DIGITAL DEMOCRACY INSTITUTE OF THE AMERICAS

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

Part 1 (of 3): Commercial and Product Scams

Table of Contents:

The Digital Democracy Institute of the Americas

www.ddia.org | info@ddia.org

November 2025

DIGITAL DEMOCRACY
INSTITUTE OF THE AMERICAS

1. EXECUTIVE SUMMARY

With scams and fraud on the rise, understanding how bad actors target U.S. Latinos on WhatsApp is a top priority for the Digital Democracy Institute of the Americas (DDIA). With Black Friday and the year-end holiday season right around the corner, this report, one of a three-part series to be released in 2025 and 2026, looks at **commercial scams and fraud circulating** within and between 3,300 public Spanish-language WhatsApp groups comprising at least 30% phone numbers based in the United States.

The major trends and threats laid out in this first installment aim to support Spanish-speaking consumers (and the companies, creators and journalists communicating with them) in spotting red flags and rejecting scams before they expose personal data and/or lose money.

The second installment will detail how digital criminals are forging ties with U.S. Latino communities, with a particular focus on immigrants, by exploiting their need for legal resources, work, services, and support, to obtain personal information or financial gain through WhatsApp.

In the third installment of the series, the investigation will turn to the world of dubious investments and cryptocurrency scams – a fast-growing ecosystem where financial promises are exaggerated, risks are hidden, and "too good to be true" rewards are the bait pulling WhatsApp users into harm's way.

Deepening the conversation about scams and fraud, and about what major tech companies must do to better protect users from cybercrime – especially in non-English languages - is urgent. A recent study by the Global Anti-Scam Alliance (GASA) found that 70% of U.S. residents encountered a scam in the past year, with individuals encountering an average of 377 scam attempts annually. As widely reported, these schemes carry staggering financial consequences: in 2025 alone, an estimated $64.8 billion was stolen from U.S. victims.

But above all and connecting to DDIA's work, GASA reports that digital platforms with direct-messaging features, including WhatsApp (widely used among Latinos) have become primary vectors for malicious activity.

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 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. EXPLOITING CONSUMER DESIRE

Scammers – much like disinformers – rely on sophisticated social-engineering tactics designed to exploit predictable human emotions. Fear, hope, trust, and greed are the most common triggers. And when it comes to commercial fraud, the desire to save money, pay less, or "get a great deal" whenever possible are levers most frequently pulled.

In DDIA's analysis, two strategies stood out as the most common methods used to potentially deceive U.S. Latinos online: fake giveaways and surveys, and fraudulent online sales.

a. Fake Giveaways and Surveys

Capitalizing on consumers' appetite for discounts and free products, scammers regularly misuse the names of popular brands such as Shein, Temu, Macy's, AT&T, Apple, Walmart, and Tesla to catch people's attention. WhatsApp users are lured with promises of "mystery boxes," gift cards, or exclusive promotions in exchange for completing a quick game, filling out a form, playing with an app, or participating in a survey.

The goal does not seem to be an immediate financial payoff, but rather data harvesting. After victims surrender personal information, the promised reward never materializes. Instead, their data seemingly becomes fuel for future fraud attempts.

