Bitdefender

The Global Scam Intelligence Report 2026

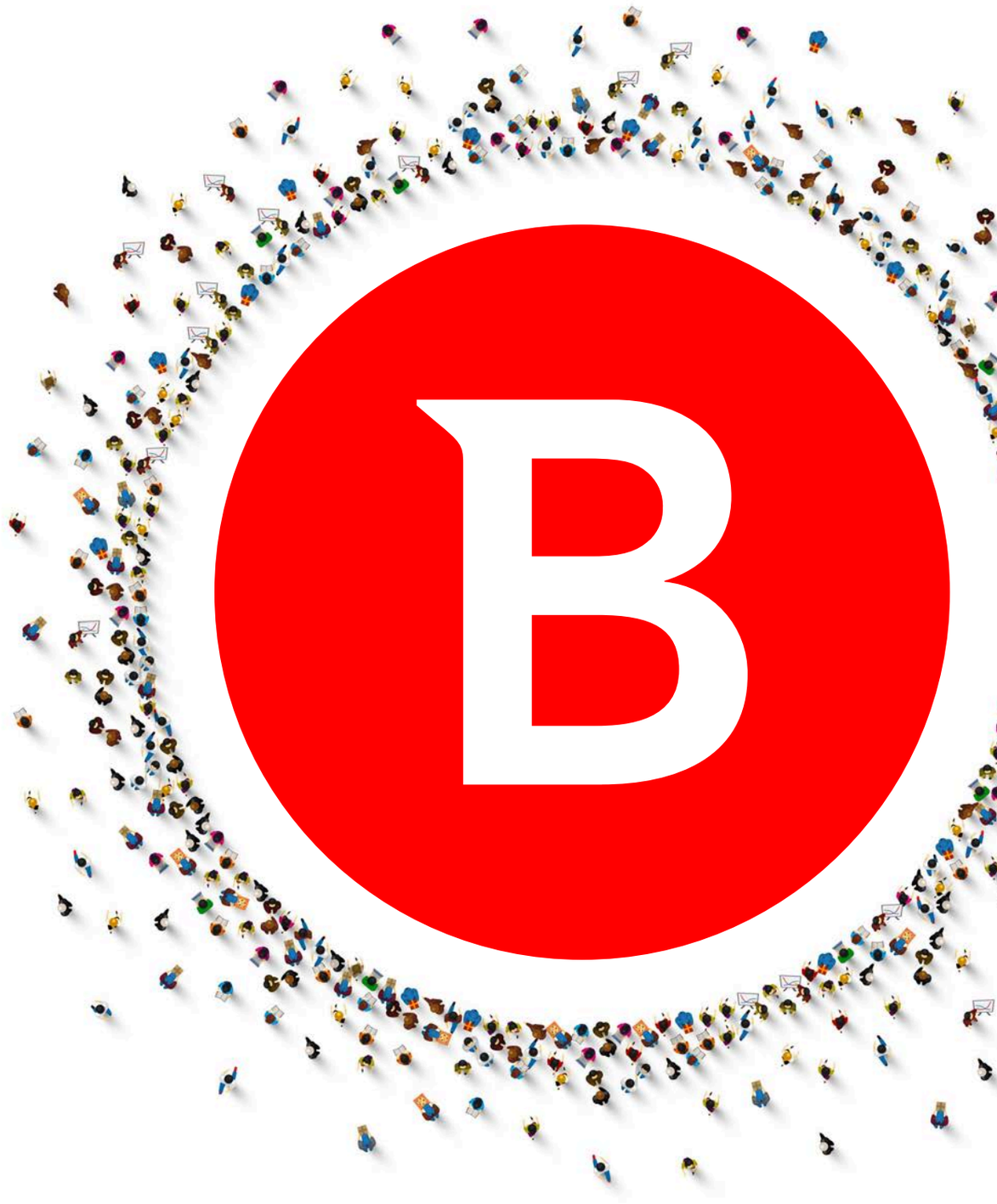
We block billions of scams every year. Here's what we learned from the front-line battle with a trilion dollar criminal business model.

Foreword

In 2025, scams **inflicted roughly $442 billion** in consumer losses, making this underground industry a global financial threat to any consumer unlucky enough to stumble into one.

Despite the numbers, most conversations about scams rely on personal stories, surveys, and victims sharing their experiences after the fact. This approach creates sympathy but does not help people understand the situation as it happens. This **Global Scam Intelligence Report** changes that by treating scams as an active, adversarial system that can be measured and tracked in real time.

Scams are no longer just local crimes. They now operate across borders and use many channels, acting like real businesses with staffing schedules, regional targets, marketing budgets, and performance metrics. No single country, platform, or law enforcement agency sees the whole picture. Without a global view, defenses remain scattered while scammers work together effectively.



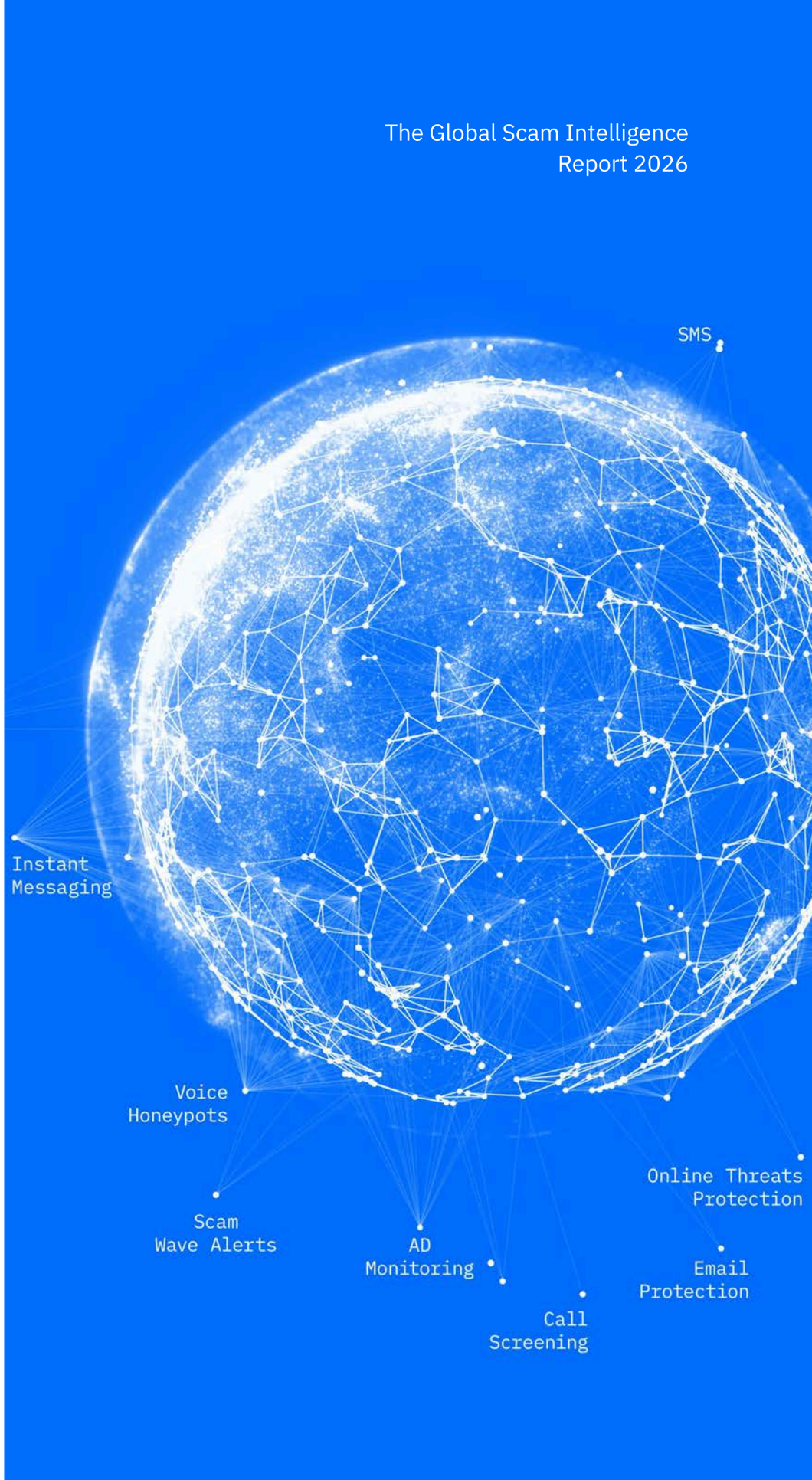
Bitdefender

About this report

We analyze and block billions of scams every year

Few organizations see scams as they happen, across channels, at a global scale. Bitdefender does. The visibility behind this report comes from real-time insights, not surveys, spanning **trillions** of URLs, **billions** of messages, live ad ecosystems, call honeypots, and direct consumer submissions. That vantage point allows patterns to emerge early, campaigns to be tracked across platforms, and shifts in attacker behavior to be documented while they are still in motion. The **Bitdefender Global Scam Intelligence Report** is a field report built from the front lines of consumer digital life, by a company that has spent decades watching adversaries adapt, and learning how to stop them.

This report is built on insights collected and analyzed between January 1 and December 31st, 2025. It captures the most recent developments in the scam landscape



Bitdefender

Scams were the fastest-emerging **forms of cybercrime** in 2025

Our 2025 Consumer Cybersecurity Survey of 7,000 people across seven countries found that **1 in 7 consumers** (14%) **fell victim to a scam** in the past year. The US led, at 17%, followed by the UK and Australia, at 16% each. Global losses exceed $1 trillion annually.

2.8 T
Short URLs scanned in 2025

10 B
phishing URLs identified and blocked

1.4 B
short messages analyzed

60 M
people targeted by scam ads on social media and video content websites

52 M
phone numbers analyzed for reputation

Key Findings

01 **Social media has overtaken email as primary attack vector**

Young people are now twice as likely to fall for scams as older generations (20% vs 9.7%). This is because they spend more time on platforms where scammers concentrate their efforts.

02 **Finance scams dominate every channel**

Scammers mainly target money. Investment fraud, banking phishing, and crypto scams dominate across SMS, social ads, WhatsApp, voice calls, and email

03 **Scam operations run like businesses**

Our call timing data shows peak activity Tuesday through Thursday, 70-80% declines on Sundays, and holiday patterns that mirror those of legitimate corporations. These are organized operations with shifts and schedules.

04 **Trust is THE vulnerability**

The most effective attacks don't come from strangers. They come from compromised accounts of friends and family, from brands people recognize, from platforms they use daily.

05 **Geography shapes risk**

Cultural habits create distinct vulnerabilities. Germany's SMS scam rate runs 4x the global average. Romania leads in ad scam exposure. France dominates delivery fraud.

The Global Context

The Global Context

Mass arrests in Cambodia

Cambodia spent much of 2025 running one of the largest anti-scam enforcement campaigns in the region. Starting mid-year, authorities carried out coordinated raids across provinces, shutting down hundreds of suspected online scam compounds and detaining thousands of suspects. News reports documented raids and arrests in the thousands under a government directive to “clean up online scams.” Operations detained a wide range of nationalities and seized equipment used for fraud operations.

Later figures - compiling government reporting and independent sources - put the total suspects arrested/deported into the low thousands by late 2025, with authorities claiming hundreds of sites dismantled.

In addition to broad raids, Cambodian police also took down more specific syndicates. In December 2025 law enforcement in Phnom Penh detaining about 28 suspects and seized phones, computers, and SIM cards tied to the scheme.

Those enforcement efforts continued into early 2026, with government figures showing about nearly 200 scam centers closed, hundreds of “senior crime figures” arrested, and thousands of workers deported. Critics frame this as a mix of genuine enforcement and political narrative management, but the volume of disruption was substantial.

On the humanitarian side, many workers who were freed or fled scam compounds in Cambodia ended up in shelters with minimal support due to cuts in foreign aid, creating a secondary crisis of displaced victims of scam labor.

The Global Context

Myanmar: raids and contested progress

Myanmar's situation in 2025 was complicated by politics and conflict. Scam centres — especially big hubs like KK Parknear the Thailand border — were on the radar of law-enforcement. The military junta announced raids on major scam operations, claimed to have cleared KK Park and freed over 2,000 workers, and seized satellite internet gear often used to sustain scam operations.

There were also reports of arrests in other centres like Shwe Kokko, where hundreds of individuals allegedly linked to scam operations were detained. International reporting corroborated that Myanmar's scam centres remained a target, though independent verification of enforcement effectiveness varied.

A notable individual case in January 2025 involved the kidnapping of a Chinese actor by a Myanmar-based fraud gang. The actor was forced to work in a scam centre for several days before being rescued. That attracted widespread coverage as an attention-getting and concrete illustration of how scam networks operate with real harm to victims.

The Global Context

Malvertising was a major battlefield in 2025

Looking at the broader scam landscape of 2025, we can no longer consider that malvertising is a niche tactic. In 2025, it became the primary delivery mechanism.

Bitdefender Labs uncovered wave after wave of malicious campaigns abusing Meta, Google, and YouTube ad ecosystems. Fake “TradingView Premium” ads jumped platforms. Fraudulent “Meta Verified” browser extensions stole accounts. Crypto malware chains were delivered through sponsored posts. Even fake beta invites for games like Battlefield 6 and The Witcher 4 were pushed through paid ads.

Attackers increasingly relied on legitimate advertising infrastructure to distribute malware, harvest credentials, and deploy crypto-draining payloads. Some campaigns evolved across operating systems, expanding from desktop users to Android devices. Others layered in multi-stage malware chains designed to evade detection and maximize impact.

The Global Context

Scammers hijacked real-world events in real time

Another defining trend of scams in 2025 was speed.

Fraudsters capitalized on news cycles almost instantly. When global events unfolded - from the death of Pope Francis to the tragic passing of Liverpool’s Diogo Jota - scam campaigns followed.

Seasonal moments were equally exploited: Easter, Halloween, Black Friday, Christmas, and even viral product hype like the Starbucks Bearista cup all became bait.

Concert tours featuring Metallica and The Weeknd were turned into fake ticket scams. Holiday travel spikes triggered malware campaigns targeting Booking.com partners.

Scammers monitored what people were already searching, grieving, celebrating, or anticipating - and inserted themselves into the moment.

The Global Context

Gamers were highly targeted in 2025

Gaming culture continued to prove irresistible to cybercriminals. Fake beta invites, early-access promises, and “exclusive” game builds were used to steal Steam credentials and deploy infostealers. High-profile titles generated predictable waves of fraud. The formula was simple: hype + scarcity + urgency.

Because gaming accounts often hold valuable digital assets, saved payment methods, and in-game purchases, they’ve become a lucrative target. And younger audiences, eager for early access, are more likely to click first and verify later.

What looked like fan excitement often masked credential-harvesting operations.

The Global Context

Messaging apps expand the attack surface

Email and social media weren’t the only channels under pressure.

In 2025, messaging platforms became high-speed scam amplifiers. The “Vote for My Child” scam spread rapidly across WhatsApp networks in Europe, exploiting trust between friends and family members. These campaigns relied on social forwarding mechanics, making victims unknowingly recruit others.

The Global Context

Email still thrived, but smarter

Despite the rise of malvertising and social scams, email fraud never disappeared.

