



# The Great Messaging Heist

---

Exposing  
the global  
scam cartels  
exploiting  
everyday  
messages

2026



# Contents

- The essence ..... 3
- Chapter 1 – Where trust lives ..... 4
- Chapter 2 – Speed beats scrutiny ..... 6
- Chapter 3 – The aftermath..... 8
- Chapter 4 – Collateral damage ..... 10
- Chapter 5 – The accelerant..... 12
- The wake-up call ..... 14
- Start protecting yourself now..... 15
- Methodology..... 17
- About..... 17

# The essence

It starts with the familiar.

A short message. A trusted name. A tone that sounds and feels routine.

Delivery updates, work notifications and brand alerts blend into the background noise of everyday digital life, rarely attracting scrutiny.

You check. You reply. You think nothing of it. Minutes later, you've unknowingly been drawn into a carefully constructed scam designed to disarm suspicion and exploit your trust.

This is what makes messaging scams so effective and dangerous. They prey on ordinary behaviors in everyday contexts, where instinct kicks in.

Communication didn't always feel this automatic. Letters, memos, and even the first emails were slow, took time and created space for doubt. Now messages are part of everyday life, rarely scrutinized, a shift that cybercriminals are actively weaponizing.

## The first investigation of its kind

Despite the scale of the problem, much of the public conversation focuses on how often scams happen, not what actually happens once a scam message lands.

For the first time, Kaspersky has set out to capture the full end-to-end reality of messaging-based scams to understand how quickly harm occurs, how they impact trust and what remains after the interaction ends. In doing so, the research reveals a scale and depth of harm that no government or regulator has yet fully quantified.

What emerges is a highly organized and industrialized scam ecosystem embedded within everyday messaging channels such as SMS, WhatsApp and email. These scam cartels deliberately mimic the rhythms of regular communication, using familiar tactics to siphon money and personal information while inflicting long-lasting emotional harm.

Kaspersky's data shows that more than half of successful messaging scams unfold within 30 minutes, with an average loss of \$733 per victim. When scaled across millions of "micro-losses" worldwide, the financial damage is in the billions. But financial loss is only part of what's taken. The emotional impact is immediate, intense and long-lasting, reshaping victims' relationship with digital communication long after the scam itself ends. The consequences also extend beyond individuals. By convincingly replicating brand identities and using AI to scale attacks, scammers blur the line between legitimate and fraudulent communications. Messages that once conveyed authority and reassurance now inspire doubt.

This research exposes a clear and disturbing pattern. No demographic is immune. From Gen Z to Gen X, messaging scams cut across every generation. Being "tech-savvy" is no longer a meaningful defense. The tactics employed by scam groups have evolved in lockstep with the platforms themselves, weakening traditional warning signs and behavioral defenses.

# 1

## Where trust lives

### How communication evolved, and why messages are no longer questioned

Communication hasn't always looked like this.

For most of human history, messages were physical objects. A letter took days or weeks to arrive. You recognized the handwriting before you opened the envelope, or you didn't, and that alone told you something about whether it was worth reading. A message was a deliberate act, sent with intention and received with attention.

Even the early digital era sustained some of that distance. Emails arrived in their own space, separate from conversation. You sat down at a desk to write one. You read them in batches. There was a time to check your inbox, and a time to be away from it.

Then messaging apps collapsed that distance entirely.

Today, messages arrive everywhere. They land on our phones, our watches, our laptops, our tablets, our smart speakers, even in our glasses and earbuds. Messaging apps now reach more than **3 billion people worldwide**.

What changed isn't just the speed. It's the scrutiny.

A message feels like something that happens in the background of everything else you're doing. You read them while walking. You reply while making dinner. We've stopped questioning messages because they've become part of the texture of everyday life. As routine as checking the weather or unlocking a door.

And that's exactly the vulnerability scammers have learned to exploit.



**3 billion**

people use messaging apps. Messaging isn't a channel. It's the default.



### The opening move

It starts with something routine. Something you've seen a hundred times.

A delivery notification. A banking alert. A message from a retailer you ordered from last week. Messaging apps have made this kind of contact feel completely normal.

The platforms people trust most are also the ones targeted the most.

