the seemingly predatory ways in which potential scammers push dubious legal services, fake job opportunities, and questionable healthcare options onto Latinos navigating the U.S. immigration system, looking to provide for their families, and working to build a better life.

As this report shows, many scammers are unfortunately tailoring their schemes to exploit Latinos working to acquire legal status, preying on often-complicated immigration processes and pathways for accessing traditional banking, stable housing, health insurance, and full-time employment. By weaponizing everything from Temporary Protected Status (TPS) deadlines and asylum procedures to the documents needed to obtain a driver's license or a small loan, digital scammers are profiting from both hope and fear.

With this three-part series of investigations, DDIA aims to center U.S. Latino experiences in the conversation about what major tech companies must do to better protect users, especially those navigating the digital world in non-English languages and far from their home countries.

2. METHODOLOGY

DDIA researchers examined more than 18,400 unique messages suspected of facilitating scams shared within 3,300 Spanish-speaking public WhatsApp groups between January 1 and September 1, 2025. Hundreds of these pieces of content were so widely circulated on the app that Meta marked them with its "frequently forwarded" double-arrow label, a sign of how rapid and dangerous this type of information can be.

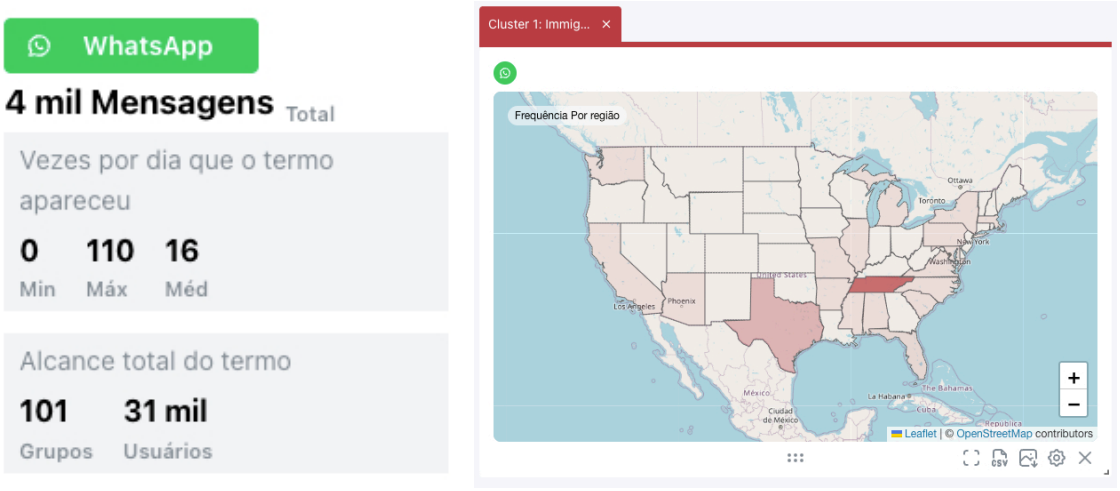
The DDIA team relied on two primary tools and data sources: Palver, a social listening tool that analyzes more than 3,300 public WhatsApp channels in the United States, and the Google Fact Check API, which has been aggregating fact-checks produced by media organizations around the world for years.

Researchers also reviewed and categorized 139 Spanish-language fact-checks published since 2017 that debunk various scams. This dataset from Google Fact Check API provided essential historical context to help DDIA trace how quickly online fraud has expanded in Spanish and how scammers' techniques have adapted and grown more sophisticated over time.

Note: In researching WhatsApp public groups with Palver, DDIA does not have access to people's personal data and does not collect demographic information about WhatsApp users. The tools do not allow DDIA to see full names or phone numbers of users. For more information on Palver, please visit www.palver.com.br.

3. PREYING ON PATHWAYS TO LEGAL STATUS

Between January 1 and September 1, 2025, DDIA identified more than 4,000 unique messages that appeared to promote fraudulent immigration services circulating in Latino public WhatsApp groups, digital spaces with hundreds of users that use Spanish as a primary language and comprise at least 30% U.S.-based phone numbers. According to data extracted from Palver, this content might have potentially reached over 31,000 users in 101 groups, making immigration-related scam attempts one of the most prominent and widespread forms of fraud targeting Latinos during the period DDIA analyzed.

