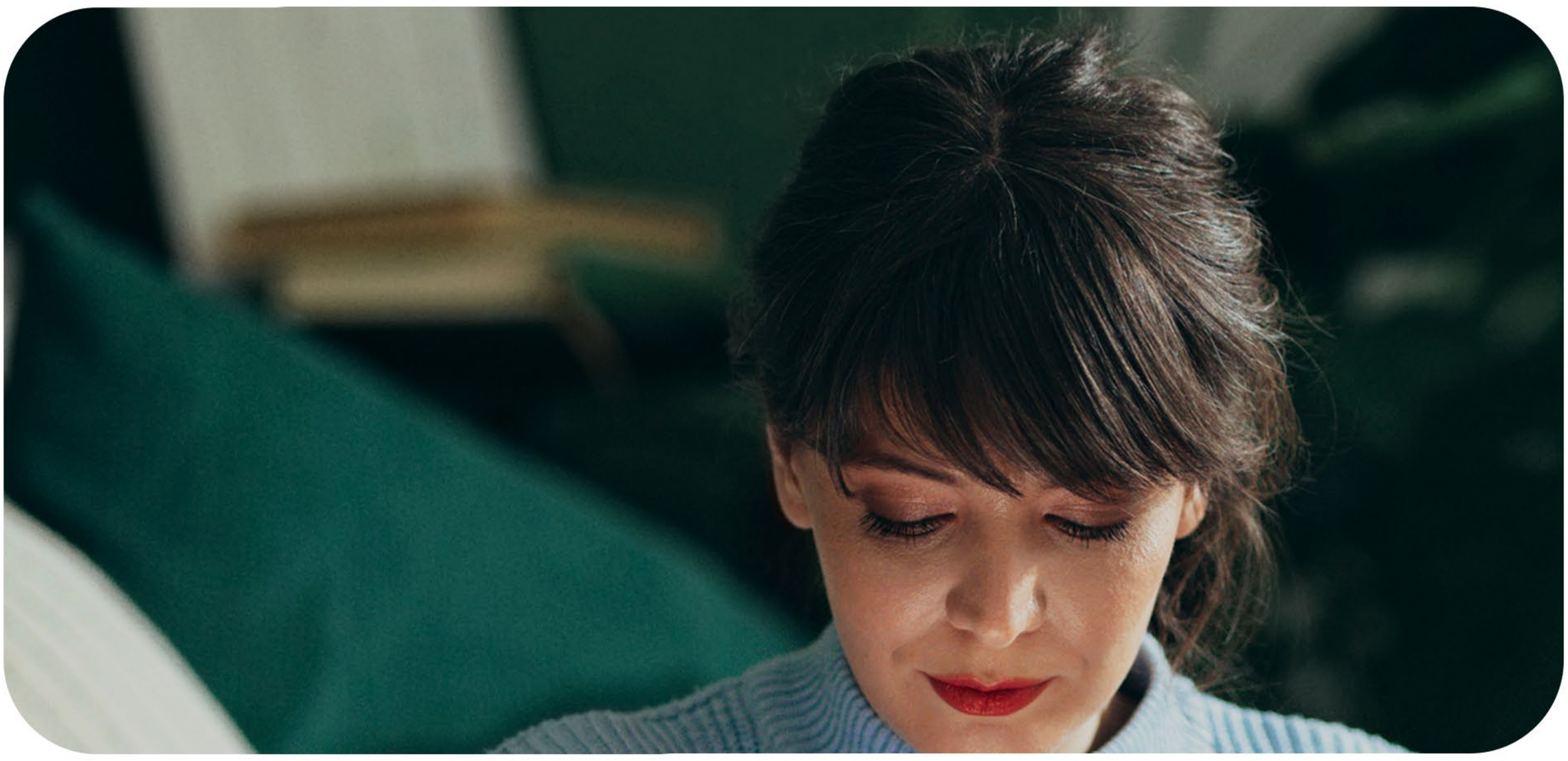
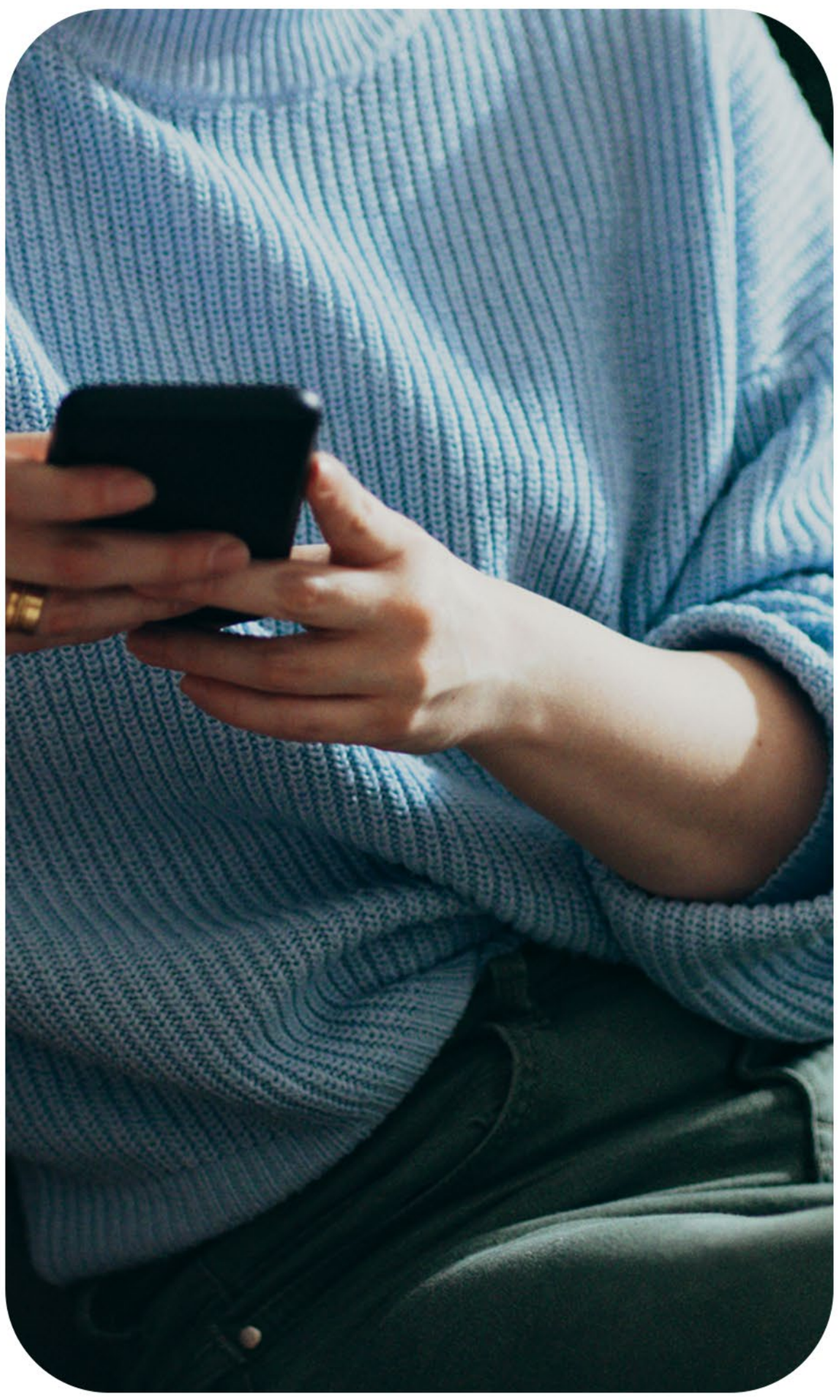