Where scams begin



"I received a message about a delivery and, because I was actually expecting a package, I fell for it." – Anonymous respondent, Portugal



WhatsApp  
43%



SMS/iMessage  
40%



Facebook  
27%



Telegram  
22%



Instagram  
19%

These aren't fringe platforms. They're where people talk to their mothers and fathers, their children, their partners, their bosses. The very familiarity has conditioned us to trust these spaces.

# 2

## Speed beats scrutiny

### How scam cartels engineer interactions to outpace human judgment

Pressure, when it's applied well, doesn't announce itself. It just moves you incrementally forward.

A follow-up message arrives. Then a link. A request to confirm a detail, verify an account, or make a payment. There's always a reason to act now. A delivery that can't be completed without immediate action. A security alert that can't wait. An offer about to expire. None of it feels extreme. Not in the moment.



"It all felt so real, I didn't even question it." — Anonymous respondent, Spain

### The 30-minute window

Kaspersky's findings show that more than half of successful messaging scams (52%) unfold in under 30 minutes, from first contact to the moment money or personal data changes hands. For 14% of victims, one in seven, the whole thing is over in less than five minutes. That's quicker than boiling an egg. Quicker than taking a shower for most people.

The speed isn't accidental. It's the method.

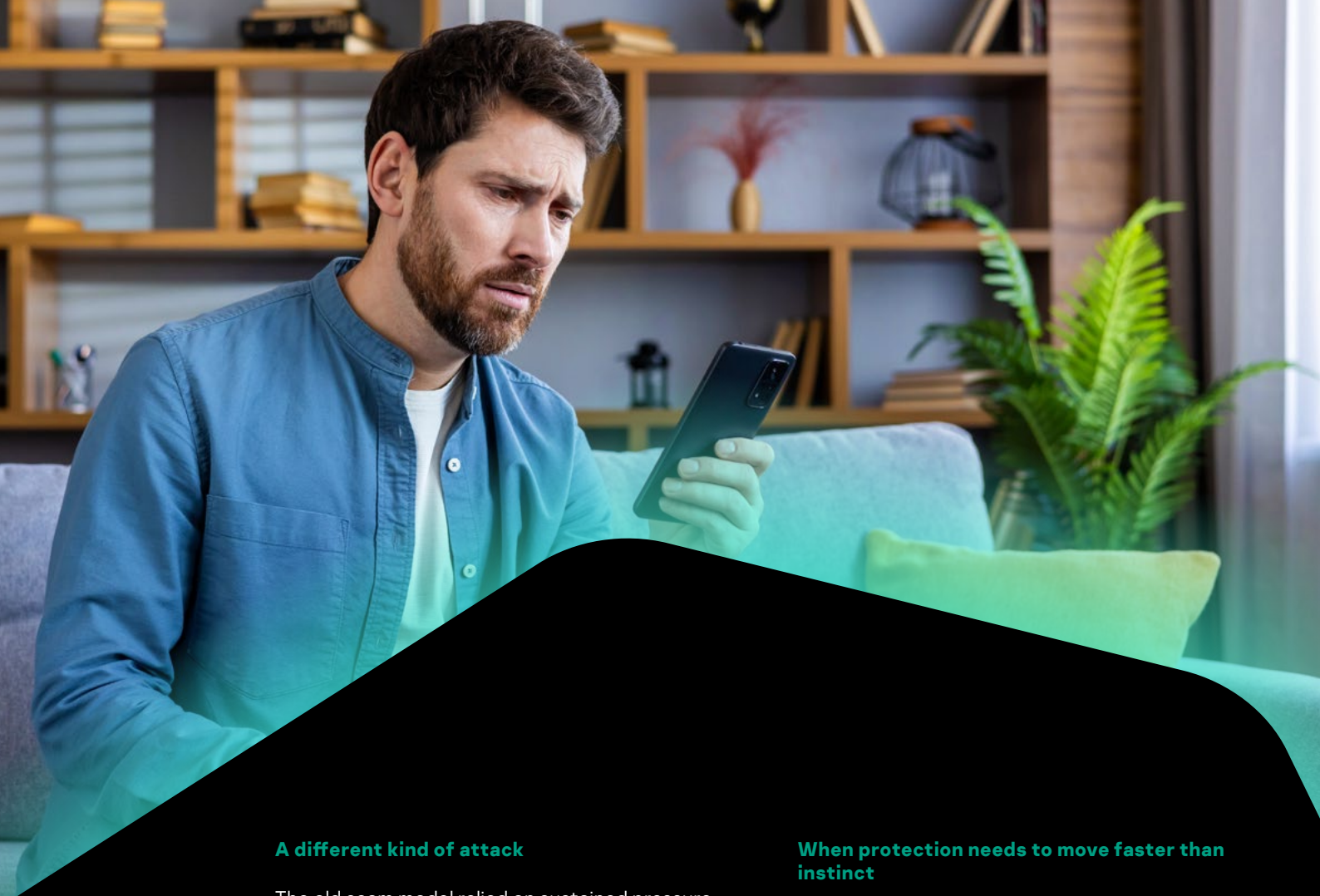
Every element is engineered to compress the decision-making window: the urgency of the scenario, the familiarity of the format, the plausibility of the request. When something feels urgent, the instinct is to resolve it, not question it. Click the link. Confirm the details. Approve the transaction.