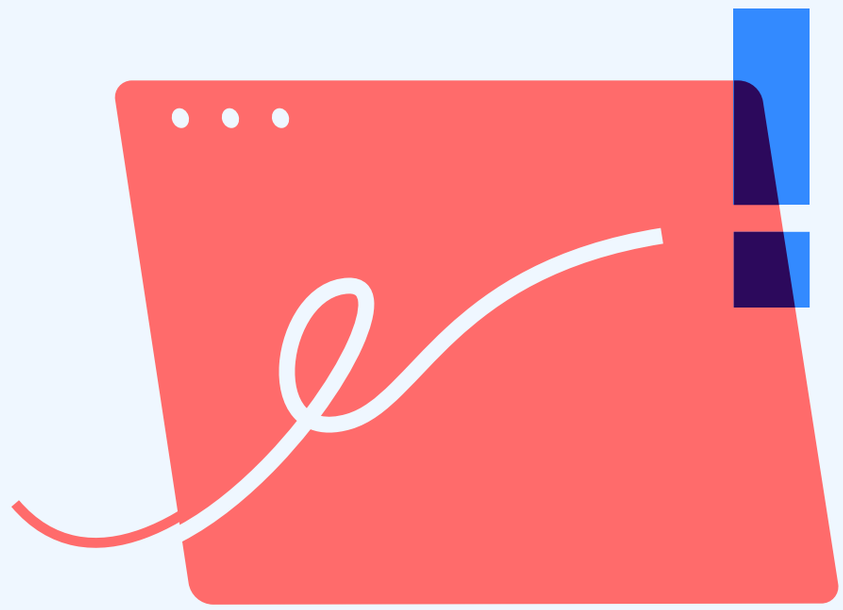
Holiday-themed spam analysis revealed that more than half of Christmas-themed spam emails in 2025 were scams. Black Friday inboxes were flooded with brand impersonation campaigns. Tesla and SpaceX stock giveaway emails circulated widely. Fake invoices, travel confirmations, and investment pitches continued to land in inboxes around the world.

Modern phishing emails are cleaner, better written, and often paired with secondary attack stages like malware loaders or credential-harvesting portals.

Email remains a foundational tool in the scammer playbook. It simply evolved alongside everything else.

Scams are no longer isolated tricks. They’re coordinated ecosystems operating across ads, search engines, social platforms, messaging apps, and inboxes, often simultaneously, designed to blend seamlessly into everyday online activity.

The Evolution of Scams Globally



Bitdefender

The Global Scam Intelligence Report 2026

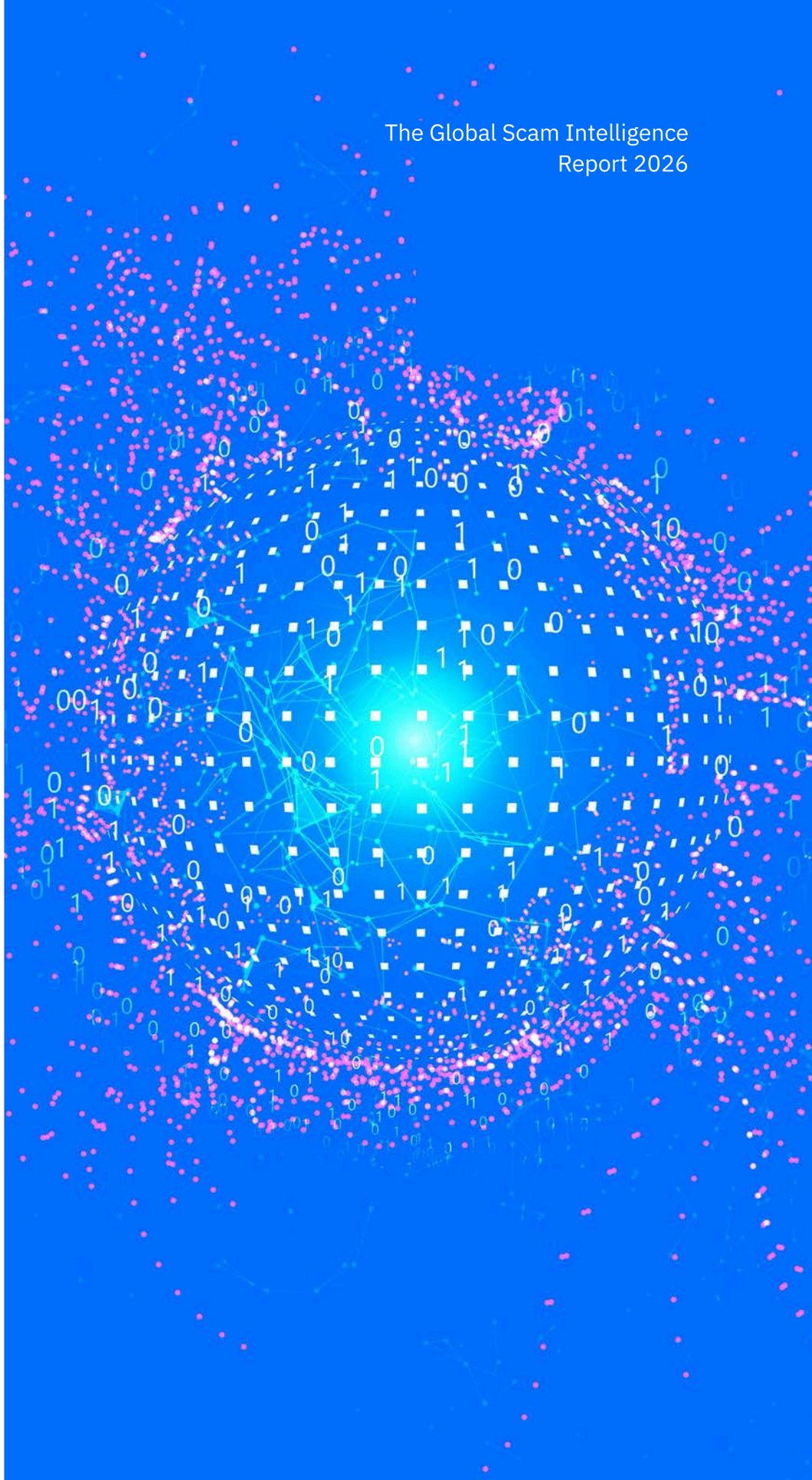
The Evolution of Scams Globally

Web-based threats

Web-based threats remain the primary delivery infrastructure for digital scams. Between January and December 2025, Bitdefender scanned 2.8 trillion URLs across browsers, email clients and messaging apps.

This dataset sheds light on malicious link distribution and its scale, phishing infrastructure, fake storefronts impersonation pages and scam delivery through email and messaging platforms.

Unlike user-submitted reports, Web/URL-based telemetry reflects exposure-level activity, including both successful and blocked attempts, providing useful insight into scam infrastructure, as well as its deployment and propagation.



The Evolution of Scams Globally

Global scam breakdown by category

Phishing is the dominant category globally, accounting for roughly a quarter of all reported incidents, or 24.5 percent. It is followed by financial and investment scams at 10.7 percent, fake shop and advertising scams at 9.3 percent, and job scams at 8.7 percent.

Social media scams at 7 percent and delivery scams at 5.9 percent round out the upper tier, with romance, crypto, advance fee, and survey scams completing the global top 10.

The top three categories alone account for close to half of all reported activity, indicating a high concentration of criminal effort in a small number of scalable fraud models.

The Evolution of Scams Globally

Global overview

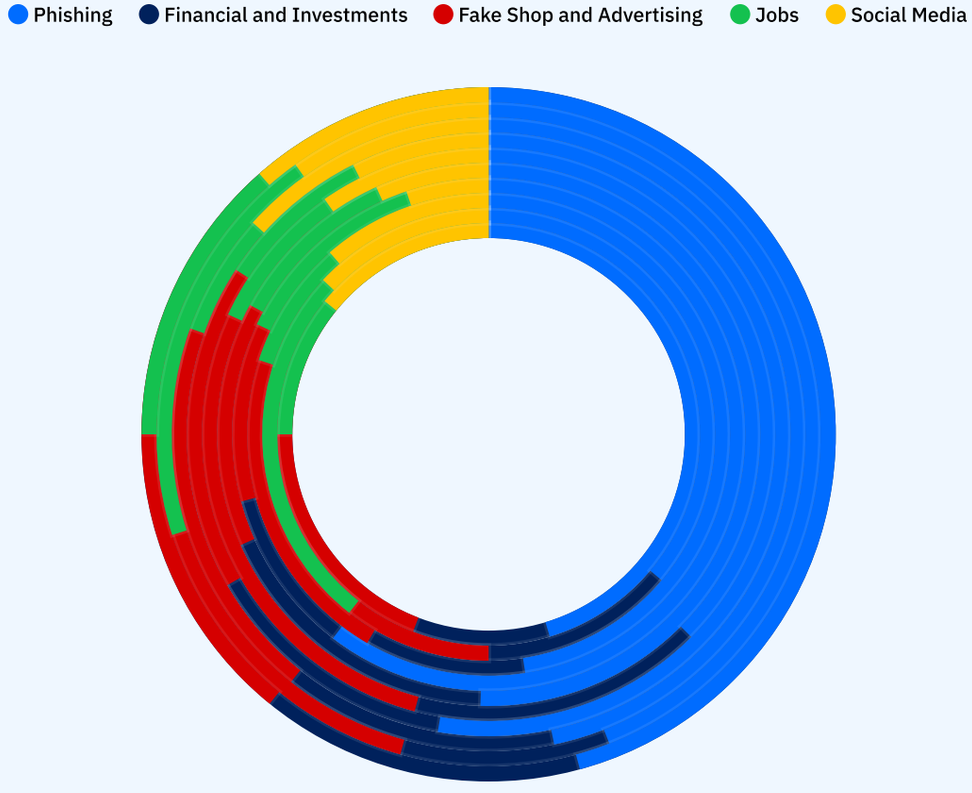
Regionally, **phishing** is consistently the leading threat across all analyzed markets. However, its relative weight varies, exceeding 30 percent of total scam volume in some countries.

Financial and investment scams show strong performance in multiple Western markets, reflecting both higher disposable income and mature online trading ecosystems.

Fake shops and fraudulent advertising campaigns also rank prominently across regions, underscoring the role of social media and online ad platforms as primary distribution vectors.

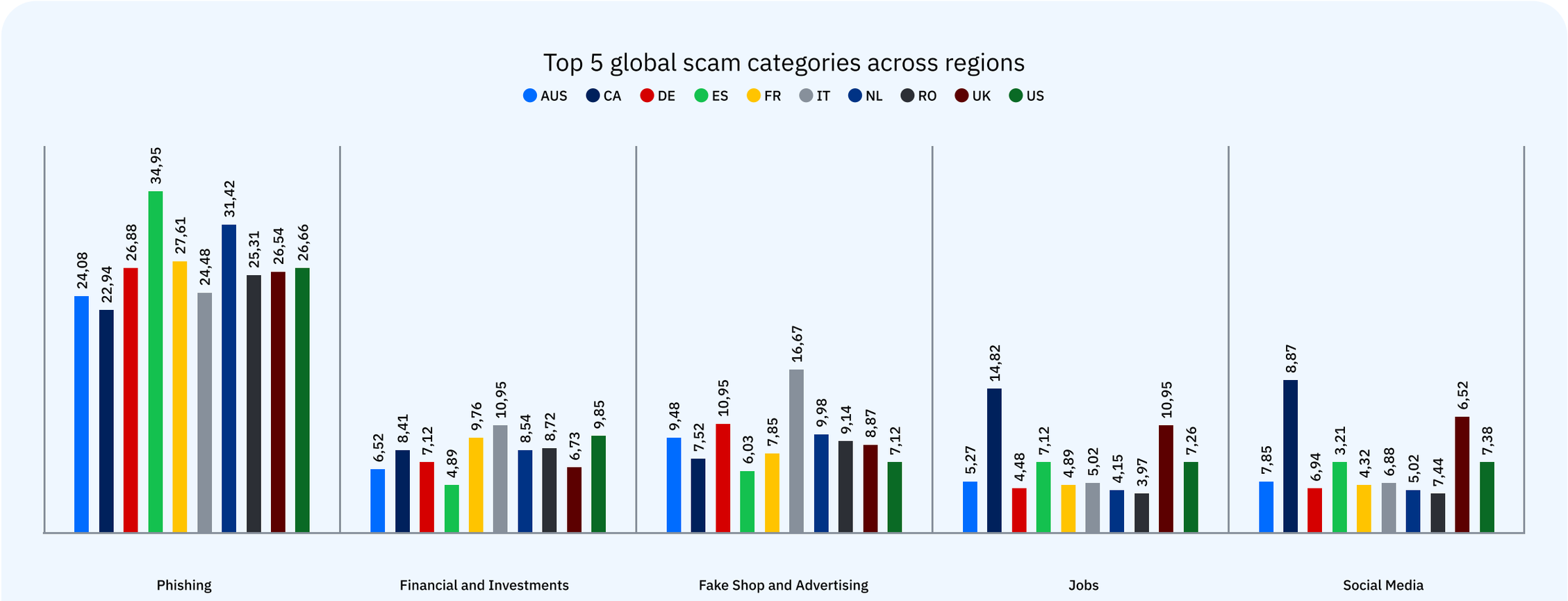
Job scams and **social media scams** appear as embedded categories rather than local anomalies, suggesting that criminals are systematically exploiting employment anxiety and platform trust at scale.

Top 5 global scam categories



The Evolution of Scams Globally

Global overview

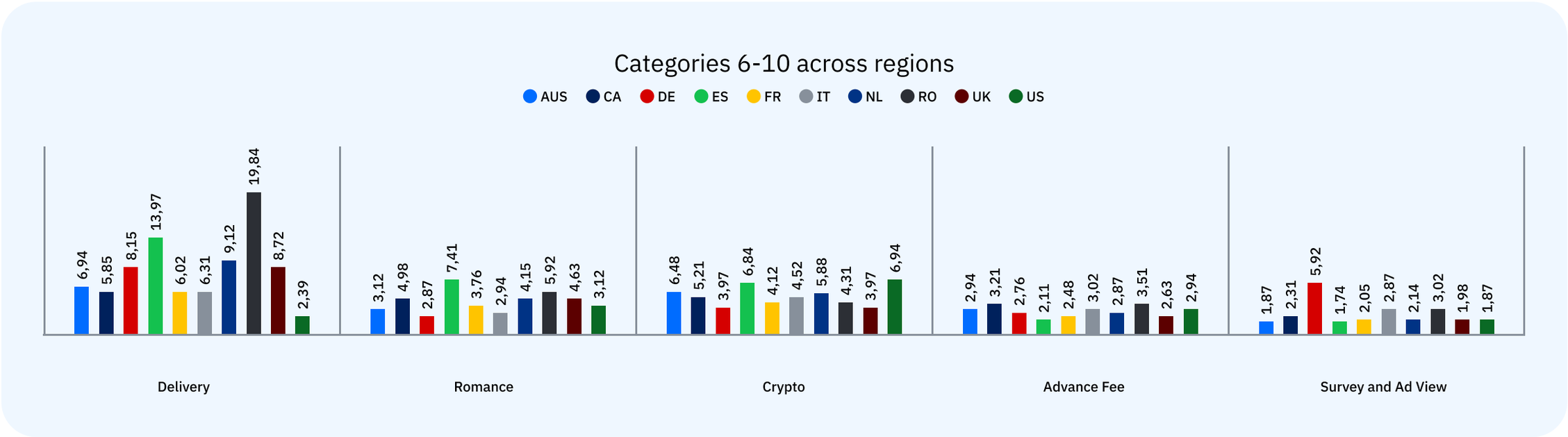


The Evolution of Scams Globally

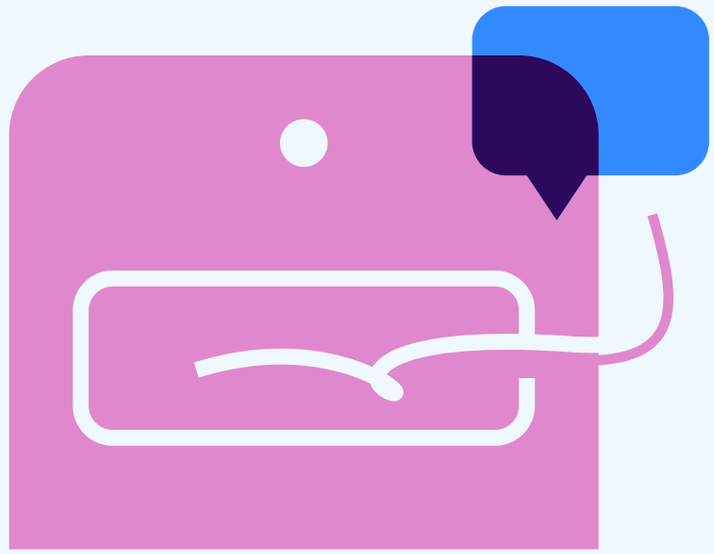
Global overview

The cross-regional comparison highlights that while the top five categories are broadly consistent worldwide, mid-tier categories such as delivery scams, romance scams, and crypto fraud fluctuate significantly by country. This indicates that fraudsters adapt lures to local context while preserving the same operational backbone.