October 2025 Report

Behind the Screens

A Report from Android on Text-Based Scams

Table of contents

Mobile phones are at the center of our daily lives.

They connect us to the people we care about, help us manage our schedules, and navigate the world around us. But that same convenience has created new opportunities for criminals, with text-based scams evolving into a sophisticated, global enterprise designed to inflict devastating financial losses and emotional distress on unsuspecting victims.

And only

4%[1]

of victims recovered their money

A survey conducted by YouGov on behalf of Google shows just how pervasive these threats have become, with

94%

of people reporting receiving a scam text message.

This widespread exposure is reflected in public sentiment, with

73%

of respondents saying they were very or extremely concerned about mobile scams, and...

84%

believing that mobile scams are very or extremely damaging to society as a whole.

Android is on the front lines of this fight.

With billions of mobile devices in active use across the globe, we have unique visibility into how scams emerge, spread, and evolve. We have been building protections against these threats for well over a decade, and today, powered by Google AI, we protect against billions of unwanted messages every single month. This scale, and track record gives us a comprehensive understanding of the problem and how to fight it.

The insights and analysis in this report are based on **user-submitted SMS and RCS spam message reports** from 2025.

We'll start with the scammers' tactics, revealing the most common archetypes and delivery methods. Next, we'll explore the machinery behind the messages, from the anatomy of an attack to the underground economy that powers them. We'll also analyze key international trends, tracking the shifting origins of scams and examining how tactics are customized for different countries. We will close with practical advice to help you navigate the mobile world more confidently.

[1] Global Anti-Scam Alliance, October 2025 https://www.gasa.org/research

The Scam Playbook

Types, Tactics, and Timing

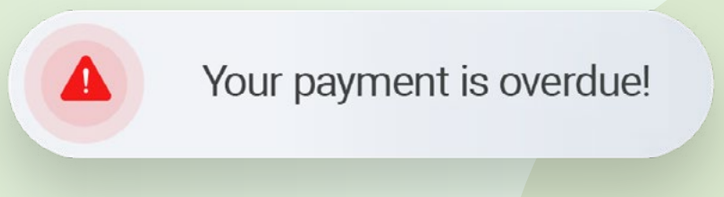
Scammers are constantly evolving their strategies, changing both the types of scams they use and how they deliver them. This analysis looks at two key dimensions of their playbook: the most dominant scam types currently being used and the changing methods scammers use to reach potential victims. Together, these two threads **reveal the current threats users face and show how fraudsters adapt** in an effort to stay ahead.