By the time the instinct to pause arrives, the scam is already complete. For just over half of all victims (51%), what gets stolen is money. For 43%, it's personal data, most commonly phone numbers, names and email addresses. Often, it's both.

**52%**

of messaging scams succeed within 30 minutes. For 1 in 7 that drops to 5 minutes.





### A different kind of attack

The old scam model relied on sustained pressure. Long phone calls, drawn-out conversations, a scammer working to wear down resistance over hours or days until something gave. Detection was possible because the attack had a recognizable rhythm, and the pressure itself felt wrong.

The new model is the opposite. Scam cartels don't want to hold victims on the line. They want to catch people in motion, between meetings, on a commute, or during everyday tasks, when your attention is already fragmented. They mimic your mother's turn of phrase. They match your bank's tone of voice. They copy your courier's format exactly. Then, casually, almost conversationally, they make the ask.

The attack doesn't feel like an attack. It feels like the same message you've received hundreds of times.

That's why "tech-savviness" no longer offers protection. The familiar signals that used to give scams away, the bad grammar, the awkward phrasing, the obvious urgency, have been systematically engineered out. What's left looks, sounds and reads like the real thing.

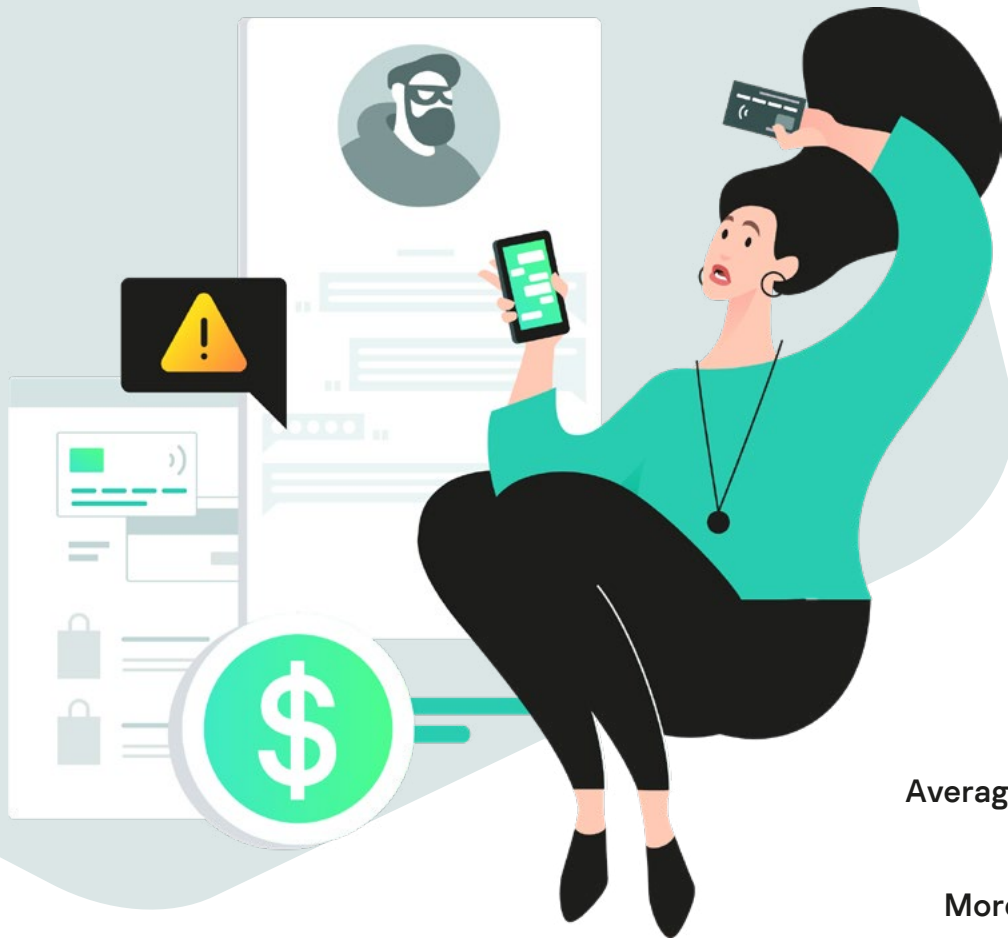
### When protection needs to move faster than instinct