The long tail of smaller categories, including advance fee, survey, gambling, and extortion scams, represents lower individual percentages but collectively contributes meaningful volume. For slide purposes, the key message is straightforward: phishing remains the global anchor threat, financial and ad driven scams form the second wave, and regional variation reflects tactical localization rather than fundamentally different criminal playbooks.



SMS-Based Scams



SMS-Based Scams

SMS remains one of the most intimate digital communication channels

Unlike mail or web content, text messages arrive directly on personal devices, often alongside legitimate communications from banks, delivery services, family members and employers. This proximity creates an inherent trust bias, one that threat actors systematically exploit.

These figures reflect organized, campaign-based activity rather than isolated spam attempts, hinting at structured and repeatable operational models.

140 K
scam clusters

260 K
risky campaigns

92 M
risky messages

SMS-Based Scams

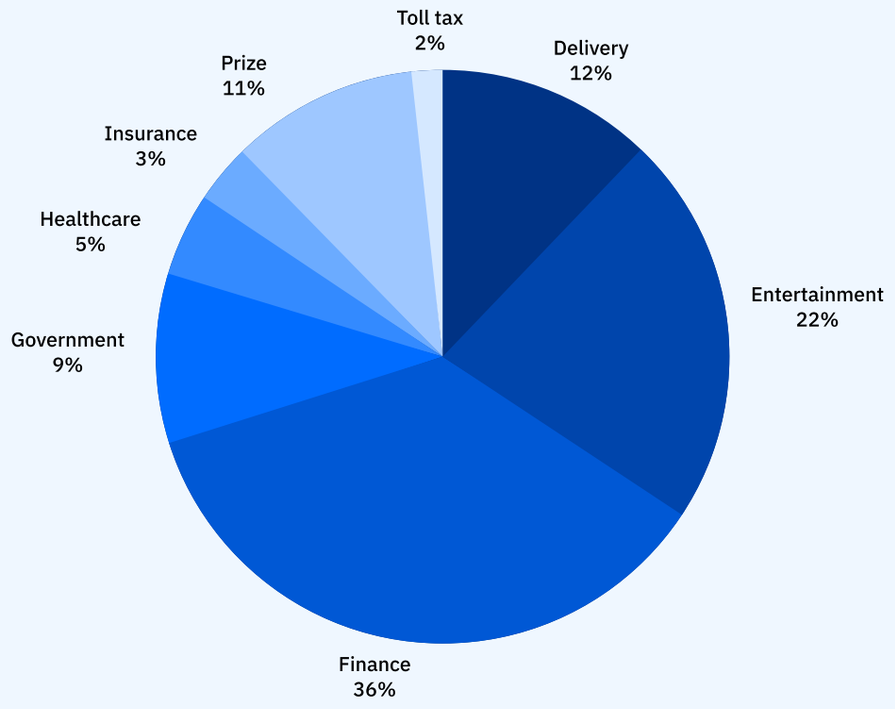
SMS campaign density and risk ratio

Across the analyzed SMS aggregation, 5,16% of all analyzed SMS traffic was associated with risky campaigns.

This means approximately 1 in 20 analyzed SMS messages exhibited characteristics consistent with scam infrastructure or coordinated fraud. From a defensive standpoint, this represents a high contamination rate for a communication channel typically perceived as high-trust.

Analysis of identified risky SMS campaigns shows a clear concentration in financially motivated and service-impersonation scams via SMS.

SMS scam category distribution

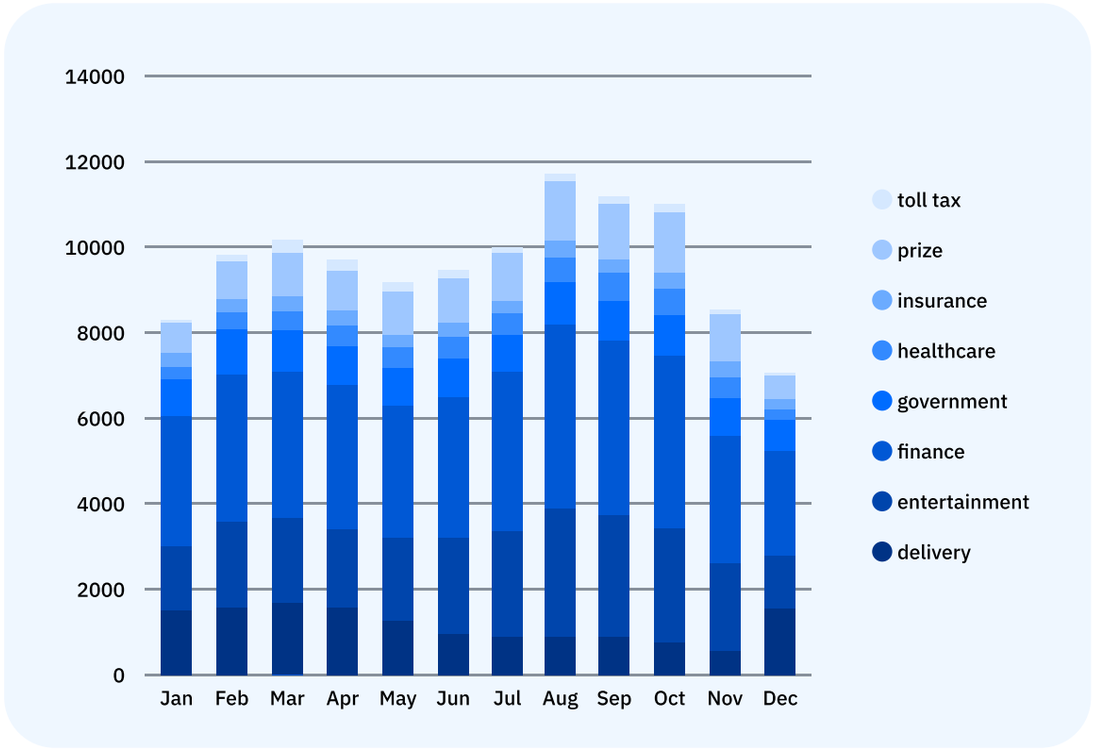


SMS-Based Scams

Risky SMS category evolution in 2025

Finance is dominant every single month. Entertainment is the clear second pillar, showing rapid growth through summer, and peaking around August before softening. Prize scams show a noticeable rise mid-year into early Q4, suggesting campaign bursts rather than constant background noise.

Government, delivery, insurance, healthcare, and toll tax remain secondary but persistent. Government scam campaigns spike in Q1, stabilize mid-year, then soften.



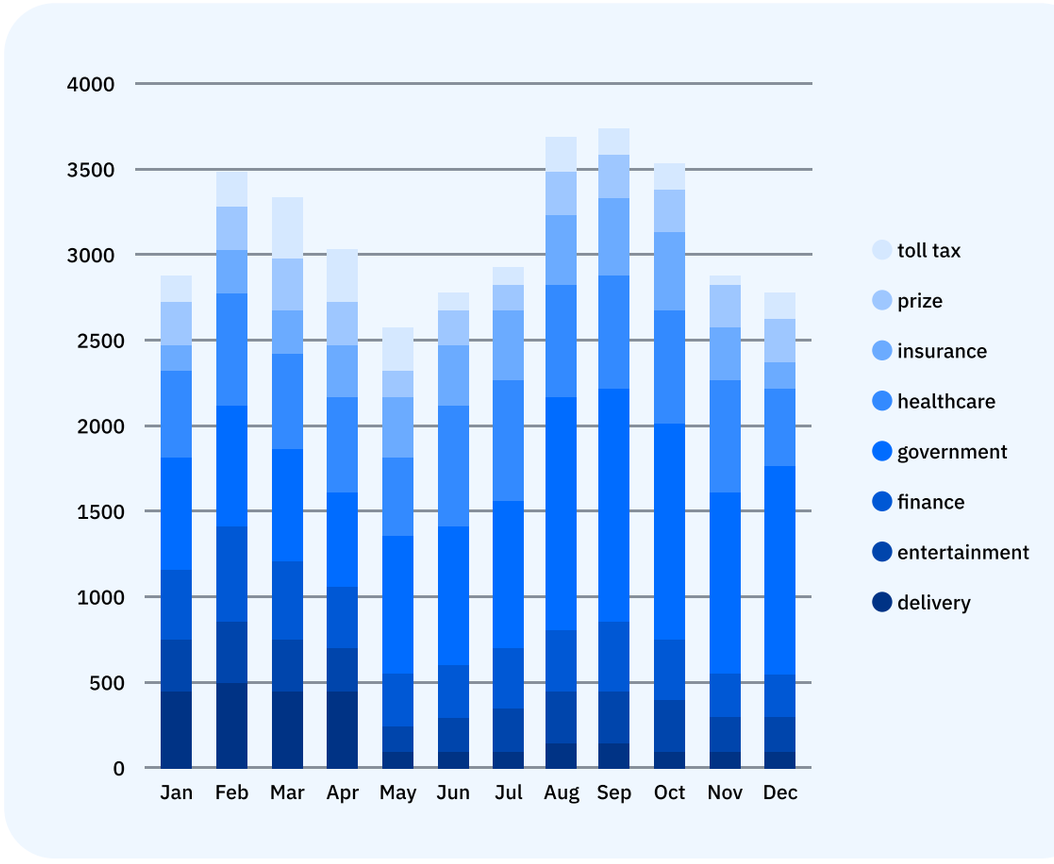
NOTE: This chart shows the number of scam clusters (scam campaign typologies), rather than the number of scams or campaigns

SMS-Based Scams

Regional SMS scams – the USA

In the US, almost 4.5 percent of the short messages received contained a form of riskware.

Finance is the dominant type of scam throughout the entire period driving most of the visible movement in total volume. When overall clusters rise in late summer, finance expands with them. Government and healthcare form a stable second tier, contributing consistently but not driving spikes. Entertainment grows into Q3, while delivery trends downward compared to early months.



NOTE: This chart shows the number of scam clusters (scam campaign typologies), rather than the number of scams or campaigns

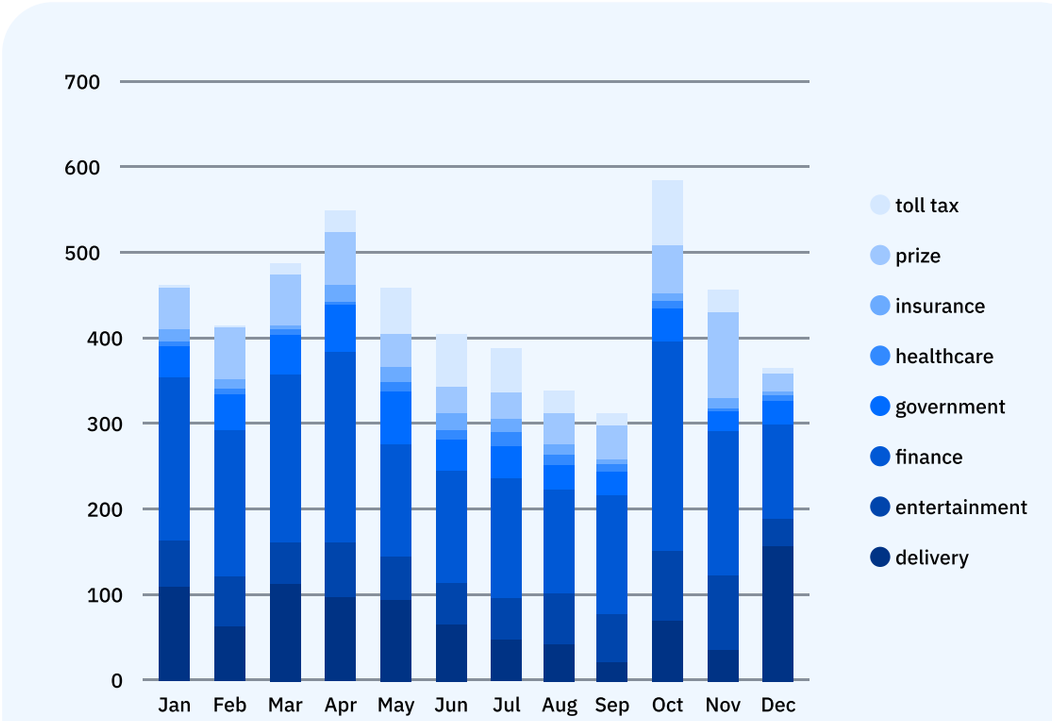
SMS-Based Scams

Regional SMS scams – Canada

Canada shows a different rhythm than the US and UK.

Finance scams dominate across all months and drives most of the spikes, particularly in Q1. Delivery and government contribute steadily but do not dominate. Prize campaigns are episodic and more visible during higher-risk months.

Overall, Canada presents a more cyclical pattern - high Q1 intensity, mid-year suppression, and a Q4 resurgence led primarily by finance.

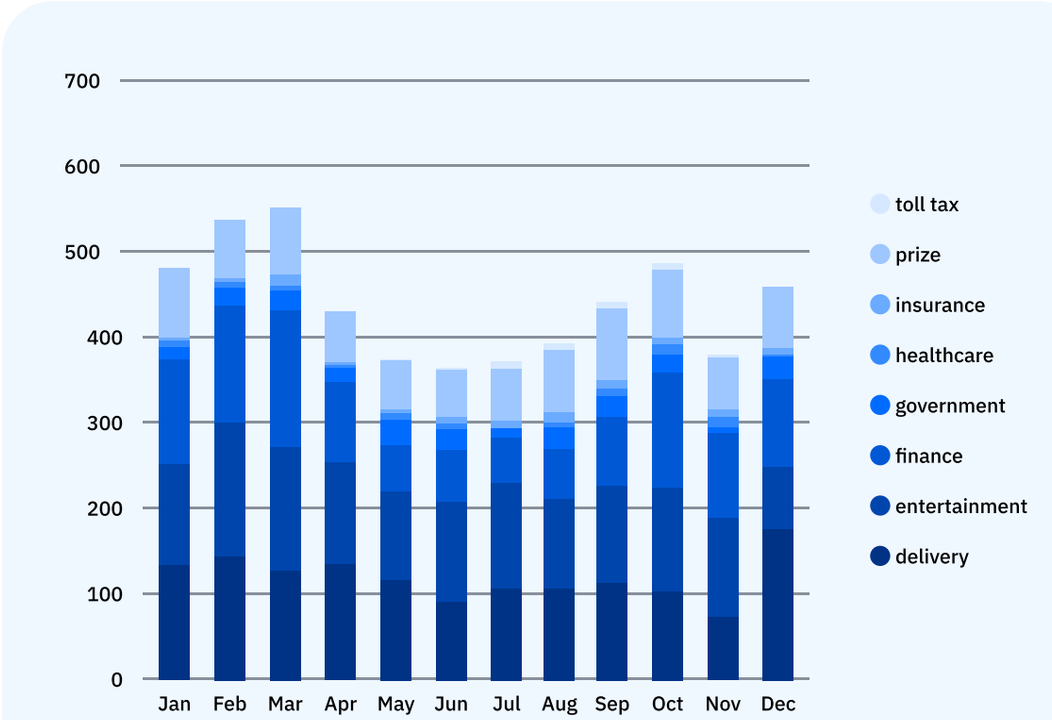


NOTE: This chart shows the number of scam clusters (scam campaign typologies), rather than the number of scams or campaigns

SMS-Based Scams

Regional SMS scams – the United Kingdom

The US, the UK threat mix is more balanced and less dominated by finance than in the US. In Q1, finance, entertainment, and delivery all contribute meaningfully to the peak. As the year progresses, finance becomes less dominant and entertainment maintains a steady presence, while delivery remains consistently relevant across most months. Prize scams fluctuate but do not drive significant spikes. Government, healthcare, insurance, and toll tax remain marginal throughout. Overall, the UK landscape shows a diversification in scam types rather than reliance on a single dominant vertical.

