All Rights Reserved. © 2026 Bitdefender.
All trademarks, trade names, and products referenced herein are the property of their respective owners.

WHITEPAPER

Telco Customers Are Being Targeted by Scammers Every Day. It’s Time to Protect Them.

Contents

Executive Summary

Scams happen every day, often escalating within hours. Your customers believe they can protect themselves, yet modern scams powered by AI have removed the obvious warning signs. The gap between what people rely on and what actually protects them is growing.

When the damage happens, customers do not blame technology, and they do not blame themselves for long. They turn to the institution closest to their money, their payments, or their connectivity. In other words, they turn to you, expecting support, answers, and their money back.

You can respond after the damage is done and help them recover. But imagine being able to step in before the scam happens.

This white paper looks at how scams are evolving and what that means for you, and how choosing to protect your customers before they become victims strengthens relationships, builds lasting trust, and gives you a clear advantage in a rapidly changing landscape.

Introduction

Globally, 70% of adults encountered a scam in the past year, and 23% had money stolen. According to the Global Anti-Scam Alliance (GASA)*, the estimated financial impact across 42 countries reached $442 billion USD last year alone.

These are working parents, seniors, veterans, people who believe they are answering a call from their bank or clicking a link from a trusted institution.

They are also your clients.

For many, Scam attempts are part of daily life, with **13% reporting being targeted at least once a day**.

AI has industrialized deception. Deepfakes, voice cloning, and hyper-personalized phishing have removed many of the warning signs people once relied on.

Beyond financial loss, scams erode confidence, strain relationships, and weaken trust in institutions, companies, and platforms.

Every Day, Scammers Steal More from People Worldwide

Many victims are contacted again and again, sometimes through different channels, sometimes by different criminals using the same data.
According to research from the Global Anti-Scam Alliance (GASA), the following scams are among the most common affecting consumers today:

Shopping scams (54% targeted, 24% more than once)

People order products from what appear to be legitimate online stores or marketplace listings. The items never arrive, or what arrives is nothing like what was promised. These scams tend to spike around holidays and high-demand product launches, when urgency lowers caution.

Investment scams (48% targeted, 23% more than once)

Victims are offered high or "guaranteed" returns through crypto platforms, trading communities, or exclusive investment groups. The websites and testimonials feel legit and authentic.

Unexpected money scams (48% targeted, 23% more than once)

Individuals are told they are owed money, have won a prize, or must pay a small fee to unlock funds. The message creates urgency: act now, or lose the opportunity.

Identity theft (42% targeted, 17% more than once)

Personal data is stolen and used to open accounts, apply for credit, or execute unauthorized transactions. Many victims only realize something is wrong when the financial damage is already visible.

Impersonation scams (41% targeted, 20% more than once)

Scammers pose as banks, government agencies, telecom providers, or even family members. With spoofed numbers and voice cloning, the interaction can feel entirely authentic.

Charity scams (40% targeted, 19% more than once)

Crises and natural disasters are exploited to solicit donations through fake organizations or cloned websites that closely resemble legitimate charities.

Fake invoice scams (40% targeted, 21% more than once)

Victims receive invoices for services never requested, or payment details are subtly altered in legitimate-looking bills. Both households and businesses are affected.

Employment scams (39% targeted, 19% more than once)

Job seekers are offered remote roles and asked to pay onboarding fees or share sensitive information under the guise of recruitment.

After losing money, victims are contacted again — this time by someone claiming they can recover the funds, for a fee. Those already harmed are often targeted a second time.

Romance or relationship scams (34%targeted, 17% more than once)

Emotional relationships are built over time, creating trust before financial assistance is requested for fabricated emergencies or travel plans.

Blackmail or extortion scams (31% targeted, 17% more than once)

Victims are threatened with the release of personal information, images, or fabricated accusations unless payment is made quickly.

These scams may take different forms, but they rely on the same levers: trust, urgency, and vulnerability. And once someone engages, even briefly, they can become part of a cycle, contacted again and again because they've been identified as likely to respond.

Key Takeaways

- ↳ **There isn't one "main" scam.** The threat is broad, from shopping and investment fraud to impersonation and fake invoices.
- ↳ **Trust is the common entry point.** Whether posing as a bank, a charity, or a family member, scammers rely on credibility and urgency.
- ↳ **Once someone responds, they become more vulnerable.** Engagement can place victims into a repeated targeting cycle.

The Gap Between What People Do and How Protected They Really Are

Most people believe they are prepared to deal with scams. Globally, 73% say they feel confident in their ability to recognize one. One in ten even claims they can always spot a scam. At the same time, scams continue to succeed at scale.

When asked why they were deceived, many victims say the interaction simply felt real. That is especially true among older generations. Others admit they acted quickly and only later realized they had missed warning signs, or that the opportunity seemed too good to question in the moment. More than one in ten still struggle to explain what happened, describing the experience as confusing and disorienting.

At the same time, 93% say they take at least one step to verify whether an offer is legitimate. The issue is that the methods people rely on are no longer strong enough for the threats they are facing.

Some of the most common protective behaviors include:

- ↳ Following the rule "if it seems too good to be true, it probably is" (31%)
- ↳ Searching for reviews on other websites (30%)
- ↳ Checking for spelling and grammar errors (27%)
- ↳ Looking for a visible phone number (25%)
- ↳ Reviewing whether the email comes from a free provider (24%)
- ↳ Checking if the company is active on social media (21%)
- ↳ Asking friends or family for advice (21%)
- ↳ Verifying the presence of an SSL certificate (20%)
- ↳ Preferring refundable payment methods (18%)

These steps reflect the common-sense digital hygiene we have promoted for years. But in an environment shaped by AI-generated content, cloned voices, and highly polished fraudulent websites, they are no longer enough. It is like treating today's virus with an old medicine. The intention is right, but the remedy no longer matches the threat.