In reality, no one trusts what lands in their inbox or messaging apps anymore. And when asked what would actually restore that trust, there is no single, clear solution. Some look for obvious signals, such as verifying the sender (24%), using a built-in scam detection tool (24%) or keeping an eye out for warning labels (19%).

Others want more control over how messages are filtered or delivered. Beyond that, certainty drops quickly. Only 11% cite integration with security tools such as antivirus. A small proportion say nothing would help at all, while on the flip side only 1% say they already trust incoming notifications.

When decisions have to be made in seconds, relying on instinct or awareness alone isn't enough. Protection has to kick in earlier. Not after the click, but before it. At the point where a message appears, where a link is first seen, where a decision is about to be made.

Increasingly, that means using technologies that can detect suspicious activity in real time, flag malicious links and reduce the need for people to make flawless decisions under pressure. That's the only way to cut away the advantage that scam cartels have created.



Average loss per victim:

**\$733**

More than 1 in 10 lose  
over \$1,350.

# 3

## The aftermath

### The illusion of control, the weight of what's taken and the damage that stays

The illusion of control, the weight of what's taken and the damage that stays

### Micro-losses, macro-damage

The financial hit doesn't look catastrophic in isolation. The average loss per victim is \$733. A few hundred here, a few hundred there. More than a third of victims (36%) lose under \$135.

These are micro-losses by design. Small enough that some never report them. Small enough that banks don't always investigate. Small enough to be dismissed as bad luck rather than organized crime.

But \$733 is not nothing. It's a month of groceries. An energy bill. Childcare for the week. In the middle of a global cost-of-living crisis, a single scam can tip a household from managing to desperately struggling. And for more than one in ten victims (11%), the loss is over \$1,350. That's a serious financial shock.

Scaled globally, across billions of messaging app users, these individually small amounts add up to a devastating financial drain measured in the billions. And the damage isn't landing on one demographic. Kaspersky's data shows victims spread evenly across generations, from Gen Z to Gen X. Being "good with technology" doesn't protect you.

## Scammed once, scammed again

More than a quarter of victims (28%) report being scammed three or more times. Once scam cartels know a number responds, a person clicks and an inbox is active, that contact becomes an asset. The targeting intensifies. The scripts adapt. What starts as bad luck hardens into a pattern. Each repeat erodes more than money. Each repeat interaction erodes the belief that you can learn your way out.



**“They kept asking me for more and more money so I could get my payout. I felt cheated, sad, angry and helpless.” – Anonymous respondent, Serbia**

## The emotional reckoning

When people describe what happened to them, money is rarely the first thing they mention. 54% of the victims we spoke with say they felt angry the moment they realized what had happened. Not confused. Not uneasy. Angry.

It's a specific kind of anger that comes from having trusted something and discovering it was being used against you.