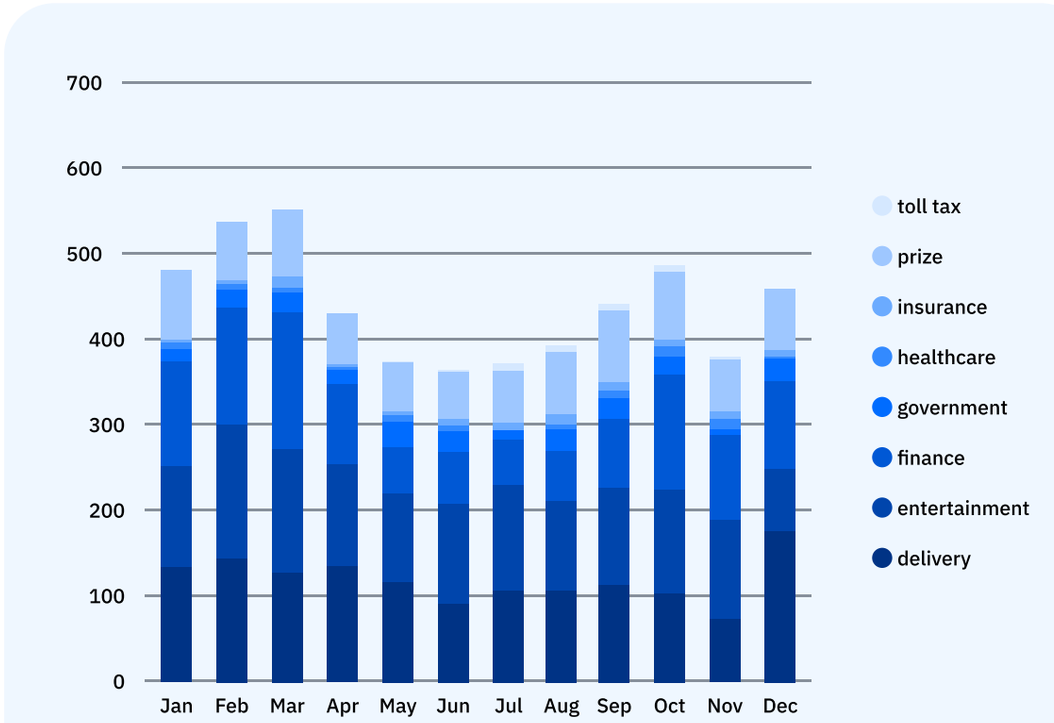


NOTE: This chart shows the number of scam clusters (scam campaign typologies), rather than the number of scams or campaigns

SMS-Based Scams

Regional SMS scams – Australia

In Australia, malicious activity related to prizes is especially strong in March and again in October and November. Finance remains consistently present and expands during rebound months. Entertainment gains relevance in Q3 and stays elevated into Q4, while government fades after early-year prominence. The Australian landscape is concentrated but cyclical, with visible reactivation in the final quarter.

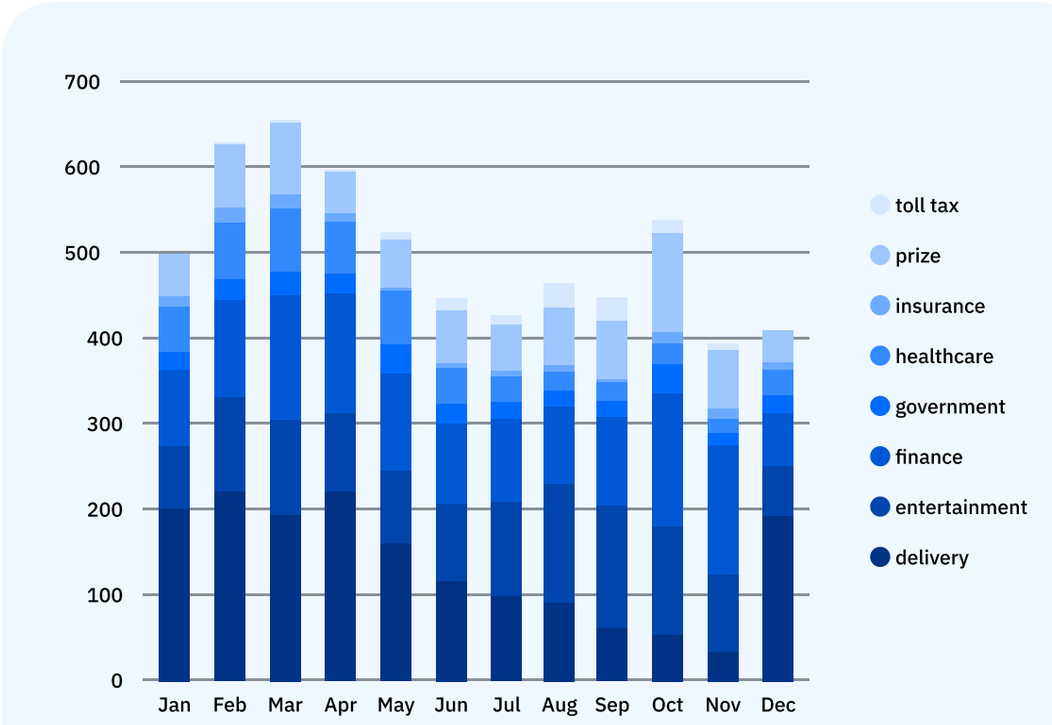


NOTE: This chart shows the number of scam clusters (scam campaign typologies), rather than the number of scams or campaigns

SMS-Based Scams

Regional SMS scams – France

France shows one of the strongest Q1 risk concentrations in our dataset. Risky SMS clusters rise into a February peak, with risk intensity reaching double digits at its highest point. From March onward, both volume and percentage trend downward through summer, bottoming out around August and September. The trajectory is clear - early-year surge, sustained compression, then controlled Q4 reactivation.



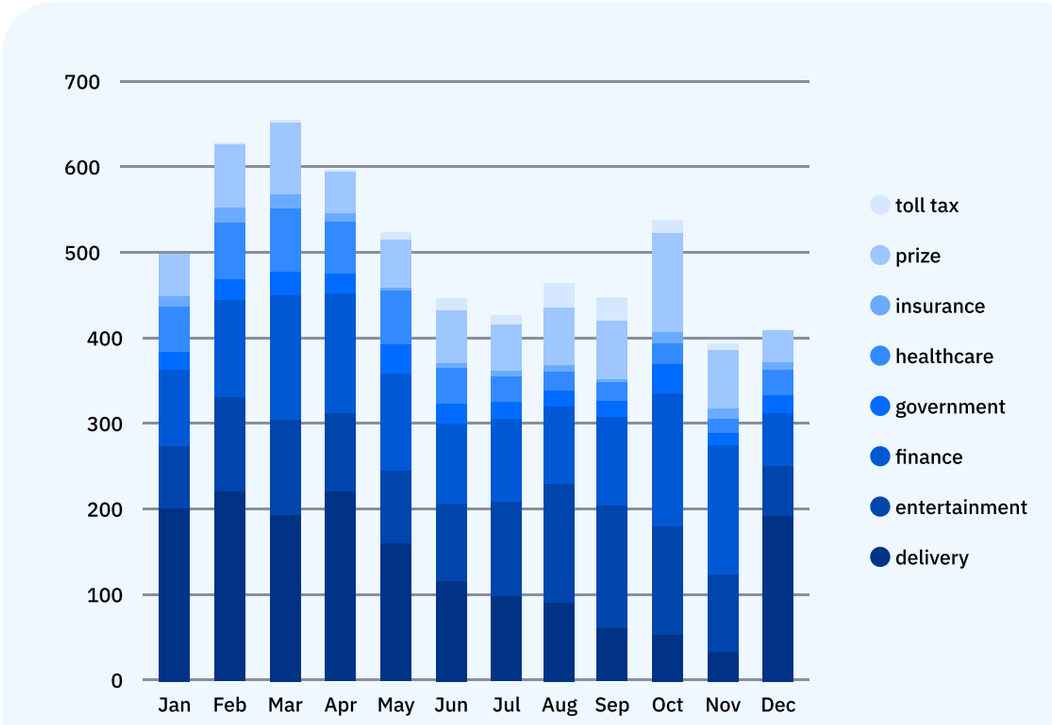
NOTE: This chart shows the number of scam clusters (scam campaign typologies), rather than the number of scams or campaigns

SMS-Based Scams

Regional SMS scams – Germany

German fraud campaigns start extremely high - above 30 percent in Q1 - then declines steadily across the year, reaching 12 percent by November.

Finance is consistently the primary driver, anchoring every monthly peak. Entertainment and delivery form a strong second tier early on, particularly in Q1 and Q2, but delivery weakens notably in late summer and autumn. Prize campaigns gain visibility in the second half of the year, especially October and November, partially compensating for finance softening.



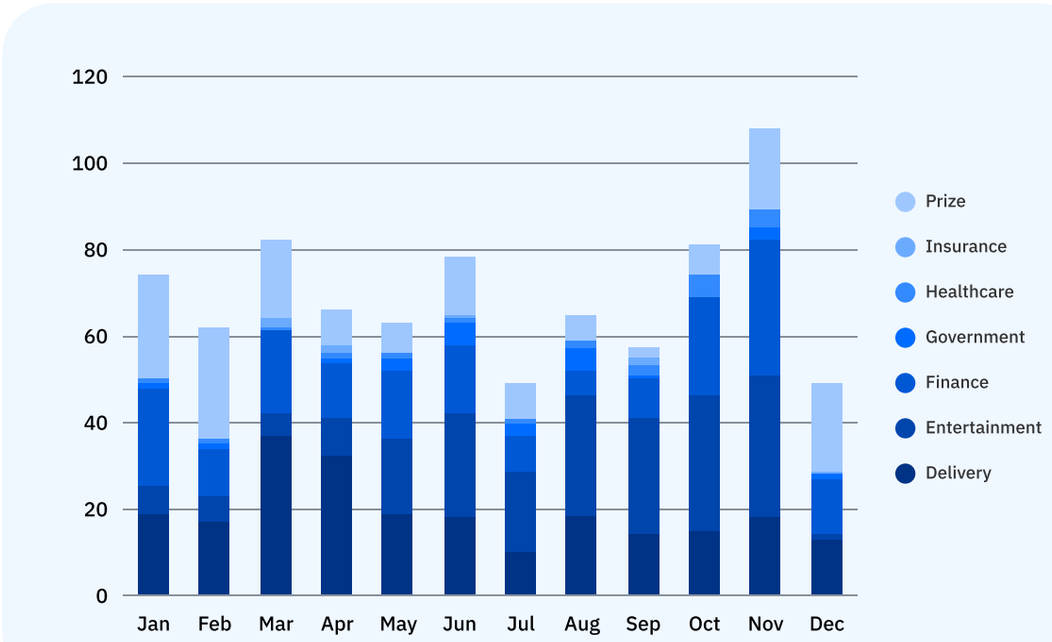
NOTE: This chart shows the number of scam clusters (scam campaign typologies), rather than the number of scams or campaigns

SMS-Based Scams

Regional SMS scams – Romania

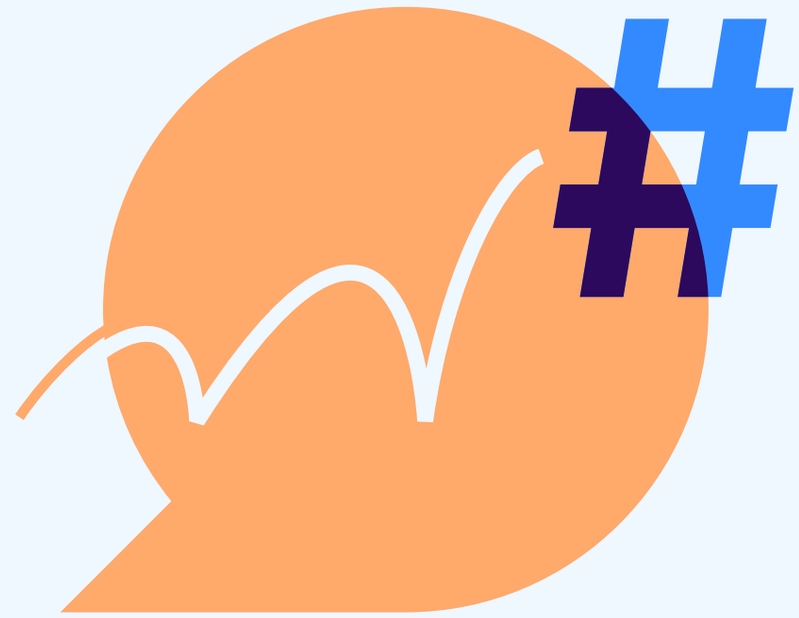
The threat mix in Romania is more fragmented and less dominated by finance than in larger markets. Prize and delivery are consistently present in the first half of the year. Entertainment becomes more prominent mid-year and into autumn.

Finance fluctuates but does not dominate until November, where it grows alongside entertainment. Government, healthcare, and insurance remain marginal. Romania's defining feature is low baseline intensity, summer dilution due to traffic surge, and a visible Q4 reactivation.