Dominant Scam Categories

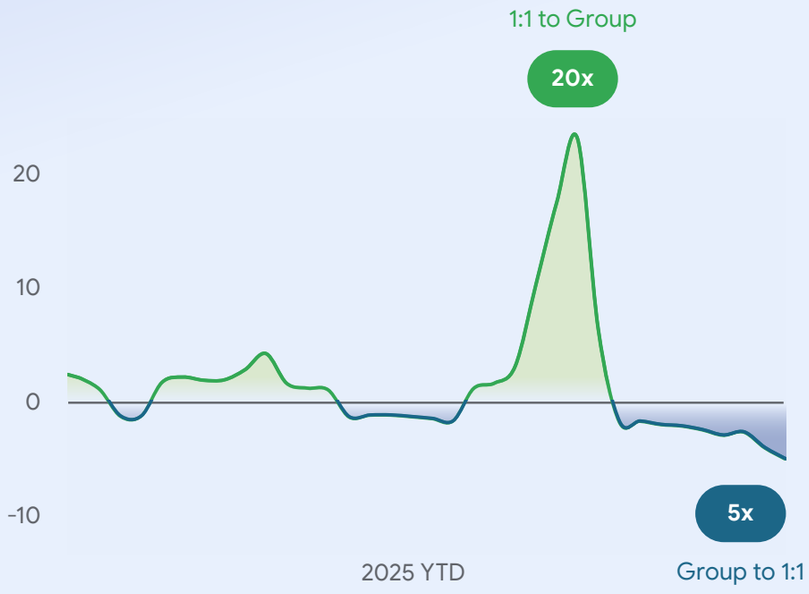
Our analysis of user-submitted reports in August 2025 indicates that a few scam categories dominate. **Employment fraud is the most common**, targeting individuals searching for work with false promises of income to steal personal or financial data. Following this, financially-motivated scams are also widespread, particularly those involving fake unpaid bills, subscriptions, and fees, as well as fraudulent investment schemes in cryptocurrency and other assets. Other notable categories include package delivery and government agency impersonation, with romance and technical support scams being less frequently reported.

>3/4

of user-reported scam messages are related to job offers, unpaid bills, and fake investment schemes



Ratio of 1:1 to group spam messages



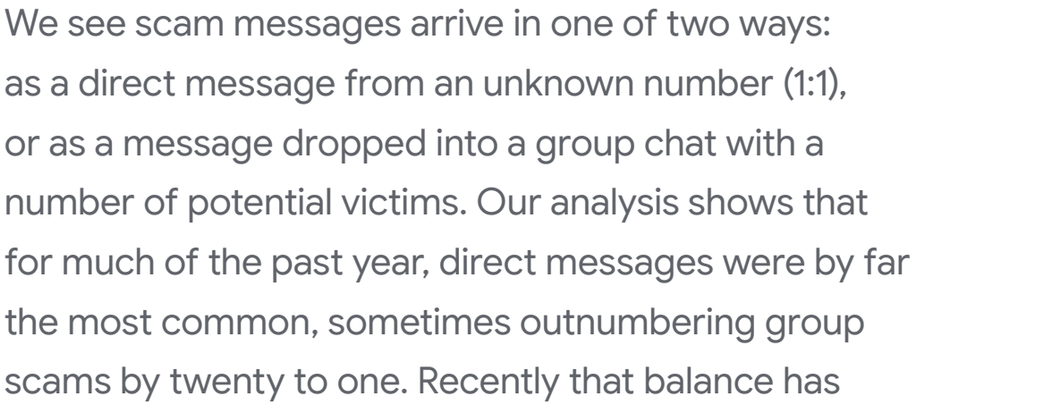
Changing Delivery Methods

We see scam messages arrive in one of two ways: as a direct message from an unknown number (1:1), or as a message dropped into a group chat with a number of potential victims. Our analysis shows that for much of the past year, direct messages were by far the most common, sometimes outnumbering group scams by twenty to one. Recently that balance has flipped. Group messages now dominate, outnumbering 1:1 scams by about five to one. This shift may have happened because group messages can **feel less suspicious to recipients,** particularly when a scammer includes a fellow scammer in the group to validate the initial message and make it appear to be a legitimate conversation.