Underneath the anger, for many, something more disquieting moves in. Shame. A sense of having missed something so obvious. 42% of victims report frustration, 38% report feeling upset. These feelings don't exist in isolation. They press down all at once.



**“I cried, I felt so bad.” – Anonymous respondent, France**

For victims of larger losses, the damage goes deeper still. One French respondent described losing €23,000 to a fake cryptocurrency investment scam. The money was gone within minutes. The consequences weren't: **“Once I sent the money, there was no way to recover it. I fell into depression. I felt abused and betrayed.”**

That pattern, depression, betrayal, a long recovery that sometimes never arrives, is the part that doesn't show up in loss statistics. It's the part that lingers. Nearly half of all victims (48%) say anger is still present six months after the scam. Around a third remain frustrated (33%) or upset (30%).

What also lingers is suspicion. A distrust in incoming messages, of unknown numbers, of anything that asks for a decision. It's a small but permanent recalibration of trust. A cost paid not just by the victim, but by every legitimate sender who now has to work to be believed.

## A deafening silence

Most victims deal with the aftermath alone. Nearly one in ten don't tell anyone at all.

The shame has another effect. It keeps victims silent. It discourages disclosure, delays reporting and keeps a significant portion of the harm invisible. As a result, official statistics capture only a fraction of the true economic and emotional damage.



# 4

## Collateral damage

### When brands become the unwilling face of the crime

The victim isn't the only one who pays.

When a brand is impersonated convincingly enough that someone acts on it, loses money, or hands over personal information, the damage attaches to the name that was exploited. Customers who've been deceived often can't separate the criminal from the brand. Rationally, they know the company didn't send the message. Emotionally, there's an association.

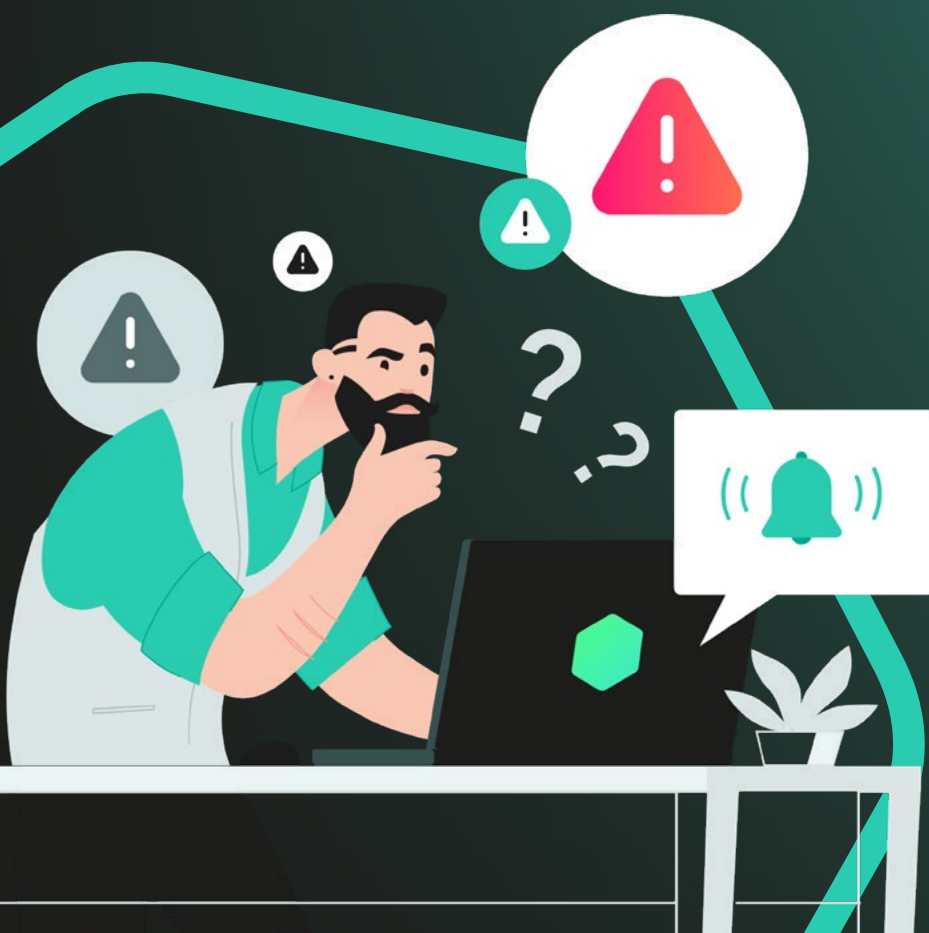
The result is a quiet, hard-to-measure kind of harm.