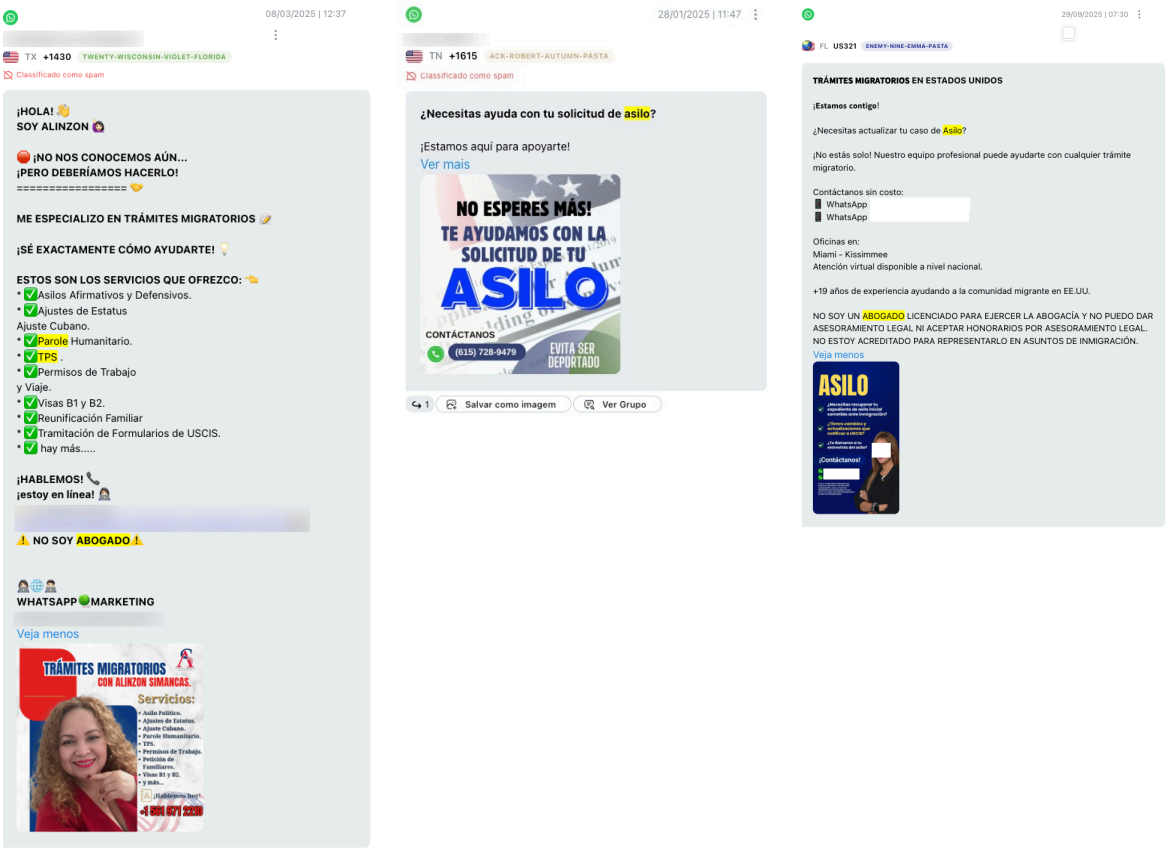


The Scam:

Non-lawyers who make it clear they have no legal credentials usually pose in public WhatsApp groups as "specialists" or "consultants" and offer shortcuts to U.S. residency, work permits, asylum, and even citizenship. Their messages commonly use psychological manipulation tactics (detailed below), and appear to primarily target Venezuelan migrants.

To avoid legal consequences for the unauthorized practice of immigration law, these scammers usually include a bold disclaimer in the messages they share: “No soy abogado” (I am not a lawyer), which at first glance appears to be a calculated trick to feign transparency while still preying on vulnerable individuals.