b. Fraudulent Online Sales

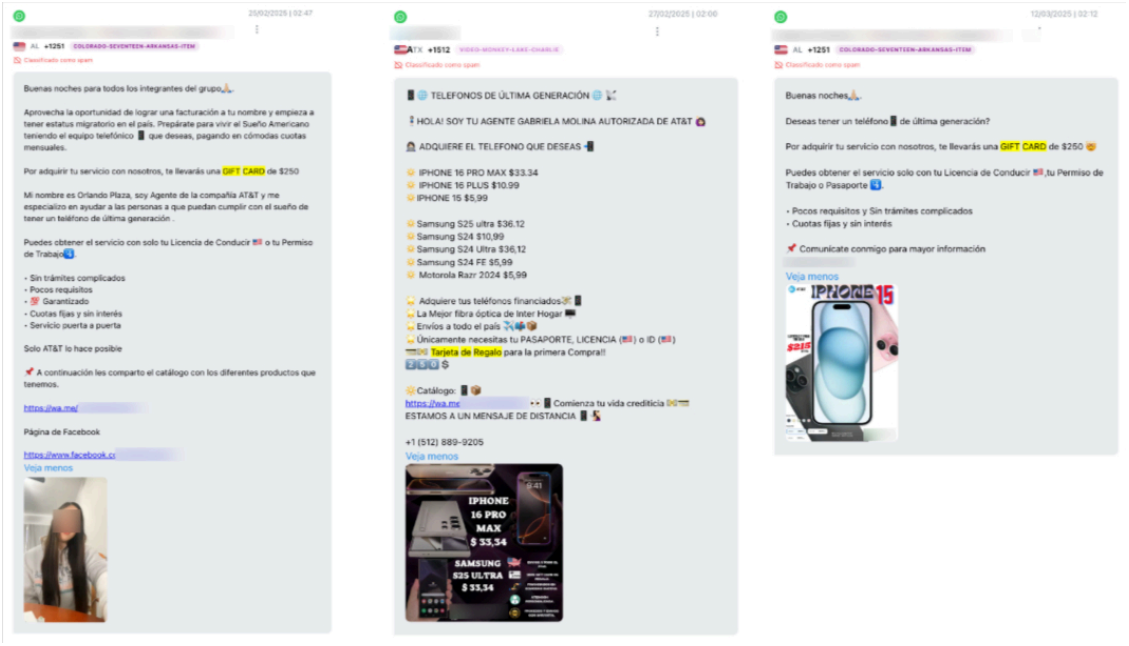
Another widespread scam involves creating fake e-commerce shops on TikTok or Facebook and then promoting those accounts through WhatsApp (or social media ads). Scammers often recycle videos from real businesses to build credibility before "selling" products that will never be shipped.

Here, the damage is twofold: victims lose both personal data and the money paid for nonexistent items.