### The trust collapse

Brand impersonation is now one of the three most common types of messaging scam worldwide, accounting for 31% of cases. Fake delivery notifications top the list at 38%, followed by investment scams at 37%. These are the scams targeting exactly where people buy, bank and trust.

The fallout is severe. A staggering 99% of scam victims say they no longer trust any incoming notifications on messaging channels. That isn't a drift in consumer behavior. It's a near-total collapse of confidence in the very channels brands have invested in to reach their customers.

And the erosion of trust is constantly reinforced. Nearly two-thirds (63%) of scams span multiple platforms, moving from SMS to WhatsApp, from WhatsApp to Telegram, mimicking everyday conversations and notifications to avoid detection. Every platform a scam touches becomes a platform the victim trusts less. Legitimate and malicious messages now appear in the same environments, often with similar formats and timing, leaving customers to make judgment calls without clear trust signals.



**98%**  
of victims no longer trust  
incoming notifications.



### When the brand is the weapon

The names used aren't obscure or unfamiliar. They're the brands people already trust.



**"I saw a website advert on Facebook for Jellycats, it looked good. I went to buy some from the website. My bank stopped the payment, it was a scam website." — Anonymous respondent, UK**

It isn't just retailers. One Spanish respondent described receiving a WhatsApp message that appeared to come from Médecins Sans Frontières, the humanitarian charity. She clicked the link. The scammers harvested her banking details. The same tactics that are used to impersonate banks and delivery companies are being deployed to impersonate telecoms providers, streaming services and employers.

For the customer, the logo and the language are familiar. For the brand, the first sign that anything has happened is often a complaint from someone who was never their customer to begin with, or the quiet erosion of engagement from people who now hesitate over every notification.

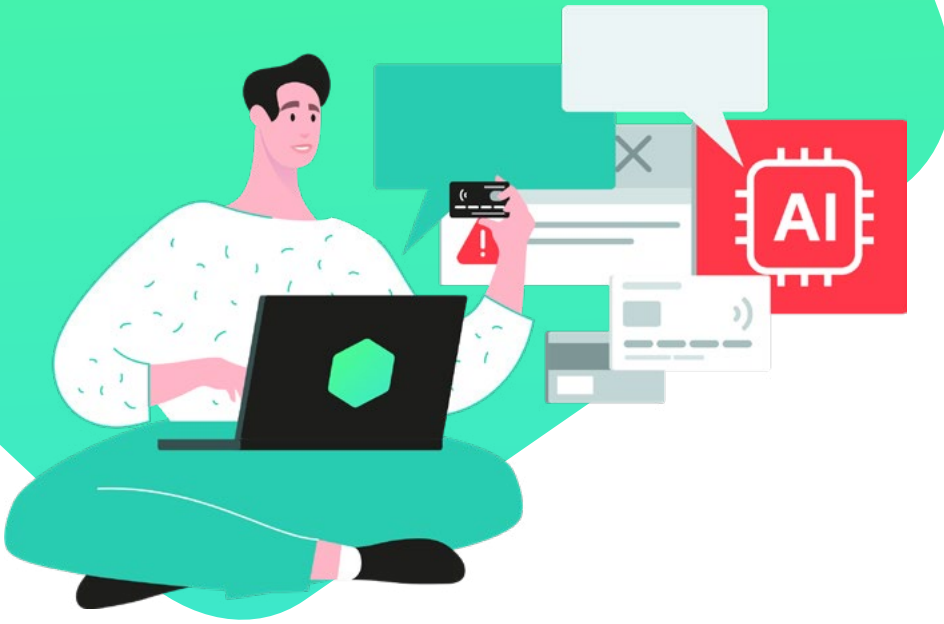
### The pressure shifts to brands

As impersonation scams become more widespread, the pressure on organizations to demonstrate that they are actively protecting their customers grows. This has stopped being "somebody else's problem". The question asked by regulators, customers, and increasingly boards is: what are companies doing to make impersonation harder and how are they responding when it happens anyway?