- **Fear and Hope:** Scammers seem to employ a two-step psychological assault. First, they fuel fear and urgency by spreading alarmist claims about unverified immigration raids (usually in a speed that does not reflect real life law-enforcement capacity) or inventing official-sounding requirements or deadlines. With anxiety at an all-time high, they pivot to offering hope and solutions with an extremely friendly and disarming tone. One of the viral messages in DDIA's dataset reads: "Soy [name here]. ¡No nos conocemos aún... ¡Pero deberíamos hacerlo!" (I'm [name here]. We don't know each other yet... but we should!). The scammer then poses as a legal advisor ready to serve as trusted guide through the complex U.S. immigration system.



- **Republishing and Echoes of Coordination:** The consistency in formatting, phrasing, and contact numbers DDIA found across more than 224 messages (shared in 20 public groups reaching more than 15,000 people) suggests scammers are not acting in isolation nor posting content in good faith. There are signs of coordinated schemes, like the use of the same image and extremely similar messaging across messages and posts.

- **Geographic Reach:** Per the names of the public groups where these potential scams were detected, researchers conclude that criminals are heavily concentrated in digital spaces comprising Latinos based in Atlanta, Miami, New York (Brooklyn, Bronx), Tampa, and New Jersey.

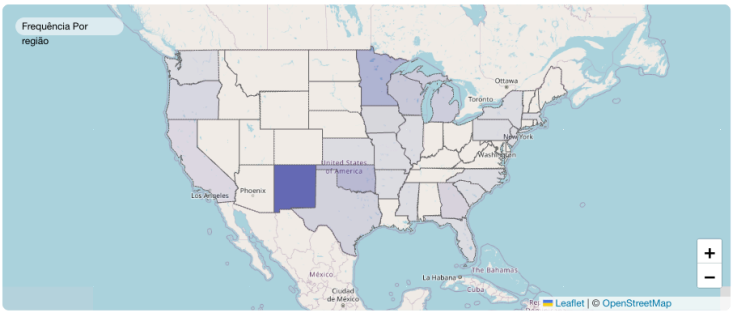
4. EMPLOYMENT AND FINANCIAL SCAMS

In this second category of scams targeting Latino communities in the United States via public WhatsApp groups, criminals appear exploiting the universal need for financial stability.

The Scam:

a. Job Offers

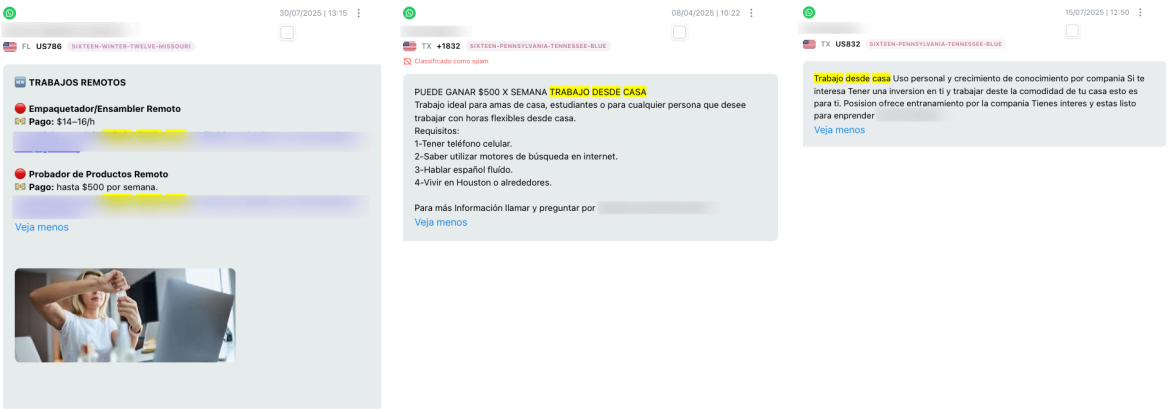
At least 83 unique messages related to potentially false work-related content were detected by DDIA. This content might have reached over 25,000 WhatsApp users in 32 public groups. These messages clearly target Latinos searching for legitimate work but mainly push deceptive employment “opportunities.” A potential Latino victim could be a person looking for a very real position but primarily getting "work from home" job offers, and positions that require little to no experience or little to no paperwork.