NOTE: This chart shows the number of scam clusters (scam campaign typologies), rather than the number of scams or campaigns

Social Media Scams

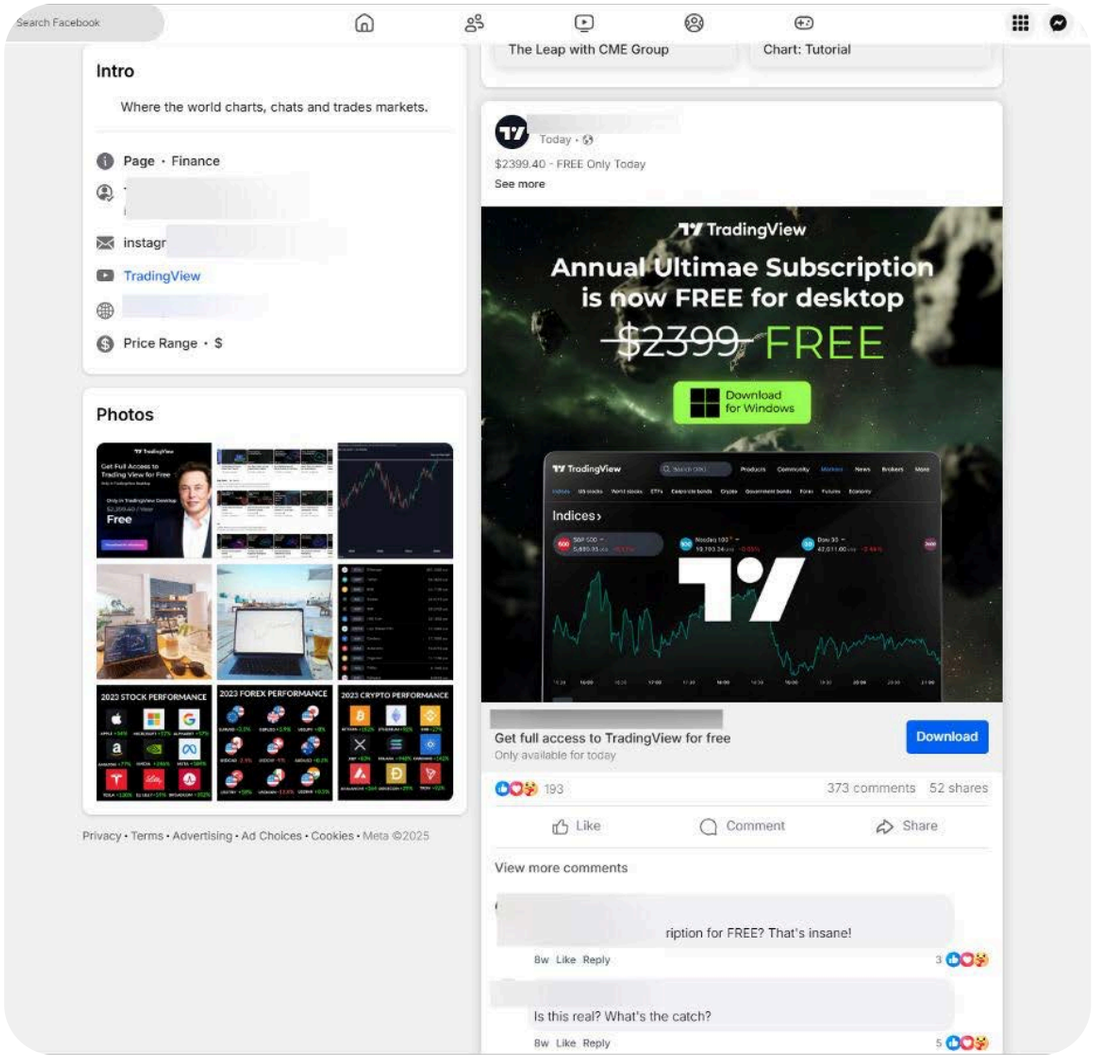


Social Media Scams

The power of social

Social media advertising scams set themselves apart from the rest of the categories by the fact that they don't arrive in the victim's inbox. These lures are delivered via paid advertisements displayed alongside legitimate content on social media.

However, social media ads are supposed to undergo a series of verifications to assess their legitimacy. In reality, a significant number of malicious ads are displayed on the feed, increasing the likelihood that regular users will interact with them, either out of curiosity or by accident.



Social Media Scams

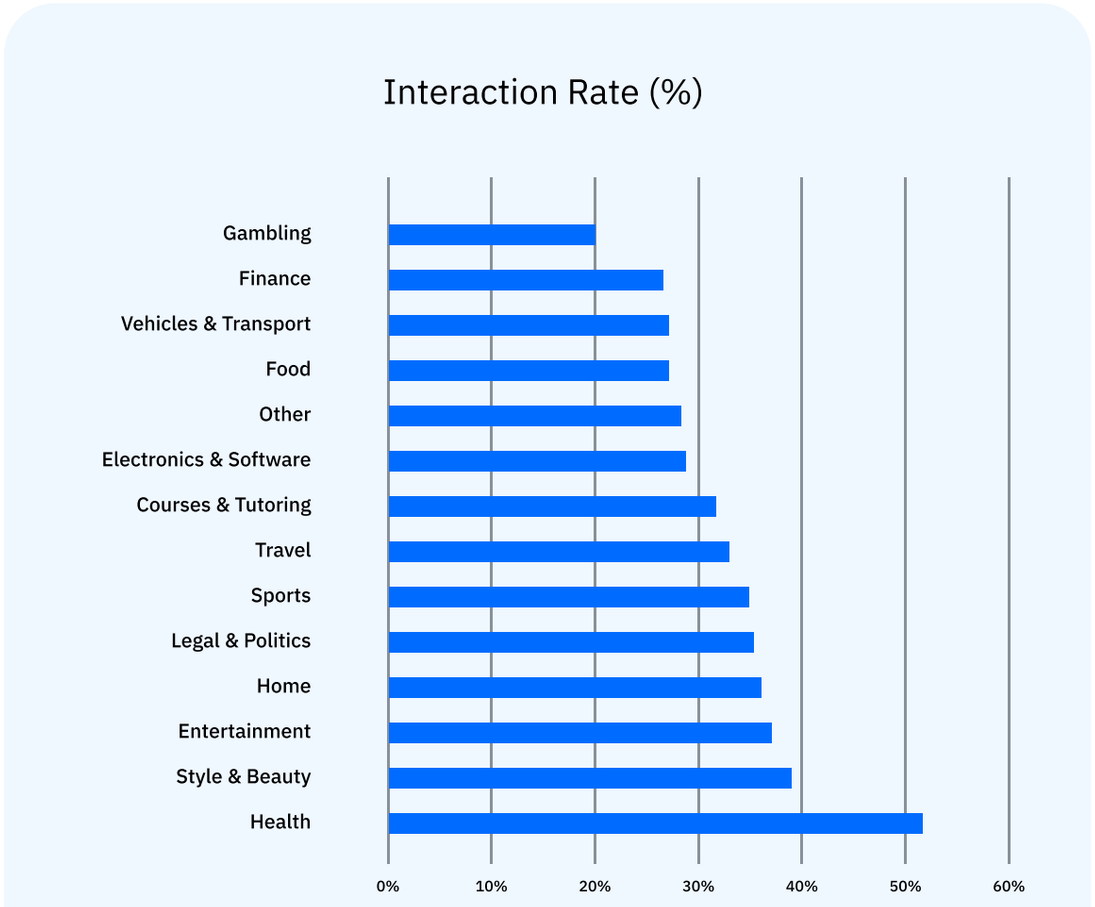
Scam breakdown by category

Our data shows that the overall victim interaction rate with scams was 36%. The top three categories (Health, Style & Beauty and Entertainment) materially outperform the overall average of 36%, indicating significantly stronger engagement with spam messages focused on lifestyle topics.

The impact is measurable at population scale, with tracked exposure rate as follows:

- **18.2 million Americans were exposed.**
- **11.1 million Germans.**
- **8.5 million people in the UK.**

Romania stands out - more than 40 percent of the population saw at least one scam ad.



Social Media Scams

Social industrialization of crypto-malvertising

On April 9, 2025, a single page launched over 100 malicious ads in 24 hours on Meta platforms. Hundreds of coordinated Facebook accounts promoted pages impersonating Binance, TradingView, MetaMask, ByBit, Gate.io, MEXC, and SolFlare.

The ads were localized across Asia, the Middle East, Europe, and Latin America. They used fake endorsements from celebrities, including Elon Musk, Zendaya, and Cristiano Ronaldo.

The technical design is sophisticated. If the landing page detects analysis tools or missing ad-tracking parameters, it serves clean content. Some payloads only activate in Microsoft Edge. The infrastructure includes coordinated front-end and back-end logic designed to bypass security detection.

By August 2025, the campaign expanded to Android, deploying an evolved Brokewell Trojan capable of screen streaming, keystroke logging, 2FA interception, wallet theft, and camera access. At least 75 malicious ads reached tens of thousands of EU users within weeks. Ad abuse has transformed into a viable malware distribution channel through mainstream advertising.

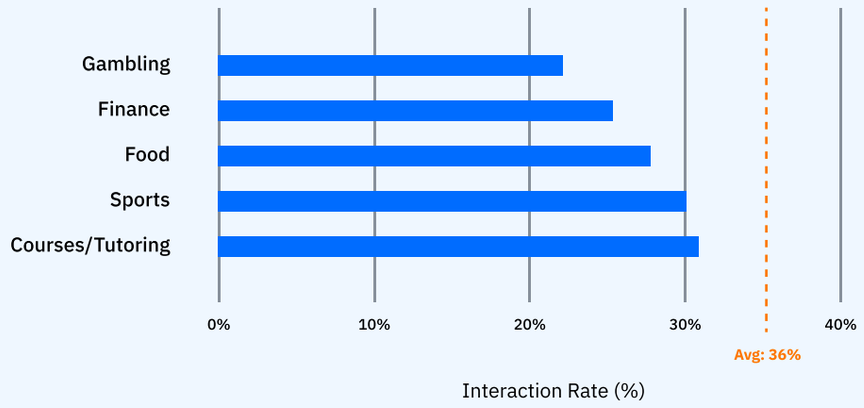
Social Media Scams

Worst performing scam campaigns on social networks

While these categories are, according to our findings, underperforming their previously presented alternatives, they’re not to be underestimated.

Their lower average score indicates a lower incidence of victim interaction and should not be deemed an inherent safety factor.

- Gambling scams exhibit the lowest engagement rate, which could suggest either high user skepticism or platform filtering.
- Finance-themed scams underperform relative to expectations, possibly indicating improved user awareness of financial fraud patterns
- Trust-sensitive categories may trigger greater cognitive caution in recipients



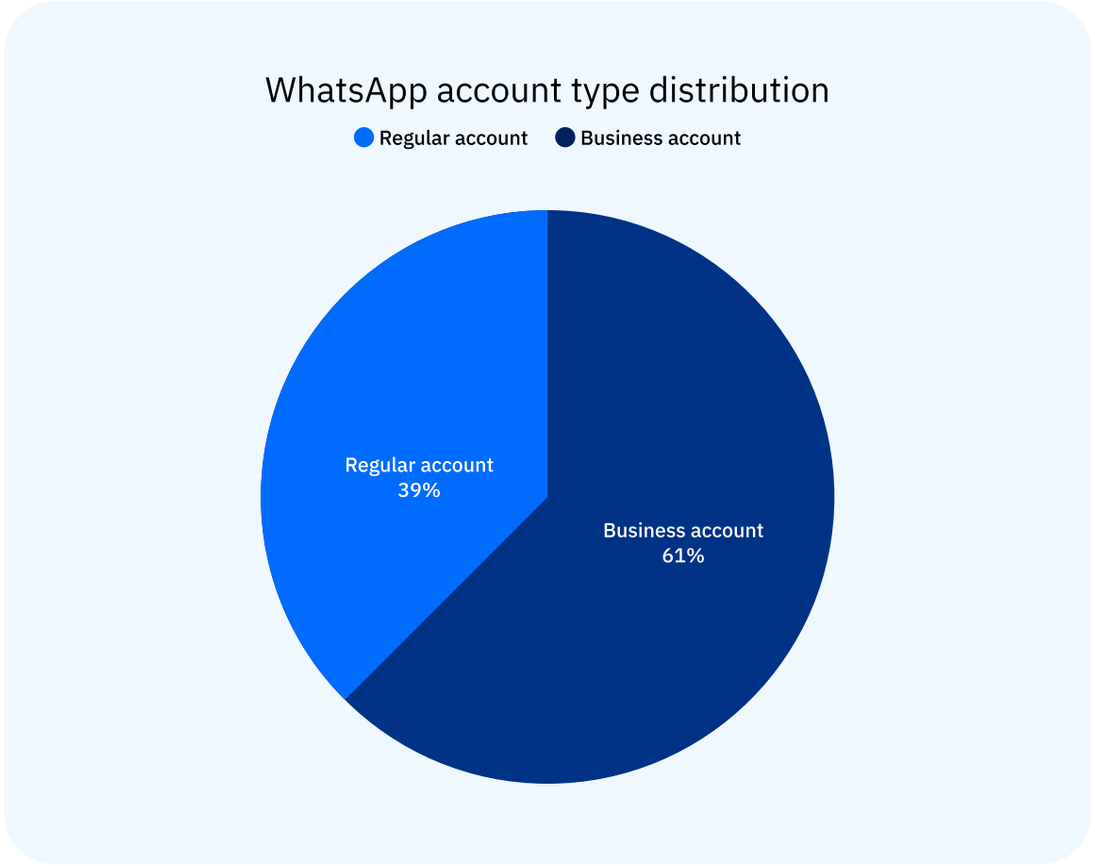
Whatsapp Scams

Whatsapp Scams

An overview of Whatsapp scams

Throughout 2025, a significant portion of scams identified by Bitdefender on Whatsapp originated from business accounts. This approach helps cyber-criminals look like a registered company, display a brand name instead of a random phone number, add a logo, business description, catalog, and sometimes even get verified.

Another important aspect is that WhatsApp Business supports quick replies, automated greetings, labels, and integrations with CRM systems or chatbots. For a scam operation running hundreds of conversations simultaneously, these features dramatically improve efficiency. Scammers can script the first stages of a phishing flow, triage responses, and escalate only high-value targets to human operators in a highly effective weaponized sales funnel.



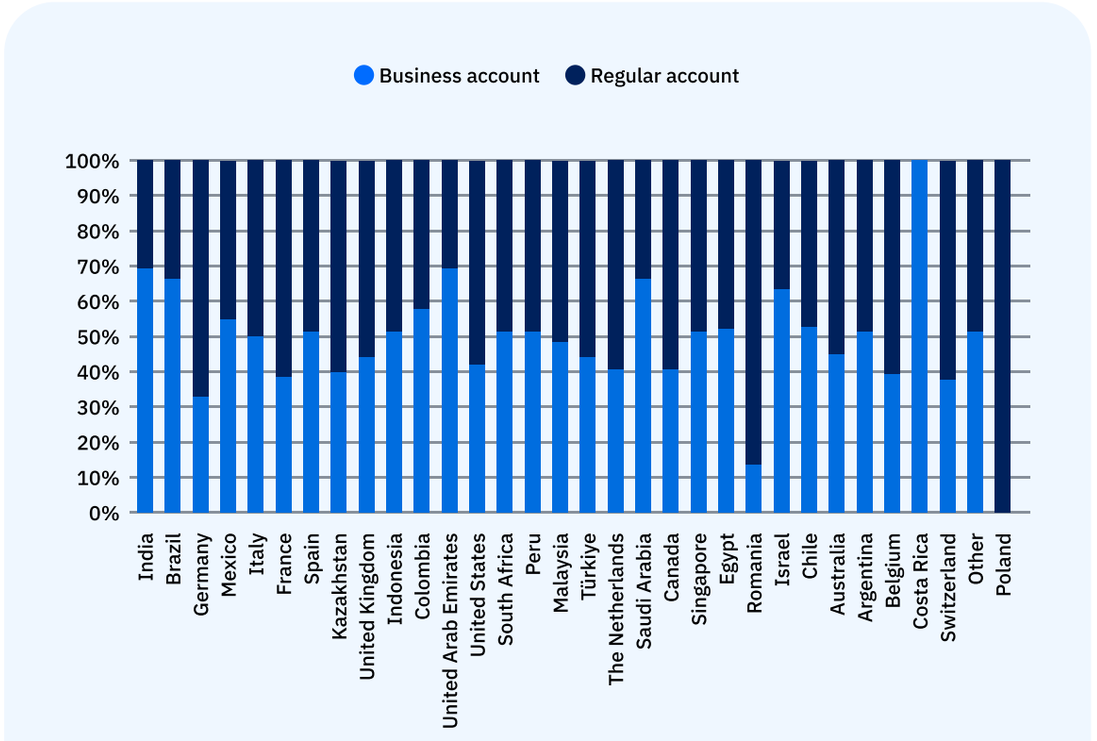
Whatsapp Scams

Distribution of business accounts in scams per country

WhatsApp Business gives scammers what they want most: trust signals, automation tools, and access to users in a channel where commercial communication is normal. It turns a basic messaging app into a scalable social engineering platform.

The use of Whatsapp for Business for scams varies significantly from region to region because WhatsApp plays very different roles depending on the country. In parts of Latin America, India, the Middle East, and Southeast Asia, WhatsApp is the default business channel.

Small retailers, banks, delivery services, even government offices use it as frontline customer support. In those markets, a “business account” is normal infrastructure. In the US or parts of Europe, email, web portals, and native apps still dominate formal communication.