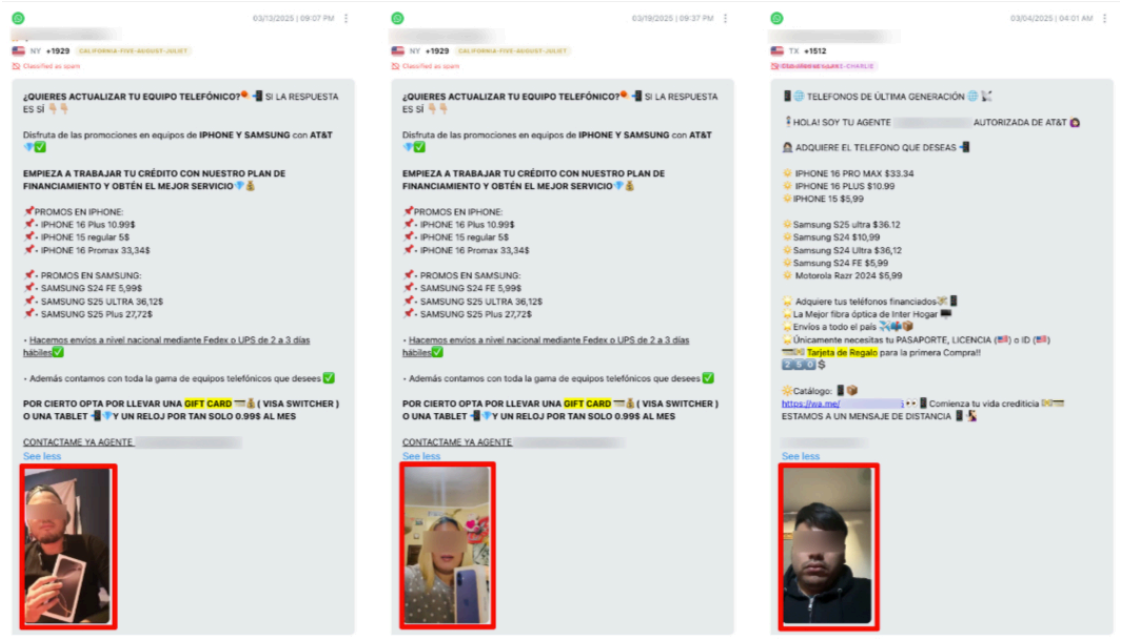
c. Key Red Flags to Watch For

- Cheap Smartphones and Internet Offers: DDIA's analysis identified at least nine individuals (Spanish speakers) aggressively promoting suspicious "next-generation phone" deals, including iPhone 16 Pro Max and Samsung S25 Ultra, as well as ultra-cheap internet plans in the Spanish-speaking public WhatsApp groups DDIA monitored. In one case, researchers observed how potential criminals dangle the possibility of getting their victims a very unlikely $100,000 Apple credit line.
    - The offers reviewed by researchers were crafted to appeal to people who may lack an established U.S. credit history, including newly arrived (documented or undocumented) migrants. Scammers often claim that driver's licenses, work permits, or passports are enough to qualify, bypassing formal financial requirements such as traditional credit score checks.

- Many of the schemes analyzed impersonated major companies like AT&T and Apple, dangling incentives such as a “$250 gift card,” which is considered a classic red flag.



- Finally, to enhance credibility, all nine individuals observed by DDIA circulated potentially fake testimonials: short videos of supposed customers thanking them and showing off newly purchased phones. These seemingly unverified endorsements appeared designed to make the individuals look more reliable, build trust and, consequently, accelerate victim conversion.



4. Fraudulent Payment and Last-Minute Discount Schemes: Scammers are also using Latino public WhatsApp groups to promote schemes where they promise to buy products for their potential targets at steep discounts (often 50% off of the total price). The pitch is simple: the buyer fills an online cart with items they want, shares with the scammer full access to it, and is told they only need to pay the store half the cost of the cart. The other 50% of the payment is to be sent to the scammer (sometimes upfront).

    a. One widely circulated example detected by DDIA reads: “Saca tu carrito de Walmart y pásamelo. Yo lo pago por ti. Solo tienes que pagarme el 50% de su valor." (“Load your Walmart cart and send it to me. I’ll pay for you - you only need to cover 50% of the total.”)

b. But behind these too-good-to-be-true offers are familiar (and well-documented) criminal tactics:

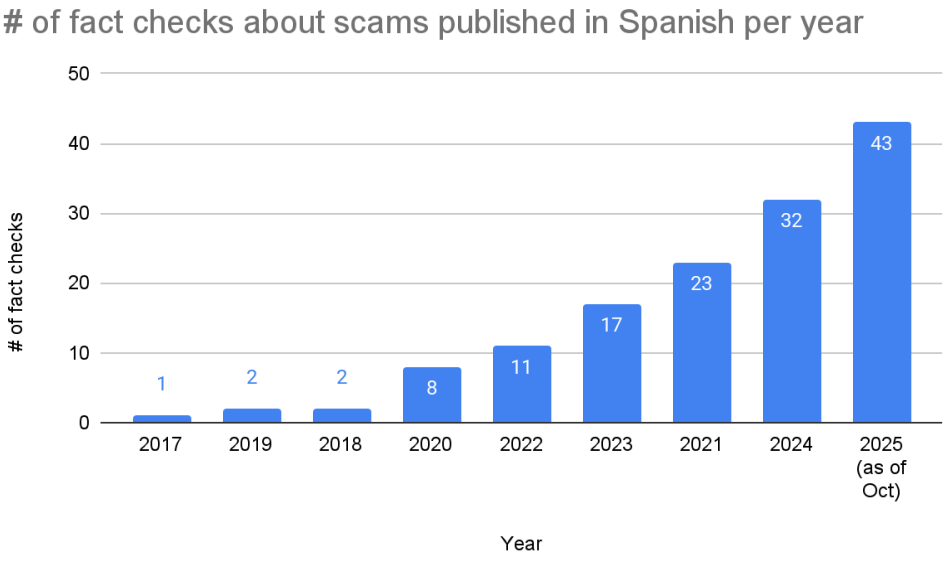
   i. Use of previously stolen or cloned credit cards, which not only leaves the victim without their purchase but may also expose them to legal scrutiny for participating in a fraudulent transaction.

   ii. Theft of victims' own personal data and payment information, collected during the interaction and later exploited for additional unauthorized purchases.