At least four distinct (but often overlapping) types of content were spotted in this universe, preying on different vulnerabilities.

- **Fake Remote and Low-Skill Job Offers:** This was the most prevalent type. Here, scammers advertise generic, easy-to-perform remote jobs like "Remote Packer/Assembler" (Empaquetador/Ensambler Remoto) or "Remote Product Tester" (Probador de Productos Remoto). The primary lure is a bit-inflated salary, such as $14-$16/hour for packaging (against $11/hour per national average) or a low weekly salary for testing ($500 versus $ 1,900 in the national average) for a position with no paperwork. These offers exploit the widespread desire for flexible, accessible employment.

- **Recruitment Schemes as Business Opportunities:** Posing as companies in sectors like insurance or energy, these potential scams focus on recruiting new agents rather than selling a product. They promise comprehensive training, flexible hours, and high commissions. A key tactic is the repeated assertion, "¡No necesitas experiencia!" (No experience needed!), which dramatically widens the pool of potential targets to anyone seeking a career change.

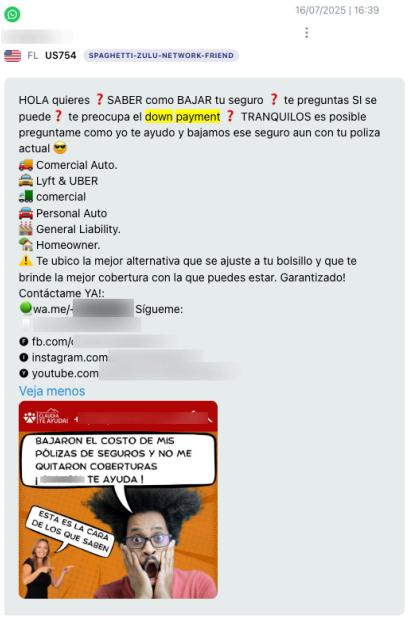


b. Housing and Healthcare Offers

Scammers are also harnessing difficult or bureaucratic U.S. processes for renting a home or contracting health insurance.

- **Rental Fraud:** These potential scams appeared in several groups named after locations in Florida (Davenport, Kissimmee, and Haines City, for example). Messages shared on these digital spaces usually had ads for low-cost rooms available for rent, but demanded an upfront deposit via an instant transfer app like Zelle or Cash App before the person could see the property.

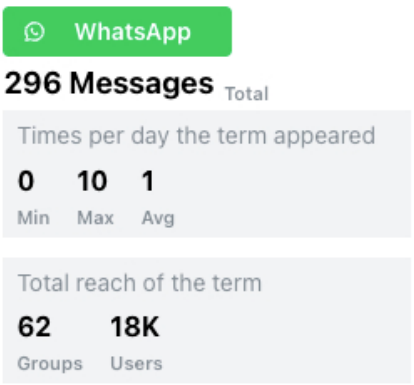
- **Insurance Sales:** Messages containing ads for insurance or credit repair were also spotted by researchers. These pieces of content use fear-based tactics about providing or protecting one's family to create a sense of urgency. A common hook is, "Necesitas seguro... ¿Te preocupa tu familia?" (Need insurance?... Are you worried about your family?) to present unverified (and usually too-good-to-be-true) health insurance plans.