Whatsapp Scams

300k+ risky conversations detected in India alone

Basic characteristics of a Whatsapp scam

There are a few aspects that set WhatsApp scams apart from other scam types, including:

- Peer-to-peer propagation
- Forward-driven amplification
- Account takeover as a catalyst
- Abuse of verified business indicators (blue checkmarks)

Thus, rather than simply relying on the so-called “cold calls,” many campaigns convert victims into distributors, increasing the scams’ effectiveness. After all, victims are more inclined to interact with a message from a contact than with one from a stranger.

Bitdefender

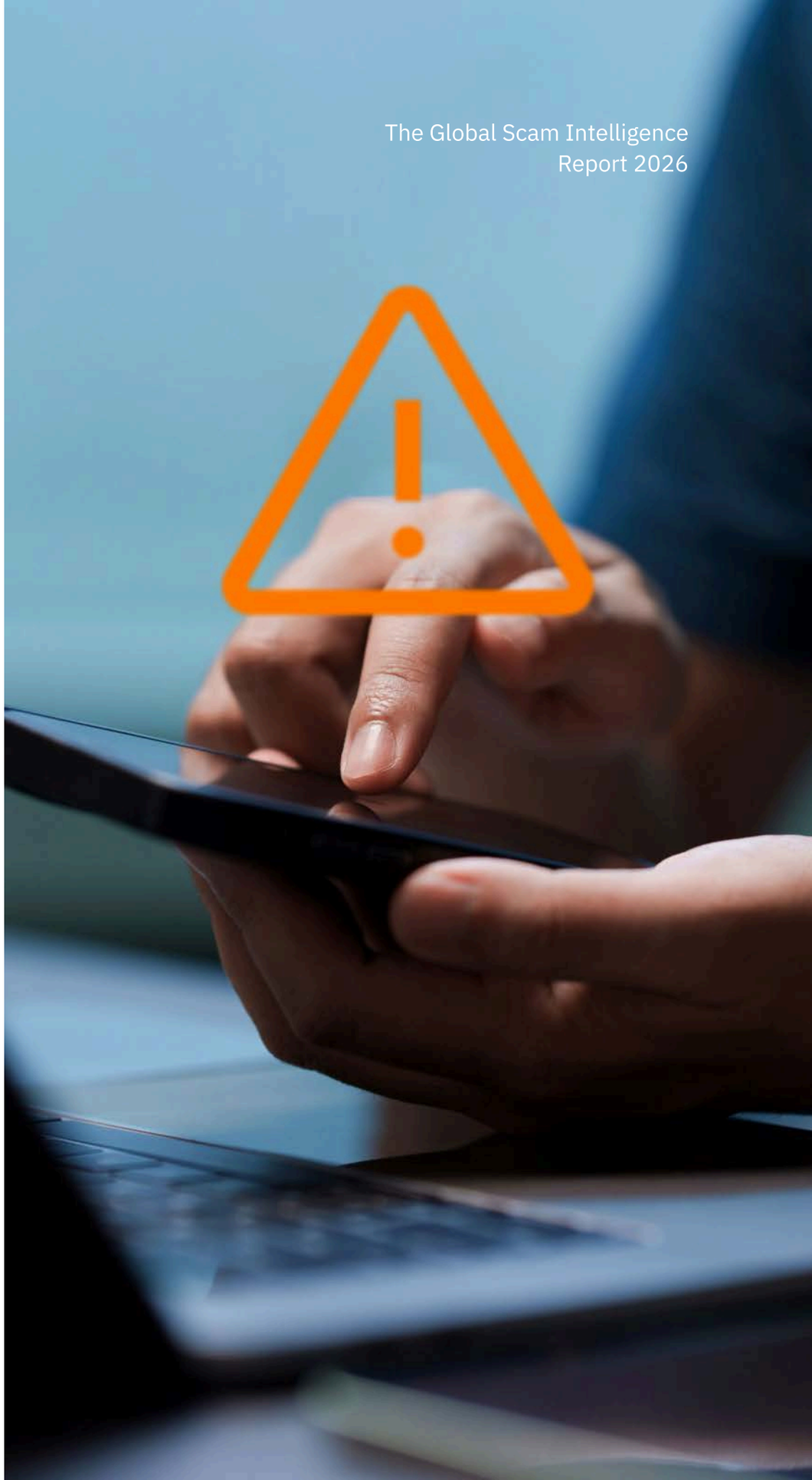
Whatsapp Scams

Whatsapp scam demographics

Encrypted messaging platforms like **WhatsApp present a unique scam surface** that combines high trust and frictionless forwarding, making them highly attractive targets for scammers. Within this environment type, malicious content spreads like wildfire, mainly through social proximity rather than mass broadcast.

During the analyzed period, we detected **over 310,000 risky WhatsApp conversations in India** alone, representing significant regional concentration and activity scaling.

A critical finding was that **60% of risky conversations globally originated from business accounts**. Furthermore, the presence of a blue verification checkmark significantly increased the perceived legitimacy of the account, a trait commonly exploited by threat actors to reduce skepticism and boost engagement from potential victims.



Whatsapp Scams

Case study – the “Vote for me” scam

In this scenario, scammers contact potential victims via WhatsApp, sending links to rogue websites, asking them to vote for their kids in a contest that promises scholarships abroad.

Victims are presented with a professional-looking website, along with photos of young dancers, to strengthen the illusion of legitimacy. In order to vote, visitors need to input their phone numbers and a verification code they receive. However, the code is actually their WhatsApp authorization code, which leads to full account takeovers.

The anatomy of the scam

1. Victims receive a message asking them to vote for a child in a dance competition
2. The message contains a link, encouraging the recipient to access it to vote
3. The link leads to a professionally designed website that prompts visitors to type their phone number to receive a code
4. The website asks visitors to type the verification code to confirm their vote
5. Victims lose access to their accounts, as the code is actually their WhatsApp verification code

Whatsapp Scams

Case study – the Sephora Advent Calendar scam

As its name suggests, this scam uses viral incentive mechanics rather than account takeovers to deceive targets. In this campaign, victims are offered a “free luxury advent calendar” from Sephora.

To claim it, users must forward the message to all WhatsApp contacts (or as many as they can). Some scammers set more realistic thresholds (like sending it to 20 contacts rather than the entire contact list) to strengthen the illusion of legitimacy.

If they take the bait, targets are turned into distributors. The scam spreads through social endorsement rather than impersonation alone.

Thus, victims amplify the campaign unintentionally, while also becoming new targets for additional scam attempts.

Bitdefender

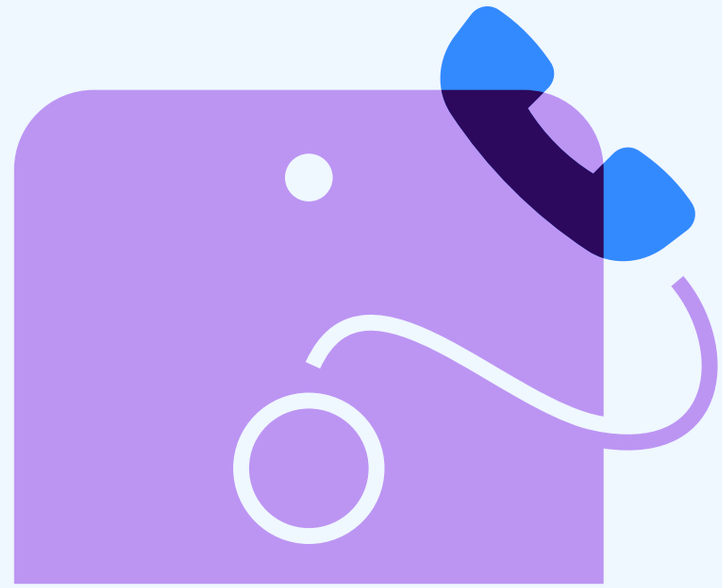
Whatsapp Scams

Additional common Whatsapp scam themes

While prevalent, the Sephora Advent Calendar and “Vote for me” scams are not the only things threat actors can use. Telemetry also shows other recurrent narratives, including:

- Requests for help with projects
- Black Friday promotional offers
- Bitcoin investment opportunities
- Small investment opportunities
- Government or institutional grant claims

Voice Call Scams



Voice Call Scams

Voice call scams – the global context

Voice remains one of the most effective scam-delivery channels. Unlike email or SMS, a phone call creates urgency, emotional pressure, and immediate interaction. It allows attackers to adapt in real time, escalate persuasion, and overcome skepticism through social engineering.

The ecosystem is industrialized. Robocall infrastructure handles scale, local spoofing builds credibility, and human operators take over once a victim engages. The model blends automation and manual exploitation. It is low cost, high yield, and difficult to attribute across borders. Voice call scams rely on structured call center operations - desks, headsets, scripts, supervisors, KPIs and shift rotations.

The model mirrors legitimate outbound sales or support centers, except the product is fraud. Leads are generated through robocalls or data leaks, callers follow scripted social engineering flows, and successful transfers are escalated to “closers” trained to extract credentials, remote access, or direct payments. The reason voice scams remain effective is sheer industrialization. Division of labor, performance tracking, and constant script optimization turn deception into a repeatable process.

Our telemetry shows that scam calling is not a marginal phenomenon. It is systematic, persistent, and heavily domestic in origin. It peaks during business hours, mimics legitimate brands, and increasingly uses scripted flows optimized to keep victims on the line long enough to extract data or money.

Voice Call Scams

Scam centers in Europe vs USA

There are documented cases across Europe and the Americas. In 2022 and 2023, Spanish and Portuguese authorities dismantled large investment fraud call centers operating from Madrid and Barcelona that targeted victims across the EU, seizing assets worth millions of euros.

In 2023, German law enforcement coordinated raids against boiler-room style crypto investment call centers operating in Berlin and other cities, arresting operators who had defrauded victims throughout Europe.

In the United States, federal prosecutors have repeatedly taken down tech support and IRS impersonation call center networks with operational hubs in states such as Florida, Texas, and New York, often tied to international partners but with domestic infrastructure handling victim interaction and money flows.

In late 2024, 24 suspects were detained in Chișinău for running several call centers suspected of using deepfakes to scam victims. Scammers were using deepfakes of politicians, businesspeople and journalists to persuade victims to “invest” into non-existing companies. When hiring new staff, call center HR would have candidates take a lie detector test to screen potential undercover law enforcement officers.

These were not isolated scammers, but rather organized teams running structured fraud businesses with payroll, management, and performance metrics.

Voice Call Scams

The scale of the problem

Throughout 2025, we analyzed nearly 150 million incoming calls. Out of these, more than 23 million were classified as unwanted - this is more than 15 percent of all incoming calls received globally.

This means roughly 1 in 6 incoming calls reaching protected devices was unwanted.

The system processed calls from 52+ million unique phone numbers, of which more than half a million were identified as unwanted numbers

The key takeaway is that the problem is shifting from volume to diversity. Over half a million distinct unwanted numbers were active in a single year.

150 M
incoming calls analyzed

52 M
unique numbers

23.5 M
unwanted calls

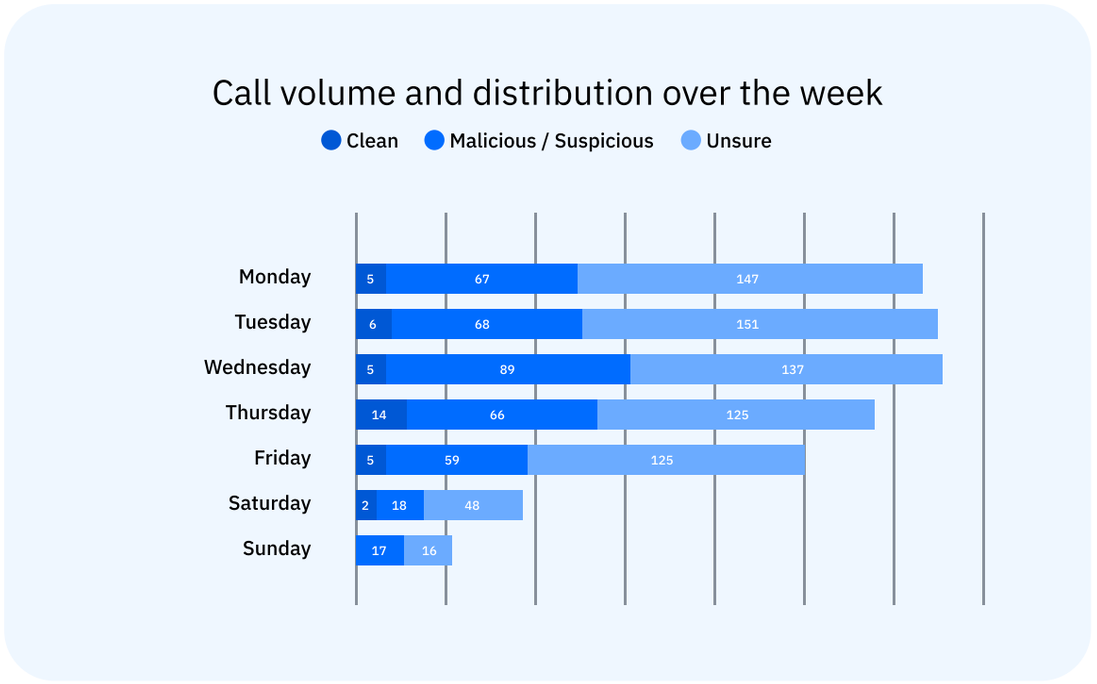
550 K
unwanted numbers

Voice Call Scams

Honeypot evidence: what happens in the wild

Bitdefender also runs a massive honeypot infrastructure with well-defined online personas. Powered by artificial intelligence algorithms with agentic capabilities, they engage in conversations with scammers, receive e-mail and indistinguishably mimic a human victim.

We use the insights we gain to perfect our understanding of scams and to collect artifacts as soon as these scams happen. As a bonus, we keep scammers engaged in conversations with our robots to limit their outreach capabilities – the more they speak with our AI agents, the less time they have to focus on your family.



Voice Call Scams

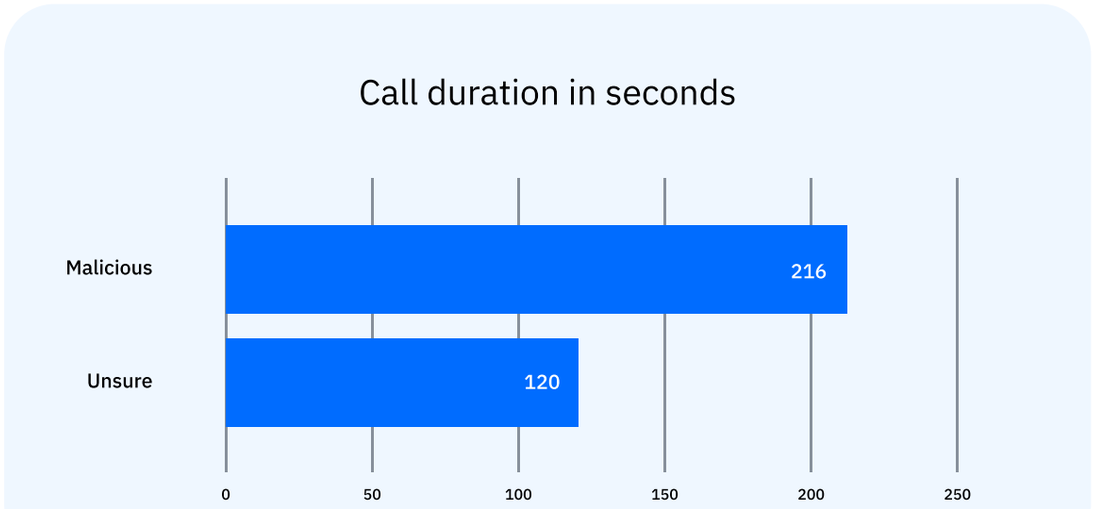
Duration patterns: how long scammers need

US honeypot data on calls longer than 30 seconds shows that “malicious” calls stretch on average for 3:36 minutes with a median of 2:30 minutes, while ”grey” calls average 2 minutes with a median of one.