4. EXTRACTING INSIGHTS FROM FACT-CHECKS

The analysis of 139 fact-checks extracted from the Google Fact Check API – all published by Spanish-language professionals since 2017 to warn Spanish-speaking Latinos and Ibero-Americans about scams and digital fraud – confirms not only the rapid growth of the problem addressed in this report but also mirrors what DDIA identified across public WhatsApp channels.

The fact-check trajectory shows a consistent upward curve over eight years, signaling both the acceleration of scam activity and an increasing demand for verification efforts in Spanish.



The surge in 2025 is especially notable: in just the first ten months of the year, 43 scam-related fact-checks were published, averaging four per month, or roughly one every week. This dramatic rise underscores how quickly fraudulent schemes are evolving and highlights the urgent need for stronger consumer protection and digital literacy initiatives tailored to Spanish-speaking communities.

a. Most Common Debunked Commercial Scam Narratives

Commercial scams detected by fact-checkers revolve (just like those seen on WhatsApp public channels) around the promise of something high-value in exchange for very little or nothing. The exploitation of the user's curiosity or desire to save money is clear. The most frequent types of scams are the following:

Type of Scam	Description and Purpose	Examples
Fake giveaways and sweepstakes	The name of recognized brands is used to announce an incredible prize for a special reason (anniversary, holiday) with the aim of stealing data or making the user share the scam.	Fake gift cards (Shein), iPhone 16 (Farmatodo), mini-fridges (Mahou), hiking kits (Decathlon).
Mystery boxes and unclaimed packages	A set of products is advertised at absurdly low prices under the excuse of "surplus stock." Similar claims are made about unverified "lost luggage" or items supposedly discounted due to a "logistical error."	Fake beauty "mystery boxes" (sold under brands like Primor or Temu), unclaimed Temu packages, and/or unverifiable "lost luggage suitcases" are frequently marketed as items that must be sold off because their rightful owners never appeared or cannot be identified.
Fake product sales or scarcity exploitation	Huge discounts are announced on highly desired products. Real-world shortages are exploited to	Low-cost Xiaomi TVs, high-end perfumes, flight offers near holidays, sale of groceries at low prices.

	sell items that are never delivered.	
Fake e-commerce / stores on social media	Creation of websites or social media profiles (especially TikTok) that mimic real stores or sell trending products, charging for items that do not exist.	Fake stores selling Maisons Du Monde products or profiles impersonating toy stories.

b. Social Engineering Tactics Used

The effectiveness of the scams detected by fact-checkers seems to lie in the use of psychological tactics and impersonation techniques: spoofing (brand impersonation), data harvesting (with fake forms and surveys), and the exploitation of holidays and other special occasions that may feel personal or important to the buyers (Christmas, International Women's Day, Valentine's Day, and anniversaries).

The idea of scarcity and urgency is also used, as publications often frame the promised item as "limited stock" or on "last day" sale to push for immediate action.

c. Some of the Most Frequently Impersonated Brands

Scammers impersonate retailers and consumer brands with massive public recognition across multiple sectors, with some retail chains and e-commerce platforms standing out in the Latino-focused analysis:

Brand/Company	Primary Type of Fraudulent Offer
Temu	Unclaimed packages, mystery box, and survey offer.
Mahou (Spain)	Sweepstakes for mini-fridges and coolers (tied to holidays).
Shein	Mystery box/gift card offers and Telegram scams.
Primor	Mystery boxes and highly discounted perfume offers.
HiperDino	Christmas gift bag giveaway via Facebook.
Carrefour	Fake refrigerator giveaway.