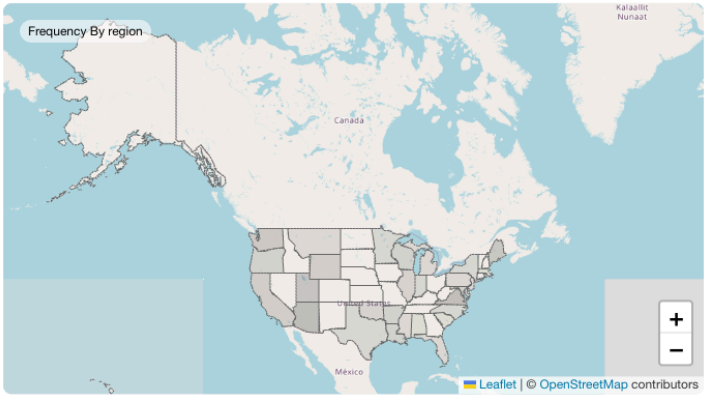


- **Legal Assistance for Accidents:** Finally, messages promoting legal specialists for accident compensation were also seen using the trust trigger. "¡Es confiable, habla tu idioma y está para ayudarte!" (She's trustworthy, speaks your language, and is here to help you!). "Confiable, comprometida y siempre está dispuesta a apoyar" (trustworthy, committed, and always willing to help). Here, the scammers are looking to engage with Latinos who have had car or motorcycle accidents.

5. WEAPONIZING VICTIMHOOD

During this study, DDIA found 296 unique messages circulating on 62 public WhatsApp groups (with more than 18,000 users) that potentially contained stories of victims of scams discussing their cases or raising doubts about “opportunities” they received. Why is this important? Because it might be connected to a second level of scamming: the recovering type (briefly discussed on the first installment of this series).

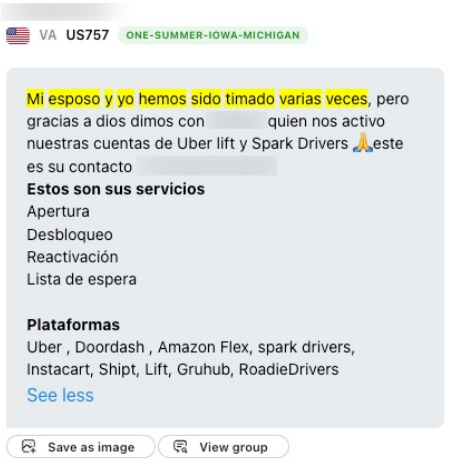




The Scam:

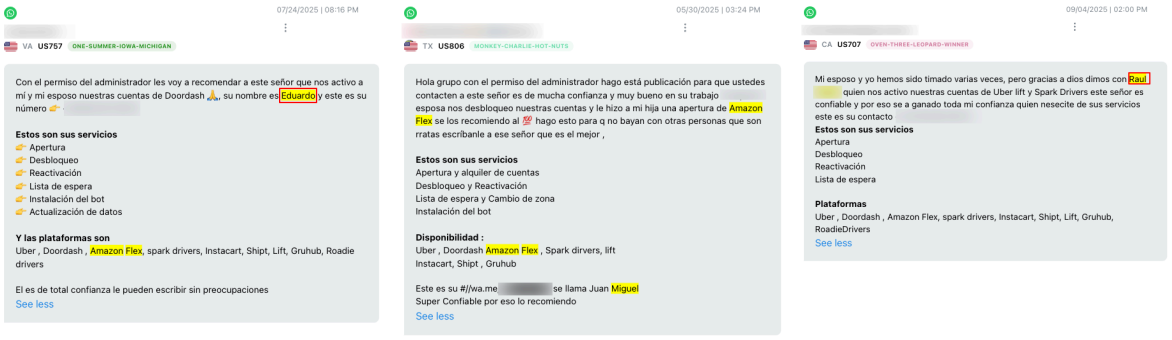
In this universe, scammers create posts that begin with a story of being a victim. A dominant example states: "Mi esposo y yo hemos sido timado varias veces" (My husband and I have been scammed several times), when discussing difficulties to find a good and reliable health insurance in the United States. After building empathy, the scammers pivot to recommending a single "trustworthy" person who has helped them and who might be willing to help other victims of a specific scam in the future. This "victim-turned-advocate" narrative is a powerful tool to disarm natural skepticism.

Common cases detected by DDIA include potential scammers targeting gig-economy Latino workers by promoting “consultants” who could supposedly unblock accounts on platforms like Uber, Doordash, and Amazon Flex.