The reputational cost is real, even when the organization did nothing wrong. The operational cost is just as real. Customer service teams are fielding calls from distressed victims. Communications teams are managing fallout from incidents they didn't create. Trust that took years to build, destroyed by a scam that took minutes to run. Every legitimate message now competes with a shadow version, and every customer is more and more conditioned to assume the shadow version is the more likely one.

### What comes next

The question isn't whether customers will continue to be targeted. They will. The question is what organizations are doing to stop it, and what comes next if they don't. Because the tools being used against them are evolving faster than the defenses.



**66%**  
of victims believe AI  
was used in their scam.

# 5 The accelerant

## How AI turned scam cartels from a small-time operation into a global threat

Everything in this report is already happening. The scams. The speed. The emotional damage. The brand collateral.

AI is accelerating all of it.

### Brands are using AI. So are scammers.

There's a brutal irony at the heart of all this.

Brands are pouring billions into AI to enhance the customer experience: chatbots that sound more human, support agents that respond in real time, personalization engines that know what you need before you ask. Every one of those investments depends on customers being willing to engage with AI-mediated communication from a trusted name.

Scam cartels are using the same technology to undermine the same channels. They write in your bank's tone of voice because the same large language models are available to them. They produce synthetic customer service agents because the same voice cloning tools are available to them. They mirror the rhythm, structure, and style of authentic brand communications across messaging platforms such as WhatsApp and SMS to fool people.

In fact, researchers now describe voice cloning as having crossed an "indistinguishable threshold." A few seconds of audio, the kind easily scraped from a voice note, a TikTok post or a voicemail, is enough to generate a convincing clone, complete with natural intonation, emotion and breathing patterns.

What this creates is overlap. Legitimate and fraudulent messages appear in the same environment, using the same formats, language, and triggers. The difference between them is no longer obvious.

The data shows that two-thirds of victims (66%) believe AI was used in the scam they experienced. 42% cite AI-written messages. More than one in four (31%) report synthetic voices. More than one in five (25%) encountered deepfake images or videos. These aren't projections or warnings. They're what people have reported seeing over the past six months.



### **The cases already making the headlines**

Brand impersonation no longer requires skill, time, or even deep technical knowledge. What once required coordinated effort can now be generated instantly, repeated endlessly, and deployed across millions of messages simultaneously.

Impersonating national postal and courier services, as well as trusted delivery brands such as DHL, is one of the top scams circulating worldwide. Victims receive SMS messages that appear to come from legitimate delivery providers. The messages claim a parcel cannot be delivered without a small payment or address confirmation. Because many recipients genuinely expect deliveries, the request feels routine. Most people enter their personal details, or make a small payment, only to find their accounts compromised within minutes.

The tools used to produce this content are cheap, freely available and require little technical skill. What used to take a specialist team and weeks of effort can now be produced by one person in an afternoon.

These aren't edge cases. They're the template.

### **The only question that matters now**

Scam cartels have gone from a small-time operation to a global threat in the span of a few years. Every attack is faster and more convincing than the last. The question isn't whether AI will continue to accelerate this. It will. The question is whether the response from individuals, brands, and the institutions meant to protect both can move fast enough to matter.

# The wake-up call

This isn't a warning about what's coming. It's an account of what's already happening.

Messaging scams are no longer a fringe threat. They're globally organized, AI-accelerated and operate at industrial scale. The emotional damage runs deeper than statistics can show. The brands whose names are being used as cover are paying for a crime they didn't commit.

And the financial damage, properly scaled, is staggering.

Individually, \$733 is a big loss for the average household. Scaled across the global population of messaging app users, it becomes something much larger. If just 10% of the 3 billion messaging app users worldwide were scammed at the average loss reported in this research, total losses would exceed \$219 billion. That's not a consumer fraud statistic. That's comparable to the GDP of a mid-sized country, extracted quietly through billions of individual micro-losses that rarely appear in official crime statistics.