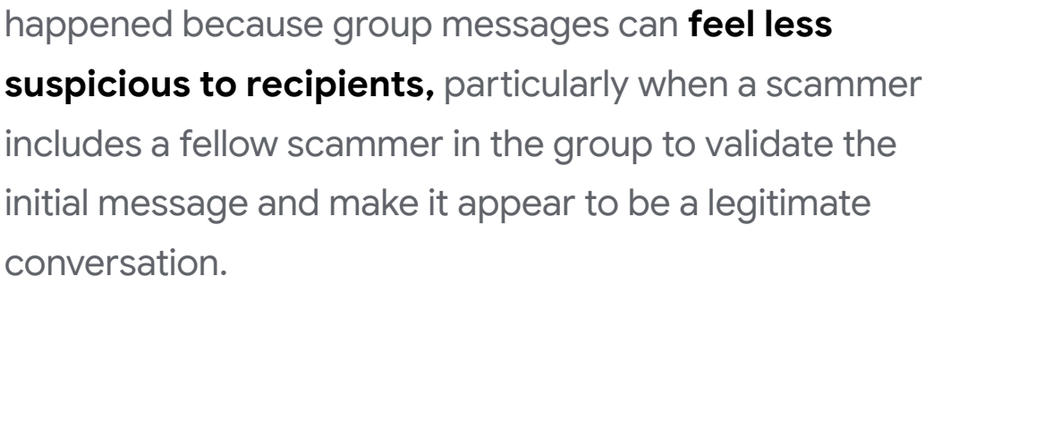
Timing of Messages

Our data reveals that malicious messages are not sent randomly but **follow a distinct daily and weekly schedule.** In the United States, this activity typically begins around 5 AM PT and peaks between 8 AM and 10 AM PT, coinciding with the start of many people's workdays. A weekly pattern also emerges, with the highest volume of fraudulent messages sent on Mondays. This timing appears strategic. At the start of the workday—especially on a Monday morning—recipients are often at their busiest and least critical of incoming messages, while the timing also lends credibility to scams impersonating legitimate businesses.

Spam reports per hour



Spam reports per day



Anatomy of a Scam

Two Paths of Deception

Now that we've covered the common tactics scammers use, we can look at the two primary strategies that guide their deception. While the specific stories change, scammers almost always follow one of two core strategies: the high-volume "Spray and Pray" or the personalized "Bait and Wait." Understanding the journey of each is key to recognizing an attack as it unfolds. From a potential victim's perspective, a scam is designed to feel like a whirlwind of trust and urgency. Whether through sudden panic or a carefully built connection, the goal is to cloud your judgment and pressure you into taking an action that goes against your own best interest.

Spray and Pray

1 Initial Contact

Every scam begins with unexpected contact, but the nature of that hook differs:

Spray and Pray

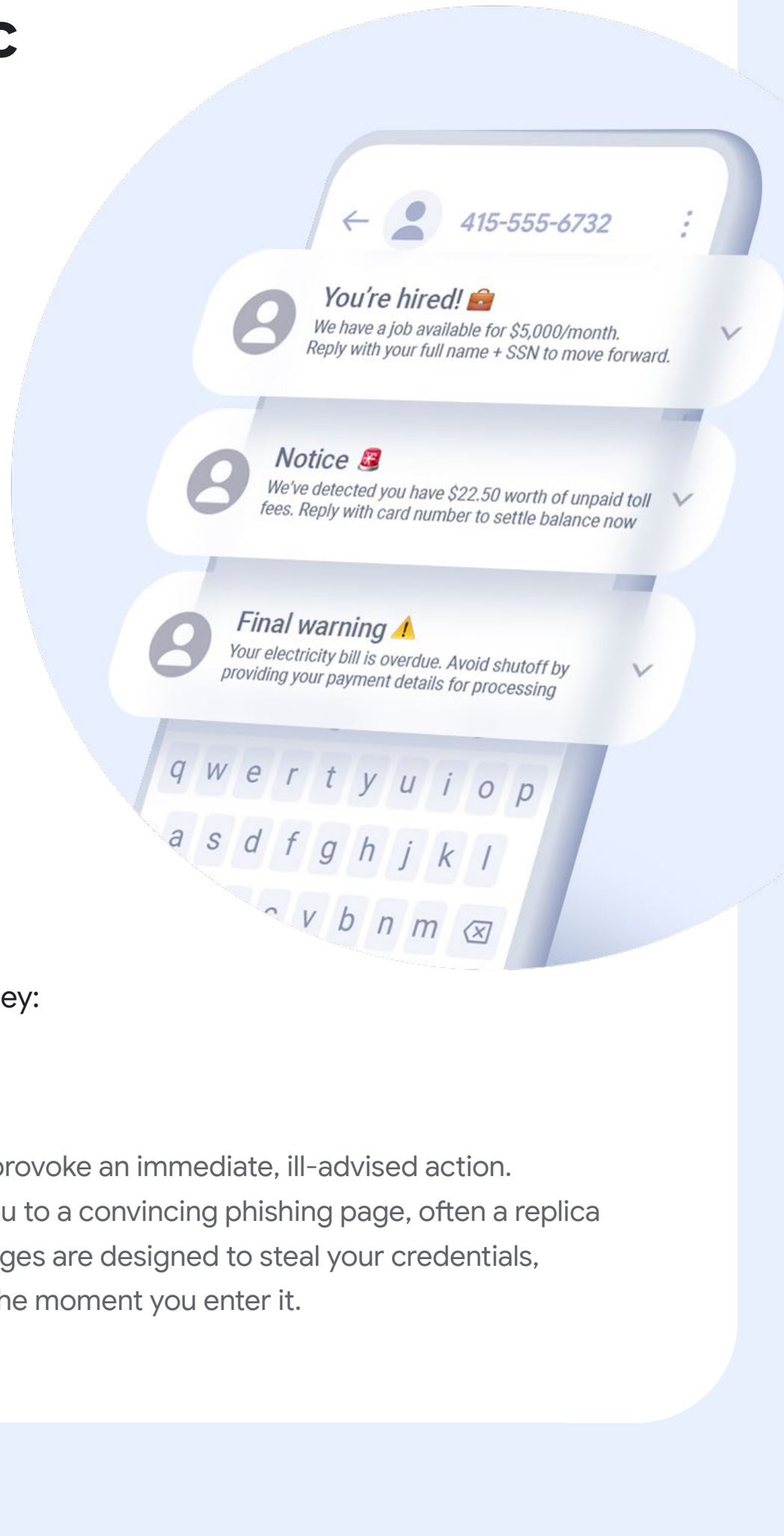
Scammers send out millions of generic messages aiming for a small percentage to fall victim, while leveraging reusable assets like fraudulent websites that they can monetize until taken down. The message is designed to **feel urgent and broadly relevant, often leveraging current events** like tax season or common situations such as package delivery notifications or toll charges.