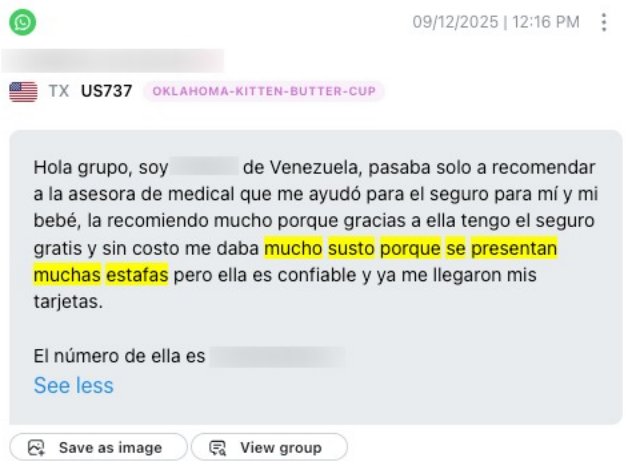


The Manipulation Tactics:

- **The Keyword is "Confiable":** The word "confiable" (trustworthy/reliable) is used relentlessly in this type of messaging to create a false sense of security.



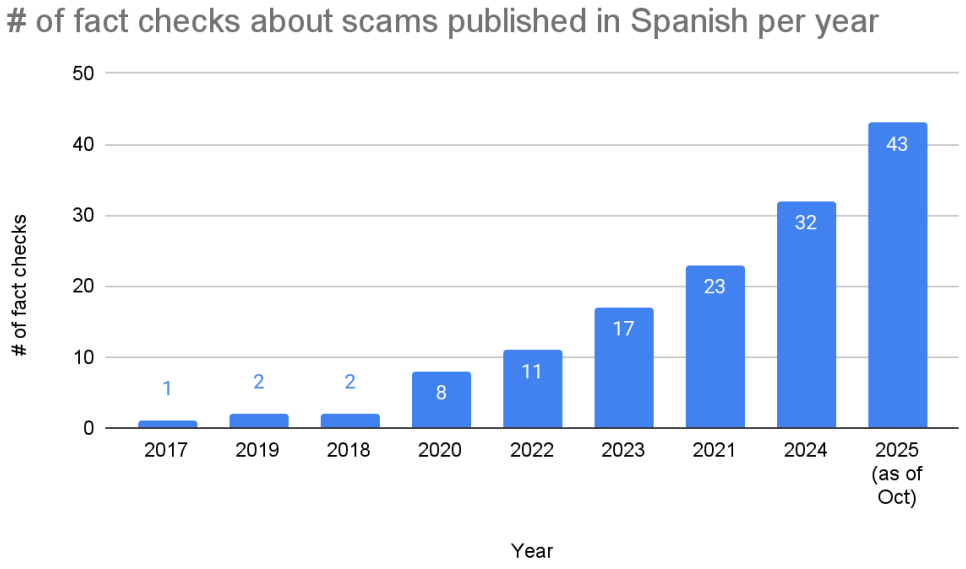
- **Fear of Being Defrauded:** In other cases reviewed by DDIA, a potential scammer highlights high levels of anxiety while seeking a product or a service, stating that they had "mucho susto porque se presentan muchas estafas" (a lot of fear because many scams occur). Later the person communicates they had the support of one great “advisor” and suggest others hire the same person to solve similar needs. "Ella es confiable y ya me llegaron mis tarjetas" (she is trustworthy and my cards have already arrived).



- **Fabricated Proof:** This tactic is again used to create a powerful illusion of success and lure victims. When promoting “great advisors,” scammers commonly post videos recorded by unverified clients repeating a very similar statement. The consistency of the format and the language indicates this might be fabricated content.

6. EXTRACTING INSIGHTS FROM FACT-CHECKS

As mentioned in the first part of this report, launched in November 2025, Spanish-language fact-checkers have been publishing warnings about digital scams targeting U.S. Latinos and Ibero-Americans at an accelerating rate. Between January and October 2025, new debunks appeared at least once per week, at a rate that reflects a growing volume of digital fraud targeting the public.