Only 24% of victims report to the police. Only 23% report to their bank. The true scale of the damage is almost certainly larger than the figures we see.

This is the moment to respond.

For individuals, that means accepting that instinct alone is no longer a reliable defense. The signals that once made a scam detectable have been systematically engineered out. What remains is the need to build habits and deploy tools that don't rely on something "feeling" wrong before action is taken.

For businesses, it means accepting that this is partly their problem to solve, even when they are the victim of the impersonation rather than its cause. When customers are targeted through a brand's name, the reputational and operational consequences land on the brand anyway. Waiting for platforms or regulators to fix this isn't a viable strategy. It's consenting to the damage.

The good news is that practical steps exist. They aren't complicated. And taken together, they significantly reduce the risk.

**If just 10% of the world's 3 billion messaging app users were scammed, global losses would exceed \$219 billion.**



# Start protecting yourself now

Scam cartels have built a business on the assumption that the rest of us aren't organized enough to stop them. The channels aren't going away. The attacks aren't going away. But the gap between being a target and being a victim is one that can be actively closed. That work can start now.

## Three steps for individuals



### Pause before you act.

The urgency you feel in the moment is almost always manufactured. A genuine bank, retailer or delivery service will not penalize you for taking thirty seconds to verify before clicking a link or confirming a detail. The instinct to resolve something quickly is exactly what scam cartels are engineering for. Pausing breaks the mechanism.



### Verify through a separate channel.

If a message appears to be from a family member, a colleague or a company you trust, confirm through a different route before acting. Use secure verification methods and cross-check identities when something doesn't feel right. For families, agreeing on a "safe word" in advance can defeat even the most convincing voice clones.



### Use protection that works in real time.

Solutions like [Kaspersky Premium](#) provide real-time protection against malicious links and phishing attempts across the apps and websites you use every day. On mobile, [a dedicated layer of anti-phishing security](#) scans suspicious links as they appear, even within notifications, identifying threats before you engage. Paired with a tool like [Kaspersky Password Manager](#) for unique, securely stored credentials, a single compromised interaction is far less likely to cascade into wider account compromise.





## Three steps for businesses

### STEP ONE

#### Stay informed and invest in robust security tools.

Verified business profiles, two-factor authentication and active monitoring of a brand's digital footprint all raise the cost of impersonation. Solutions such as [Kaspersky Brand Monitoring](#) help detect misuse of your brand across social media, online marketplaces and parts of the dark web, allowing organizations to identify impersonation early and act quickly. Paired with [Kaspersky Takedown](#), harmful or fraudulent content can be investigated and removed before it spreads further.

### STEP TWO

#### Educate consumers and employees.

Run ongoing awareness campaigns to inform customers about active scams and how to identify them. Implementation of an educational program for your employees ensures they can provide relevant information to customers while remaining resilient to cyberthreats. [Kaspersky Security Awareness training](#) significantly reduces human cyber risk: 95% of trained employees can successfully spot phishing attacks.

### STEP THREE

#### Build detection and response into your operations.

The faster the impersonation activity is identified, the less damage it does. Clear internal processes to detect, escalate and respond to scams, paired with close monitoring of emerging threats, allow organizations to act quickly when incidents occur, minimizing impact on customers and shortening the window scammers rely on.



## Methodology

The survey was conducted by Censuswide on behalf of Kaspersky in April 2026, gathering insights from 2,806 messaging-scam victims aged 16–61 across Europe (United Kingdom, France, Germany, Italy, Spain, Portugal, Greece, Serbia), North America (United States of America) and Africa (Morocco, Senegal, Ivory Coast).

## About

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. With over a billion devices protected to date from emerging cyberthreats and targeted attacks, Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection, specialized security products and services, as well as Cyber Immune solutions to fight sophisticated and evolving digital threats. We help over 200,000 corporate clients protect what matters most to them.

[Learn more at \[www.kaspersky.com\]\(https://www.kaspersky.com\).](https://www.kaspersky.com)



[Kaspersky.com](https://kaspersky.com)  
[Kaspersky.com/blog](https://kaspersky.com/blog)

© 2026 AO Kaspersky Lab.  
All rights reserved. Registered trademarks and service marks are the property of their respective owners

**kaspersky**