Longer calls correlate strongly with malicious intent. Once a scammer senses engagement, the call extends. By category, phishing calls are the longest, with a mean duration of 8 minutes and 8 seconds .

Shorter scam types such as compensation scams average around 1 minute 27 seconds.

Complex frauds require narrative building. The more elaborate the scheme, the longer the engagement.



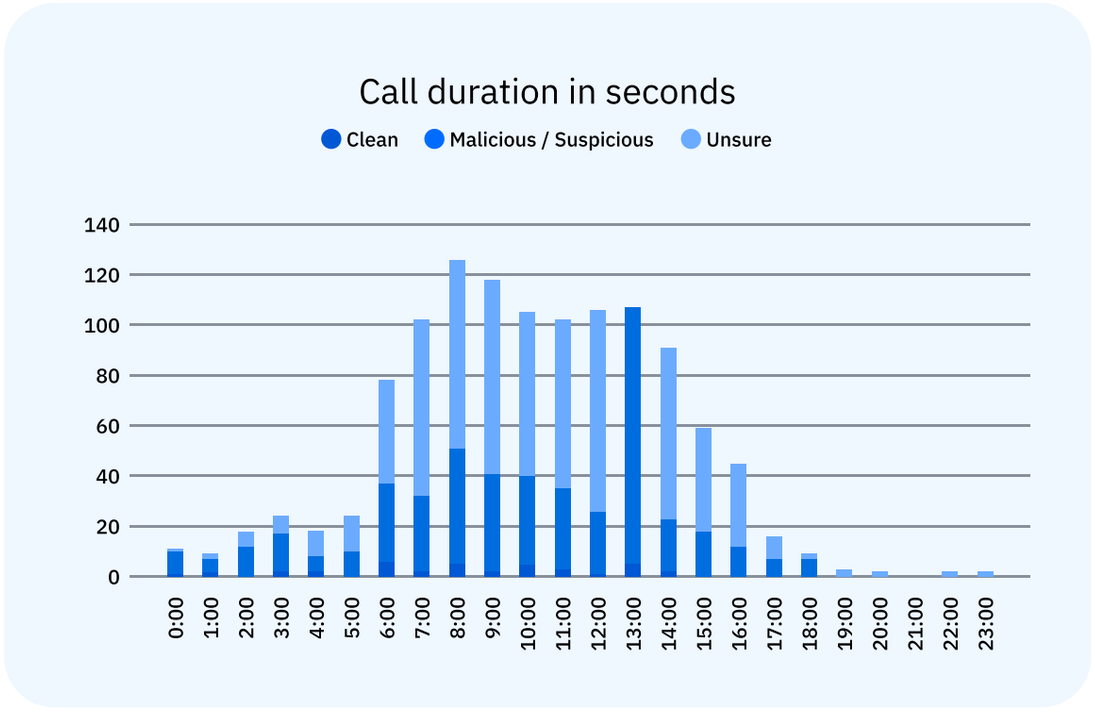
Voice Call Scams

Temporal patterns: when are scammers at work?

The US honeypot data also reveals an important aspect: out of 1,700+ calls analyzed, peak activity occurs roughly around 8 AM. For calls longer than 30 seconds, our data shows that “malicious” calls stretch on average for 3:36 minutes, while ”grey” calls average 2 minutes.

Longer calls correlate strongly with malicious intent. Once a scammer senses engagement, the call extends. By category, phishing calls are the longest, with a mean duration of 8 minutes and 8 seconds. Shorter scams such as compensation scams average around 1 minute 27 seconds.

Complex frauds require narrative building. The more elaborate the scheme, the longer the engagement.

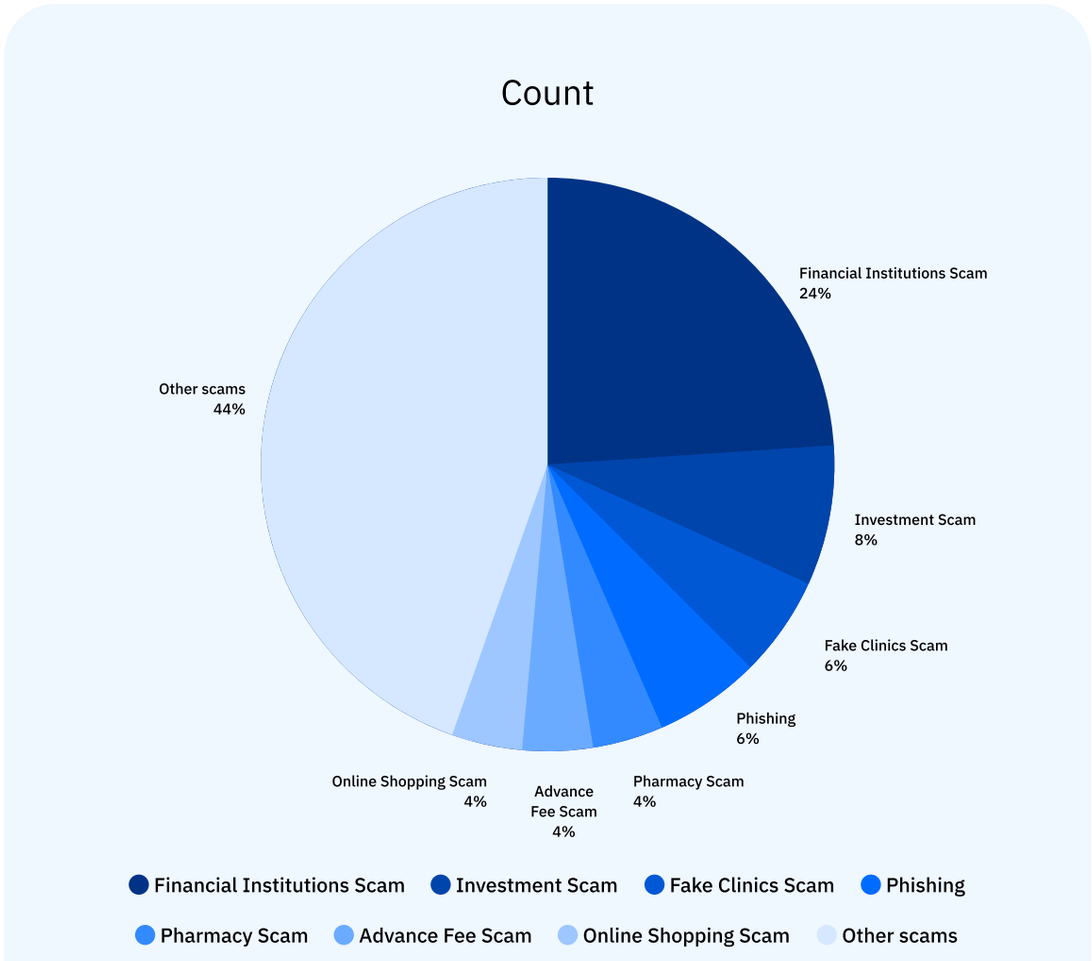


Voice Call Scams

What phone scammers pretend to be

The distribution shows a clear concentration of scam activity around financial exploitation themes. Financial Institutions alone account for roughly a quarter of all calls.

When combined with “Investments and Crypto” and “Commerce and Refund” fraud, the data shows that direct monetary extraction remains the dominant objective. These schemes rely on urgency, authority impersonation, or transactional pretexts to trigger fast financial decisions. The clustering around money-related narratives is not random. It reflects what consistently converts at scale.



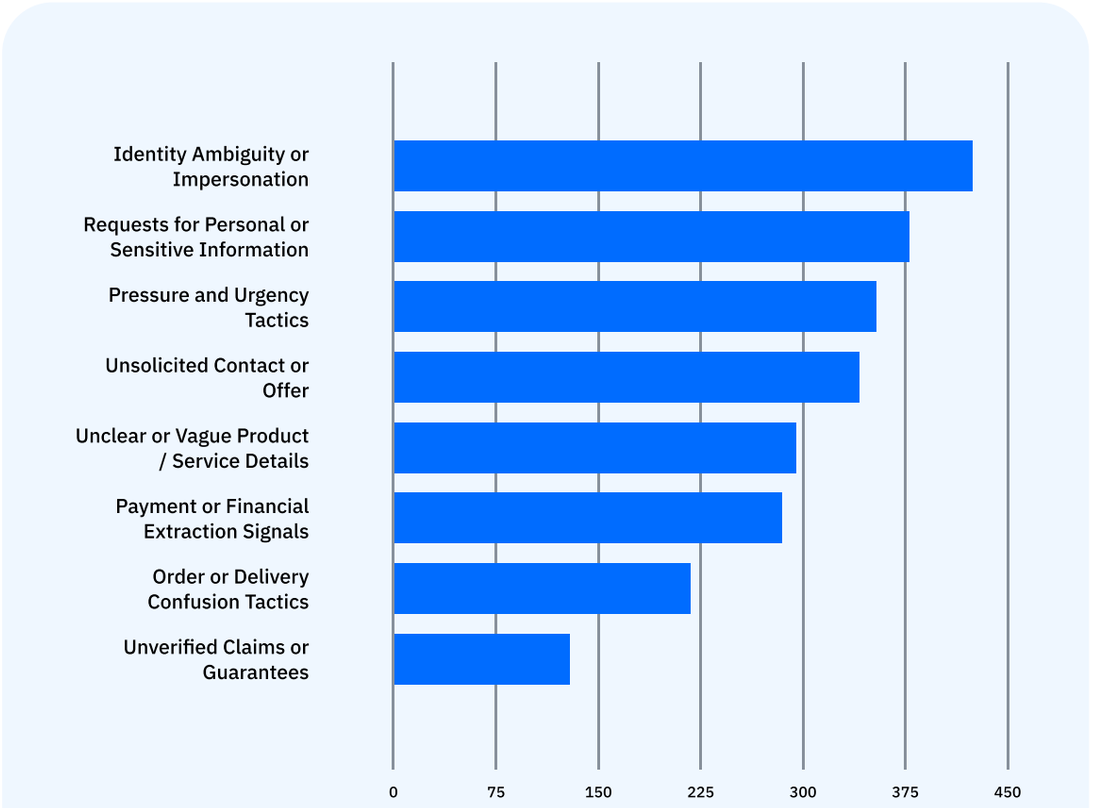
Voice Call Scams

Red flags and behavioral signals

Most scam calls follow the same predictable playbook. The biggest warning sign is unclear identity - if the caller cannot clearly state who they are and why they are calling, that is a red flag. The next common pattern is a request for personal, financial, or medical information during an unsolicited call.

Pressure and urgency are also major indicators, especially when the caller insists you act immediately. Many scams begin with unsolicited offers or references to orders, benefits, or investments you never requested. Vague product details and unclear explanations are tactics designed to create confusion.

If identity is unclear, information is requested, and urgency is applied, assume malicious intent and disengage.



Preventing Scams

Bitdefender

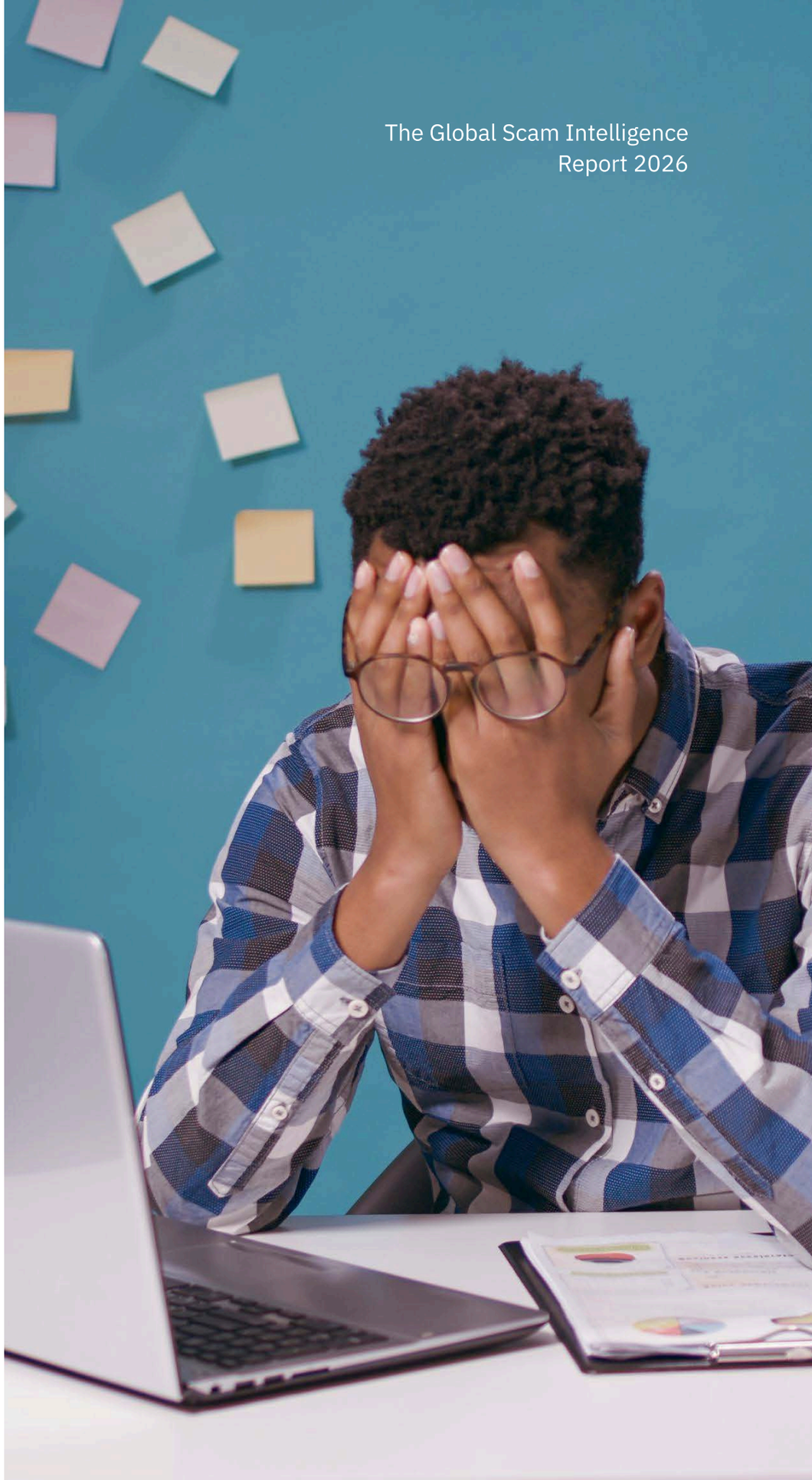
Preventing Scams

How to avoid scams

Scams work because they trigger urgency, fear, greed or curiosity. If a message pushes you to act immediately, step back. Real companies and state institutions do not demand instant decisions under threat. Never share passwords, one-time codes, PINs or recovery phrases with anyone, under any circumstances.

If someone asks for payment in gift cards, crypto, wire transfers or “processing fees,” you are dealing with a scam.

Verify requests using a second channel - call the official number on the company’s website, not the number provided in the message. Treat unexpected contact as hostile unless proven otherwise.