Druni (Spain)	Fake €800 gift card survey.
Mercadona (Spain)	Fake €500 gift card.
Nespresso	Fake coffee maker giveaway.

d. The Use of Artificial Intelligence and Other Tactics

The data available is still minimal, but scammers targeting Latinos are seemingly beginning to use AI to create more convincing bait. One example detected by DDIA among the fact-checks produced includes a fabricated but realistic-looking image of a warehouse fire at Temu.

Another predatory trend involves "recovery" scams – fraudulent services that target people who have already lost money to fraud, promising to recover their funds for an upfront fee, thereby victimizing them a second time.

In this sophisticated form of psychological manipulation, scammers create posts that begin with a story of how they once were a victim. After building empathy, the messaging pivots to recommending a single "trustworthy" person who has supposedly been helpful and is potentially willing to help again. This "victim-turned-advocate" narrative is designed to disarm natural skepticism, and common cases detected by DDIA include potential scammers targeting gig-economy Latino workers by promoting “consultants” who could allegedly unblock accounts on platforms like Uber, Doordash, and Amazon Flex. (More on this topic on the second installment of this report. Stay tuned!)

5. Final Takeaways and Recommendations

Category	Main Takeaway	Recommendation
Problem and Urgency	Spanish-language WhatsApp channels are vectors for commercial scams targeting U.S. Latinos. Messages circulate dangerously quickly through frequently forwarded messages.	**Tech Companies** (Meta, in this case) must urgently increase oversight of frequently forwarded messages and strengthen safety interventions against the buying and selling

		of products in public groups, especially for non-English languages. **Policymakers** should fully understand the scope of scams and hold platforms accountable for enforcing safety standards in accordance with existing laws and companies' terms of service. **News outlets and local journalists** must promote awareness of scams and fraud, by investigating and exposing bad and their tactics in English and Spanish-language coverage, and disseminating content in platforms Latinos use often, including YouTube, TikTok, and Instagram.
Scammer Strategy	Scammers exploit predictable human emotions, including greed and the need or desire to save money ("get a great deal"). They use sophisticated (but well-known) social-engineering tactics.	**WhatsApp Users** must be extra vigilant and harness skepticism as a defense against manipulation tactics. Good practices are: verifying websites and profiles through Google before buying, and questioning unsolicited messages on public groups.
Most Common Scams	The two most common strategies are fake giveaways / surveys (aimed at data harvesting) and fraudulent online sales (aimed at data and financial theft).	**WhatsApp Users** must be wary of any offer that seems too good to be true, such as steep discounts, mystery boxes, or very cheap high-end electronics. Google Fact Check Explorer is a good source for what has already been debunked.

Specific Red Flags	Schemes include fake luxury smartphones, internet deals, and too-good-to-be-true discounts (e.g., "50% off your Walmart cart"), and impersonating major brands (e.g., Shein, Temu, Apple, AT&T).	**WhatsApp Users** should be able to spot red flags by being suspicious of claims that bypass formal financial requirements (like credit score checks), request partial payment to a third party, or offer unlikely incentives like a "$100,000 Apple credit line."
Criminal Tactics	Scammers use stolen/cloned credit cards, steal victims' payment info, circulate potentially fake testimonials to build trust, and use psychological tactics like scarcity/urgency ("last day" sale).	**WhatsApp Users** should not share access to online shopping carts or their payment information with unknown individuals offering payment assistance or deep discounts. If an individual poses as a representative, ask for credentials that could be verified (like a business email address, for example).
Digital Literacy	Fact-checks confirm the rapid and consistent acceleration of scam activity, underscoring the need for verification efforts in Spanish-speaking communities.	**Tech Companies** should invest in digital literacy initiatives tailored to Spanish-speaking communities. **Policymakers** must build safety strategies that take into consideration two factors: the need for more data about scams and the understanding that education is a primary defense.

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