2 The Manipulation Tactic

Once you're engaged, the scammer's manipulation tactic diverges:

Spray and Pray

The next step is to **provoke a strong emotional reaction,** like panic over a locked account or excitement over an investment opportunity, to rush you into acting without thinking. Scammers use techniques like link-shortening services to mask dangerous websites or swap letters in URLs to appear legitimate, such as creating a fraudulent PayPal URL by swapping the lowercase "l" for a capital "I". The goal is to get you to click a malicious link before you can spot the deception.



3 The Endgame

The final goal is to steal your information or money:

Spray and Pray

The attacks aim to create a **sense of urgency** to provoke an immediate, ill-advised action. These scams typically involve a link that directs you to a convincing phishing page, often a replica of a legitimate site from a trusted brand. These pages are designed to steal your credentials, credit card details, or other financial information the moment you enter it.

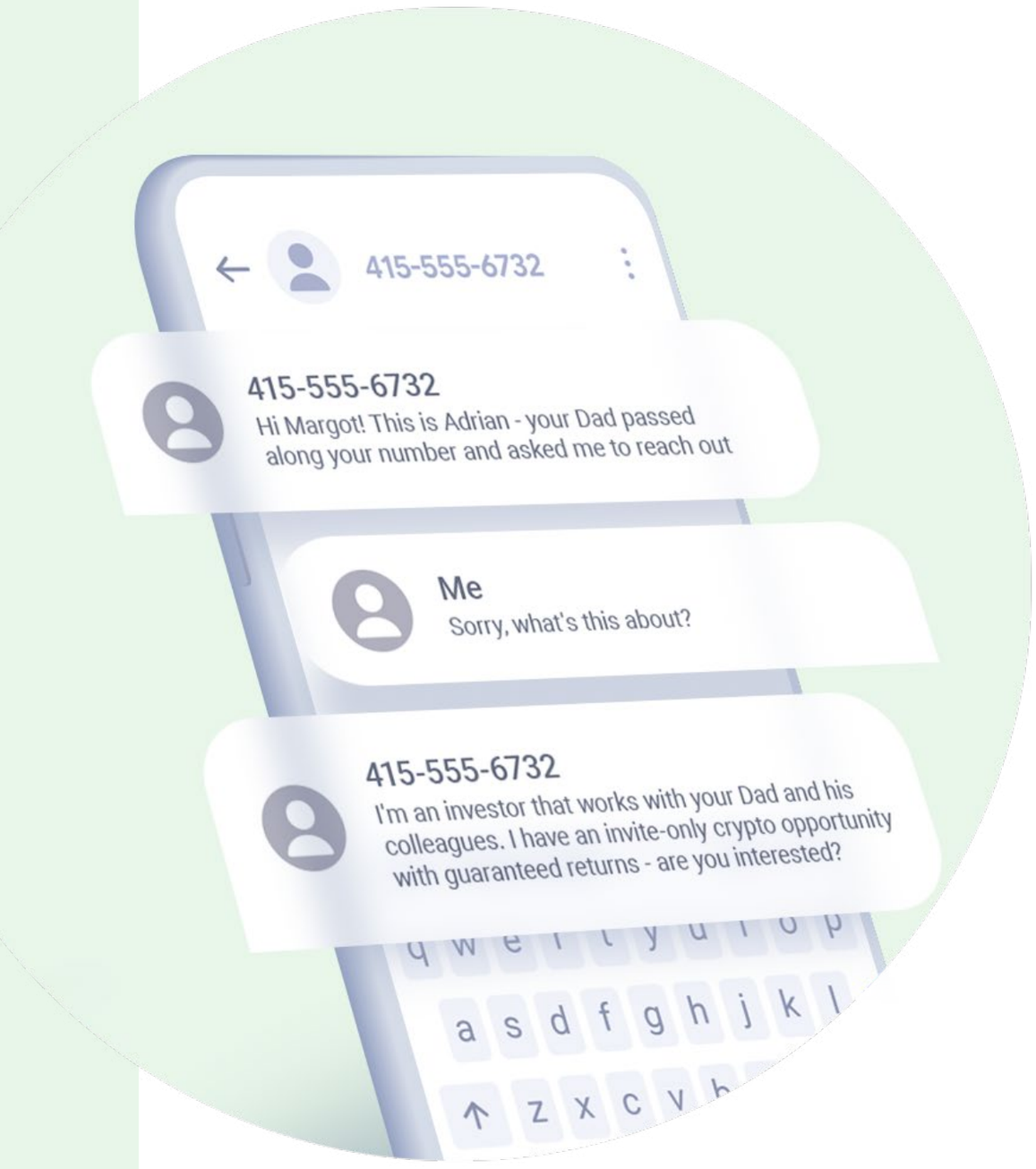
1

Initial Contact

Every scam begins with unexpected contact, but the nature of that hook differs:

Bait and Wait

This is a slow, calculated, human-operated approach that relies on building a false relationship with a single person over time. Instead of malicious links, the attack often begins with a simple, harmless-looking message like “Hello” or “Do you remember me?”. **The message has no immediate red flags** as the scammer’s only initial goal is to get a reply and begin a conversation to initiate the next step.



Bait and Wait

The Manipulation Tactic

2

Once you’re engaged, the scammer’s manipulation tactic diverges:

Bait and Wait

From here, the scammer focuses on **slowly building false trust.** The scammer engages you in a longer conversation, pretending to be a recruiter or old friend. They may even include personal details gathered from public websites like your name or job title, all designed to build trust. They use social engineering to methodically build a relationship before asking for anything.

The Endgame

3

The final goal is to steal your information or money

Bait and Wait

The tactics are more patient, aiming to **maximize financial loss over time.** Scammers often lure victims onto a third-party app to evade security and monitoring, a hallmark of “pig butchering” scams. After building significant trust, they leverage that emotional connection to make an urgent request for money or sensitive financial information. The endgame is to manipulate the victim into sending as much as possible before the scammer disappears.

Both tactics have the same final goal.