Bitdefender

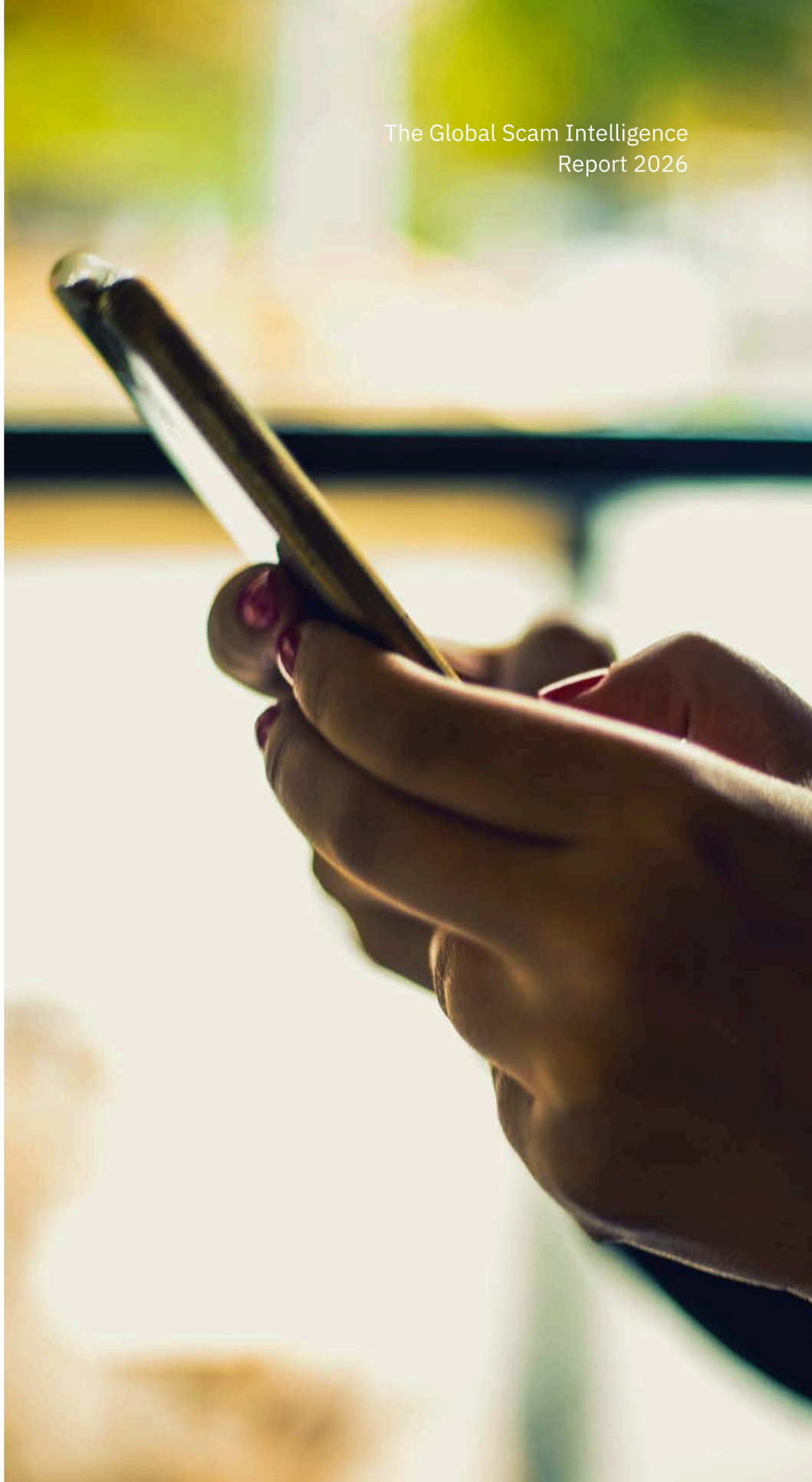
Preventing Scams

Phone calls, messaging and SMS

Do not trust caller ID. Numbers can be spoofed, including those of banks and government agencies. If a caller claims to be from your bank, hang up and dial the number printed on your bank card.

Never install remote access software because a caller tells you to. Legitimate support does not cold-call you to fix “viruses.” Be skeptical of WhatsApp or Telegram messages from “business accounts” offering investments, prizes or urgent deliveries.

Disable automatic SMS link previews if your device allows it, and do not click links in unexpected delivery or tax messages.



Bitdefender

Preventing Scams

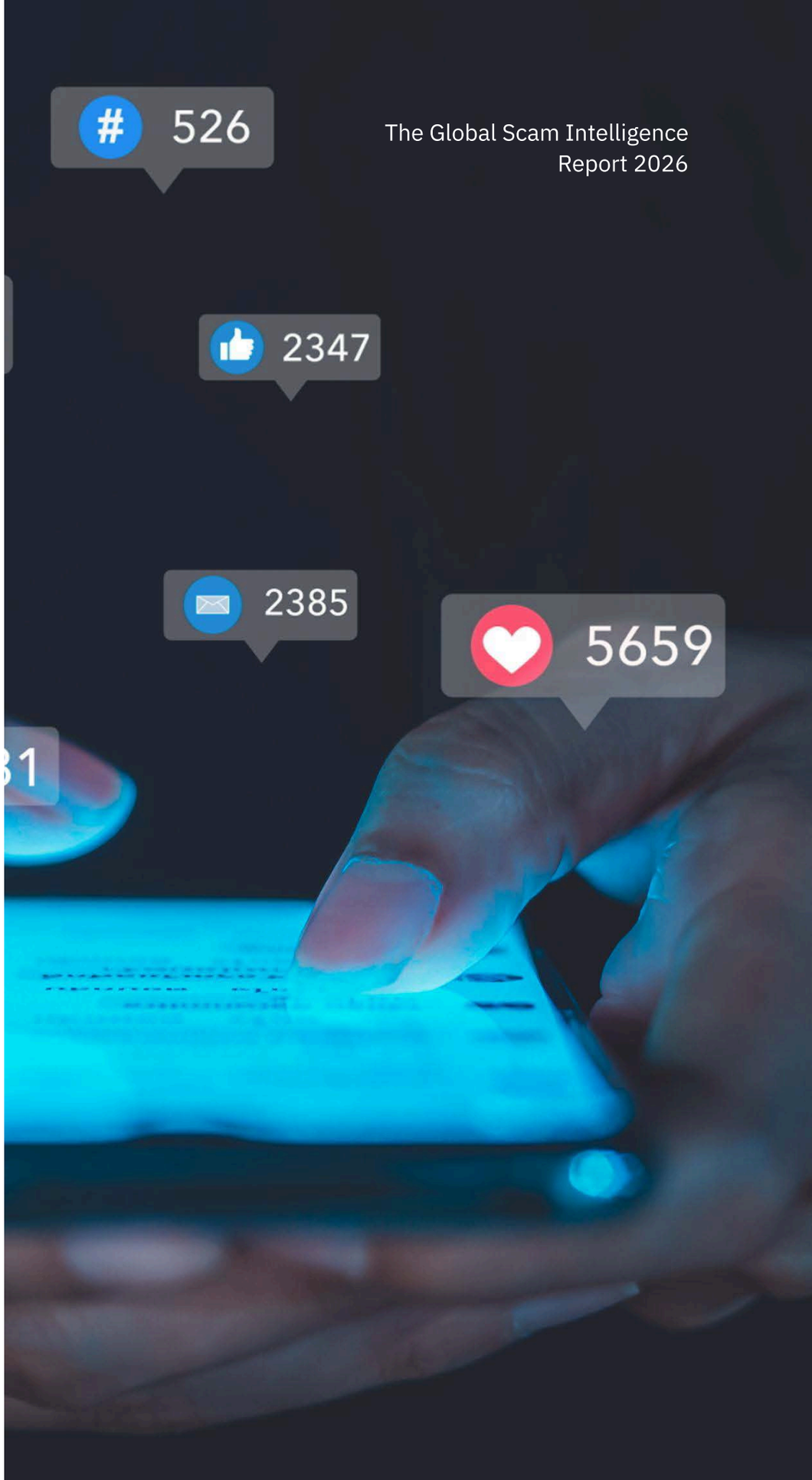
Email, social media and online ads

Scams can now appear as paid ads and promoted posts, not just spam emails. Do not assume that a verified badge or sponsored label means it’s safe.

Before entering credentials, check the domain name carefully - attackers rely on lookalike domains.

Use multi-factor authentication on email, social media and banking accounts, ideally with an authenticator app instead of SMS. Keep devices updated and use reputable security software that blocks malicious links and scam domains.

Finally, talk about scams with family members - especially teenagers and older relatives - because awareness spreads faster than fraud when people compare notes.



Bitdefender

Preventing Scams

Technology as a force multiplier

Scam operations are industrialized. They use automation, AI-generated content, spoofed infrastructure and paid advertising to scale attacks across millions of targets. Consumers cannot realistically manually analyze every call, link, message and ad manually.

Technology helps level the field. It applies real-time threat intelligence, behavioral analysis and reputation scoring at machine speed, blocking malicious content before a user has to make a decision. Instead of reacting after the damage is done, protection shifts left - preventing exposure in the first place.

Bitdefender

Preventing Scams

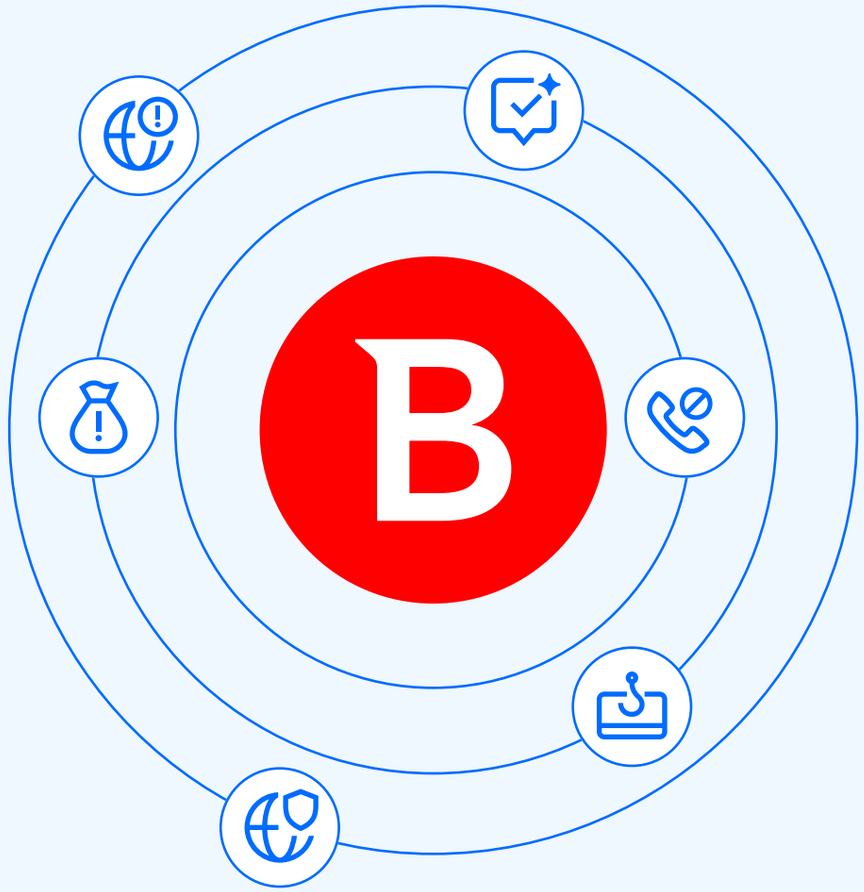
How Bitdefender can help

Our protection layers address scams at multiple control points. **Online Threat Prevention** inspects and blocks malicious URLs and exploit attempts at the network level, regardless of how the link was delivered - email, SMS, messaging apps or social media.

Anti-Phishing and **Anti-Fraud** engines analyze web page structure, domain age, impersonation patterns and behavioral indicators to stop credential harvesting and payment fraud.

Scamio provides AI-assisted scam validation, allowing users to submit suspicious messages, screenshots or links, then receive rapid, intelligence-backed risk assessments.

On mobile, **Call Blocking** and scam-detection features flag or suppress known fraudulent numbers, while **Web Protection** monitors browsing sessions to prevent redirection to malicious domains.



I. General Disclaimer Regarding the Nature and Purpose of the Report

This report serves an exclusively informational and educational purpose. It does not constitute and does not replace legal, financial, investment, or any other form of professional advice. The information contained in this document reflects how Bitdefender has analyzed and interpreted its own technical data (telemetry) and should not be treated as absolute truths or as a complete picture of digital scams worldwide.

The report is published in good faith, to raise awareness of online threats and to contribute to a safer digital environment. Bitdefender does not warrant that the information is accurate, complete, or up to date, and assumes no responsibility for decisions that readers may make based on this report.

II. Disclaimer Regarding Methodology and Data Limitations

The data in this report originates from Bitdefender's proprietary systems (telemetry), collected between January 1 and December 31, 2025, through the company's products and services. They reflect only what Bitdefender was able to observe through its own infrastructure and do not represent a complete picture or an official statistic of digital scams at the global, regional, or national level.

Estimates and projections are based on internal analytical models, which may have limitations — for example, incomplete samples, selection bias, or variations over time. The figures and percentages in the report should be read as indicative markers, not as exact measurements.

When we classify messages, links, calls, or advertisements as "risky," "malicious," or "fraudulent," we do so based on automated technical criteria. This does not mean that they automatically constitute criminal offenses or regulatory violations from a legal standpoint — only judicial and regulatory authorities can make such a determination.

III. Disclaimer Regarding Personal Data Protection

Bitdefender processes the analyzed data in compliance with the European data protection regulation (GDPR — Regulation (EU) 2016/679), applicable national legislation, and internal privacy policies. All data presented in the report is aggregated and anonymized — in other words, no individual can be identified based on the published information.

IV. Disclaimer Regarding Third Parties Mentioned in the Report

When we mention platforms, companies, brands, public figures, or authorities in this report, we do so solely to describe and document the scam phenomenon from a cybersecurity perspective. We do not accuse or suggest that these entities have violated the law or bear any fault.

Where the report describes fraudulent campaigns that misuse the name, logo, or image of brands, platforms, or public figures, we emphasize that these entities and individuals are themselves victims of scammers who have stolen their identity. The fact that we mention them in the report does not mean that we consider them involved, complicit, or negligent in connection with the frauds described.

All trademarks, trade names, and logos mentioned belong to their respective owners and are used solely for identification and reference purposes

V. Disclaimer Regarding Statements Related to Law Enforcement Actions

Information about the operations of authorities in various countries (including Cambodia, Myanmar, Spain, Germany, the Republic of Moldova, and the USA) originates from public sources: official reports, press releases, and journalistic articles. Bitdefender has not independently verified the accuracy or completeness of this information and does not express opinions on the legality, proportionality, or effectiveness of the respective authorities' actions.

VI. Disclaimer Regarding Limitation of Liability

To the maximum extent permitted by law, Bitdefender, its affiliated companies, directors, employees, and collaborators shall not be liable for any damages — direct or indirect, foreseeable or unforeseeable — that may result from the use, interpretation, or inability to use the information contained in this report. This limitation applies regardless of the legal basis invoked (contract, tort, strict liability, or any other ground).

VII. Disclaimer Regarding Governing Law and Jurisdiction

This report and any disputes related to its content are governed by Romanian law. Any litigation shall be resolved exclusively by the courts of Bucharest, Romania, subject to any applicable mandatory rules of private international law.

VIII. Disclaimer Regarding Updates and Validity of Information

The information in this report is valid as of the date of publication and reflects what was known at that time. Bitdefender is under no obligation to update, revise, or correct the report after publication. Cybersecurity threats evolve rapidly, and the data presented herein may become outdated or inaccurate over time.

Bitdefender is a **Global Leader in Cybersecurity**

Protecting millions of consumer and business environments since 2001

We take pride in our Telco-oriented solutions that include Value-Added Services, Core Network Security and Management & Intelligence Platforms, as well as the partnerships we established with some of the biggest Service Providers in the world.

HEADQUARTERS

Bucharest, Romania
Fort Lauderdale, Florida

CONTINUED INNOVATION

540+ patents

WORLDWIDE OFFICES

Europe & US HQs
17 regional offices across US, Europe, Asia and Australia

EMPLOYEES

2100+
More than half of Bitdefender's employees are security researchers and engineers

PARTNERS

35,000+ qualified partners and resellers
Distributed through partners in 170 countries