While in the first installment of this report DDIA reviewed commercial-related fact-checks, in this chapter, researchers dove into the most dominant threat detected by Spanish-language fact-checkers: the impersonation of authority. In these attacks, scammers rely on impersonating trusted entities to create a sense of urgency, fear or authority. Some examples are:

- **Impersonation of Government Agencies:** Scammers spotted by fact-checkers frequently impersonate government bodies to intimidate potential victims. A primary example cited across several fact-checks was Spain's traffic authority, the Dirección General de Tráfico (DGT). Scammers sent mass SMS messages and emails about fake traffic fines ("multas"), demanding immediate payment to avoid further penalties. Other examples, more present in Latin America, include fake notifications from tax agencies and social security offices, often requesting personal data to process a non-existent refund or benefit increase.

- **Impersonation of Financial Institutions:** Banks such as BBVA, Sabadell and ING (in Spain) were primary targets. Scammers send fraudulent alerts via SMS claiming a "suspicious transfer" had been made, an account had been "deactivated" or a "new security system" needed to be activated. The links in these messages led to malicious websites designed to harvest banking credentials.

- Attacks also impersonate utility companies, with fake invoices, and postal services, demanding small payments to "release" a package.

7. FINAL TAKEAWAYS AND RECOMMENDATIONS

Main Takeaways	Details of the Scheme	Key Recommendations
Immigration Fraud	Scammers, often self-identifying as immigration "specialists" or "consultants" (who state "No soy abogado"), offer illegal shortcuts to residency, permits, or citizenship, targeting fear and hope, especially among Venezuelan migrants.	**For WhatsApp Users –** **Question Credentials:** Be extremely wary of anyone who admits “I am not a lawyer”. **Verify Requirements and Deadlines:** Use only the official USCIS website and local immigration civil society organizations. **Avoid Unsolicited "Help":** Legitimate legal providers do not spam informal WhatsApp groups.
Employment and Financial Fraud	Scammers spread deceptive high-paying, low-skill "work from home" job offers, recruitment schemes, and high-yield investment programs.	**Never Pay for a Job:** Legitimate employers do not charge for training or equipment. **Guaranteed High Returns Are Likely a Lie:** Any massive, rapid-return guarantee is likely a scam. **Verify Companies:** Search the company name online with terms like "scam," "estafa," or "fraud."

"Weaponizing Victimhood"	Scammers create a post beginning with a story of being a victim of scams themselves, then pivot to recommending a single "trustworthy" person ("confiable") who supposedly helped them.	**Be Skeptical of the "Victim" Story:** Recognize this as a manipulation tactic. **"Confiable" is a Red Flag:** The repeated use of this word to endorse an unknown person in a group chat should raise some degree of suspicion. **Trust, but Verify:** Never act on a recommendation from an online group without independent verification. Google the names of the people featured, Google the services, verify the offer with at least two or three other sources, and rely on fact-checkers' websites (like Politifact, Factchequeado, or any member of the International Fact-Checking Network).
Other Predatory Offers (Rental/Insurance/Legal)	Rental Fraud: Scammers demand upfront deposits via apps (Zelle/Cash App) before the renter or buyer sees the property. Insurance Sales: Using fear (e.g., "Are you worried about your family?") to push unverified plans.	**Don't Pay a Deposit for Property Sight-Unseen:** Never send money for a rental property before visiting it and signing a formal lease. **Be Aware of Emotions:** Fraud tactics exploit fear, greed, hope, and trust.

Manipulation Tactics (Across All Scam Types)	Scams rely on emotional appeal, false urgency, promises of a better life, fabricated proof (unverified success stories), and the use of technical jargon to create a veneer of legitimacy.	**Ask Questions and Think Twice:** Question unsolicited messages and be wary of any offer that seems too good to be true. **Be Wary of Asks to Continue the Conversation Privately:** A major red flag is when scammers demand their targets move the conversation from WhatsApp to a more private space like Telegram.
Impersonation of Authority/Relatives	Phishing (SMS/Email): Impersonating government agencies, financial institutions, or utility companies. WhatsApp: Impersonating a family member ("Mom, my phone is broken, this is my new number") to request urgent money transfers.	**Develop Skepticism:** Verify before clicking on links and question unsolicited messages. Check URLs, visit Google Fact Check Explorer, reach out to authorities through their regular communication channels.

For further questions, please reach out to: info@ddia.org