While one method relies on volume and urgency and the other on patience and deception, the goal is always to cause financial loss. By recognizing the distinct signs of a high-pressure *“Spray and Pray”* attack versus a slow-moving *“Bait and Wait”* scheme, you can spot the danger early and stop a scam before it succeeds.

The Scamming Value Chain

A Sophisticated Underground Economy

To understand the operational mechanics behind modern scams, we conducted an in-depth investigation into dark web scammer channels and the suppliers of scam infrastructure and tools. Our research reveals that large-scale messaging campaigns are not the work of a single actor. Instead, **scammers operate like sophisticated businesses,** relying on a value chain of specialized and independent providers. Each component of a scam is supported by a thriving underground marketplace, making it easier and more affordable than ever for malicious actors to assemble and launch a campaign.

Target Acquisition and Lead Generation

The foundation of any scam campaign is a **list of potential victims.** Scammers can purchase vast, curated lists of phone numbers from dark web marketplaces, often sourced from data breaches. Alternatively, some providers specialize in open-source intelligence, scraping publicly available information from social media profiles and legitimate websites to generate targeted leads for scam operations.

Infrastructure and Hardware Provisioning

In addition to a list of targets, the operation requires physical infrastructure. A distinct set of **suppliers provides the necessary hardware for «phone farms»,** which include not only the phones themselves but also hundreds to thousands of prepaid SIM cards. These new SIMs are often available from a wide variety of carriers across the globe for under $2 USD, and there's even a robust market for used SIMs at a discount. Custom-built SIM card extenders and SIM boxes are also key components offered in this market, enabling a single device to manage and swap between dozens of SIMs, maximizing operational efficiency.

Specialized Software & Phishing-as-a-Service

Scammers turn to another layer of the supply chain for specialized software. Dark web developers create and sell **custom tools for managing the phone farms and for modifying core device identifiers like the IMEI number** to evade carrier detection. They also partner with sophisticated Phishing-as-a-Service providers. For a fee, these providers deliver a turnkey solution that includes not only hosting convincing replicas of well-known regional websites (such as banks or postal services)to efficiently harvest user credentials and financial information, but also providing the analytics and monitoring software to track and manage the scam campaign.

Message Deployment and Distribution

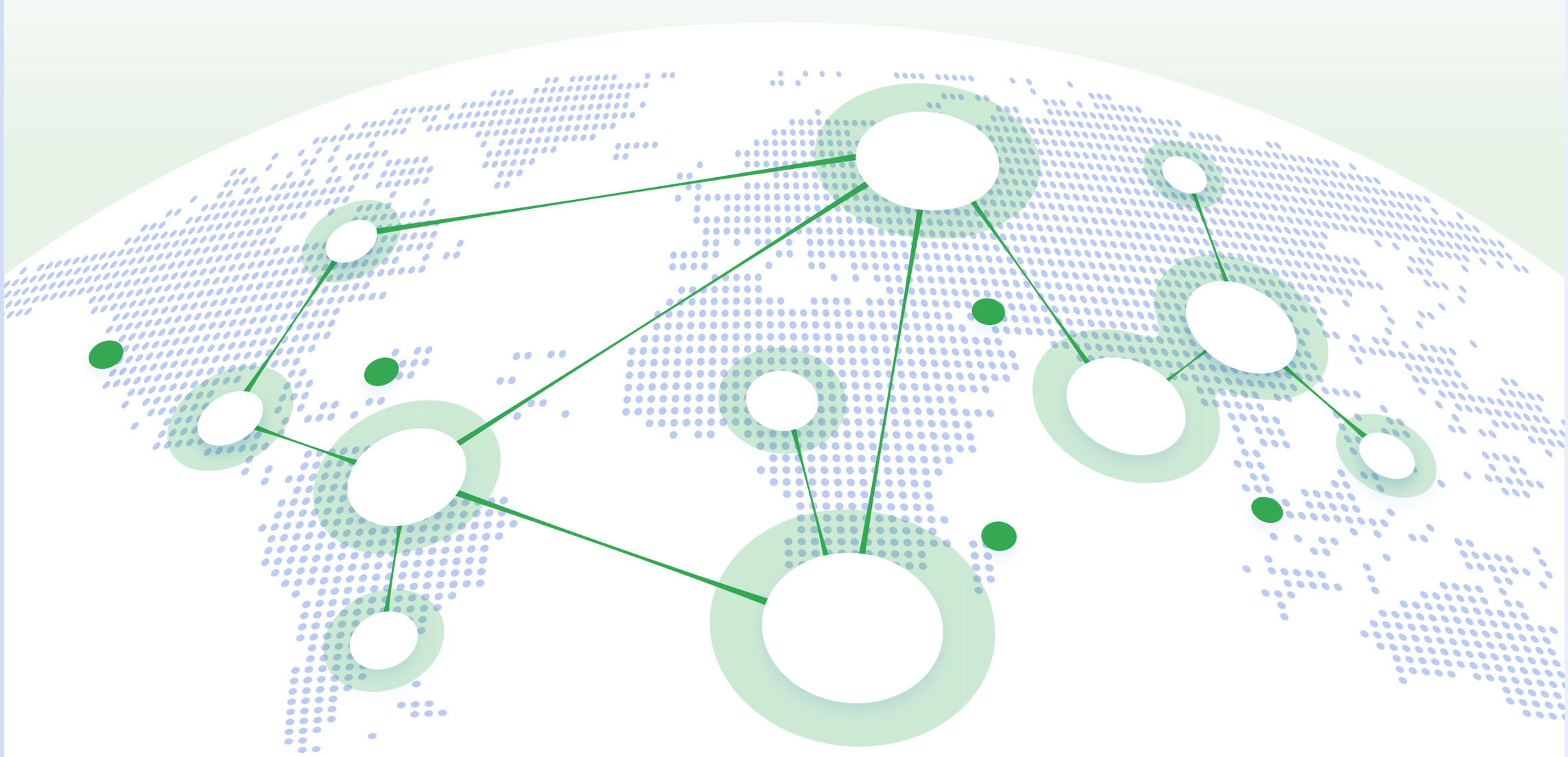
The final link in the value chain is message distribution. While some scammers use their own phone farms for this, many now outsource the work to third-party bulk messaging services. These **illicit providers offer enormous scale,** capable of sending over a million messages per day at a very low cost. They are the distribution engine that connects the scammer's infrastructure and target lists to the end victim, delivering the malicious links that lead to the PhaaS-hosted websites.

Follow the SIMs

How Scammers Exploit a Global Marketplace

Analysis of the origin of scam messages reveals a highly volatile landscape. While it may appear that waves of scams are moving between countries, this constant churn doesn't mean scammers are physically relocating. Instead, it points to a calculated strategy where fraudsters seek the path of least resistance, purchasing SIM cards in bulk from markets that present the fewest obstacles. Once enforcement tightens in one area, they simply pivot to another, **creating a perpetual cycle of shifting hotspots.**

Our data from the past year highlights several of these notable shifts.



2025

The start of the year

began with most malicious messages originating from English-speaking countries, a pattern that was disrupted in early March by a sudden, short-lived wave from the Democratic Republic of the Congo. Scammers then pivoted to Turkey, which became a new hotspot in April. From late spring through June, activity returned to English-speaking nations, culminating in a significant increase in overall scam volume.

In the second half of the year,

this trend picked up speed. After another large wave of messages from Turkey in July, August marked a clear shift toward South American countries, which remained a source of steady growth through September. At the same time, Indonesia suddenly emerged as another major hotspot. These rapid pivots are a **powerful indicator of how quickly scammers can activate new scam campaigns** across the globe.

Fraud in Focus

How Scams Evolve Across Countries

Just as the sending locations of scams change, the scams themselves are often tailored to the specific countries they target. While mobile scams are a global phenomenon, **their forms frequently reflect local economic conditions and cultural norms.** To understand these differences, we analyzed user-submitted reports and categorized each report into one of the following scam types:

- Bill, subscription, and fee scams
- Blackmail or threat scams
- Crypto and investment scams
- Employment opportunity scams
- Financial impersonation scams
- Government agency scams
- Package delivery scams
- Prize and gift scams
- Relationship and romance scams
- Technical support and security scams

Here are the top three scam categories from a selection of countries analyzed:

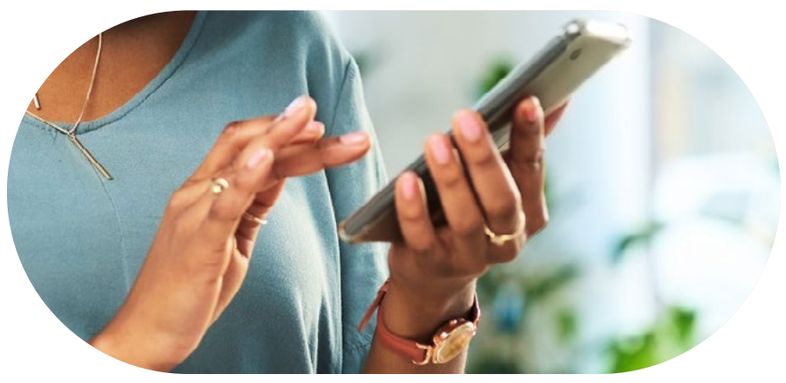
	1	2	3
Australia	Prize and gift scams	Employment opportunity scams	Crypto and investment scams
Brazil	Prize and gift scams	Crypto and investment scams	Financial impersonation scams
Canada	Bill, subscription, and fee scams	Package delivery scams	Employment opportunity scams
France	Package delivery scams	Financial impersonation scams	Bill, subscription, and fee scams
Germany	Employment opportunity scams	Package delivery scams	Government agency scams
United Kingdom	Government agency scams	Employment opportunity scams	Bill, subscription, and fee scams
United States	Employment opportunity scams	Bill, subscription, and fee scams	Financial impersonation scams

These country-specific insights highlight just how diverse and adaptive scam tactics can be. While the exact factors driving these patterns are not fully known, the findings offer a fascinating glimpse into the ways fraud evolves across different markets, revealing both local nuances and broader trends that could inform prevention and awareness efforts.

Staying Safe

3 Practical Habits to Protect Yourself from Scams

While the tactics scammers use are constantly evolving, a few key habits can make a major difference in staying safe. Scammers often pretend to be a trusted business or government agency, using familiar names and official-sounding language to gain your confidence. Most scams rely on one of two tactics: the promise of a reward (“You’ve won a prize!”) or the threat of a consequence (“Your driver’s license will be suspended”). To create urgency, these are almost always followed by a strict deadline, pressuring you into acting before you have time to think clearly.



The good news is that by following a few simple steps, you can significantly lower your risk:

Have a healthy dose of skepticism

If an unknown person contacts you with an offer or opportunity that seems too good to be true, it probably is. Be cautious with all messages from unfamiliar numbers. If someone claims to represent a business or government agency, check that they’re verified in Google Messages, and if you’re unsure, end the conversation and call the organization’s publicly listed customer support number to confirm.

Don’t take action immediately

Legitimate businesses and government agencies will not demand instant action or payment over text message. Scammers create a false sense of urgency to prevent you from thinking things through. If a message feels suspicious, slow down, pause the conversation, and talk it over with a friend or colleague before proceeding. Never share personal details, give remote access to your screen, or click on unknown links or attachments.

Stay alert and informed

Your Android device can often detect and warn you about potential scams. Pay close attention to these alerts. To ensure this and other built-in protections are as effective as possible, always install the latest OS updates and security patches from your device manufacturer. Avoid using public Wi-Fi whenever possible, as these networks can be unencrypted and easily exploited by attackers. Keep an eye on your bank accounts and credit report regularly; many banks and credit card companies offer free monitoring tools.

A Report from Android on Text-Based Scams

Mobile scams are a complex and fast-moving problem that affect people in every region and from every background. In this report, we examined how these scams work, the most common tactics in use today, and the individuals and networks behind them. We also explored how these schemes change over time as scammers adapt to new defenses and search for new opportunities.

The insights, patterns, and trends shared here come from one of the most comprehensive views of mobile activity in the world. With billions of Android devices in use and more than a decade of experience fighting scams, **we have developed a deep understanding of the scope of the threat, the forces that shape it, and the most effective ways to defend against it.** By understanding how these attacks are built and launched, we hope that you can navigate the mobile world with greater safety, confidence, and peace of mind.