The result is a widening gap between the defenses people rely on and the methods scammers use to deceive.

Key Takeaways

- ↳ **Confidence is high, protection is not.** Most people believe they can spot a scam, yet large numbers still fall victim.
- ↳ **Old red flags are fading.** Grammar mistakes and clumsy websites are being replaced by AI-polished messages and convincing impersonation.
- ↳ **Effort isn't the problem.** Nearly everyone takes some step to verify offers, but traditional checks no longer match modern threats.
- ↳ **The gap is growing.** What people rely on for safety is no longer aligned with how scams actually work.

The Human Cost of Scams

In some cases, the financial damage is devastating. People lose their life savings, take out loans to "fix" what they believe was a mistake, or give away retirement funds meant to support an entire household. Some families lose homes or long-term financial stability because of a single moment of manipulation.

But even when the monetary loss is smaller, the emotional impact rarely is. For many, the experience feels like a personal violation.

Two-thirds of scam victims report long-term emotional consequences, including anxiety, depression, and PTSD, and 69% describe the experience as highly stressful. Victims often experience distress that leaves them feeling isolated from friends and family, and in the most serious cases, those feelings can have life-threatening consequences.

The effects extend beyond the initial loss: spending habits change, access to credit becomes more difficult, essential expenses are postponed, and relationships are strained.

Scams reshape how people feel about safety, trust, and their own judgment.

The human impact becomes clearer when we look at real stories people share on Reddit:

"My Mother-in-Law Lost $250,000 to Romance Scams. We Later Discovered She Took $150,000 from Her Sister."(1)

For eight years, an elderly woman believed she was in a relationship with a series of men who never existed. The stories are familiar: an oil rig engineer stranded overseas, a wealthy businessman facing temporary financial restrictions, a soldier waiting for clearance to return home. Each promised a future together, but needed urgent financial help.

Over time, she transferred more than $250,000 of her own savings. When those funds ran out, she borrowed from others. Eventually, she began accessing the accounts of her sister, for whom she held power of attorney due to advanced dementia. Approximately $150,000 was funneled to scammers.

"My 10-Year-Old Spent $5,500 on Roblox and TikTok Before I Even Knew It Was Happening."(2)

A parent received a fraud alert from their bank and assumed their card had been compromised. Dozens of charges had appeared, many exceeding $100 each. As they reviewed the statement more closely, they realized the payments were linked to digital platforms — in-app purchases tied to gaming and social media.

Nearly 300 transactions had accumulated, totaling approximately $5,500. The child had been purchasing digital currency and virtual rewards, some of which were used to gain visibility and validation online.

The parent's first reaction was disbelief. The second was fear, not only about the financial impact, but about how easily digital ecosystems can influence behavior before adults even realize what is happening.

"My Son Deposited a Check for Someone He Knew. Now His Account Is Overdrawn." (3)

A 17-year-old high school student, described by his parent as responsible and close to his family, agreed to help someone he knew casually from town. The acquaintance handed him a check and asked him to deposit it into his account and send back part of the funds through Venmo. The teenager deposited the check and transferred the money. Days later, the bank flagged the deposit as fraudulent. By the time the reversal occurred, his account was overdrawn by more than $500.

The parent discovered the issue while logging in to send money via Zelle and was confronted with a negative balance instead. "I feel like I need to teach him how to avoid getting scammed in the future, but all the guides I see online are about avoiding online scams, not real world. And back in the real world, I'm trying to figure out how hard to pursue the scammer. I'm worried about retaliation."

Key Takeaways

- ↳ **Families absorb the shock.** Losses affect not just individuals but entire households: savings disappear, credit suffers, relationships strain.
- ↳ **The psychological impact is significant.** Two-thirds report long-term emotional consequences, and many describe the experience as highly stressful.
- ↳ **No age group is immune.** From children in digital ecosystems to teenagers navigating independence and older adults seeking connection, scams touch every generation.
- ↳ **Recovery is complex.** Even after the money is gone, families face confusion, guilt, fear of retaliation, and uncertainty about what to do next.

When Money Is Lost, Your Customers Turn to You

Consumers are divided when asked who should be responsible for protecting them from scams. Online platforms and governments are most frequently cited, yet those same institutions are often perceived as the least effective when real harm occurs.

When money is lost, expectations shift quickly. In that moment, people look to the institutions closest to their finances and connectivity — banks, payment providers, insurers, and even telecom operators — not only for support, but often for reimbursement and real protection.

Globally, adults are clear about who they believe should take responsibility when money is lost to scams and who should help return it:

- ↳ 45% believe banks should always reimburse scam victims.
- ↳ 42% expect credit card companies to intervene.
- ↳ 41% expect payment service providers to step in.
- ↳ 34% expect telecom operators to play a protective role.

In theory, responsibility may feel distributed. In practice, it lands with the institution holding the account, processing the payment, or enabling the connection: the bank that can recognize a manipulated transaction, the telecom operator that can detect a spoofed call, the insurer that can limit the damage.

Key Takeaways

- ↳ **Responsibility becomes personal when money disappears.** In the moment of loss, customers turn to the institution closest to their money or connection.
- ↳ **Expectations are high — especially for reimbursement.** Nearly half of adults believe banks should always refund scam victims.

Scam Protection Is Complex Work. We Make It Possible for You.

Scam prevention today sits at the intersection of artificial intelligence and human behavior. Criminal networks share tools, refine scripts, and increasingly use AI to make their messages more convincing. They test what works, adjust quickly, and scale their tactics faster than most traditional response systems were designed to handle.

At the same time, victims authorize transactions believing they are doing the right thing. They trust the voice on the phone, the message on the screen, or the person asking for help. Fraud now unfolds in real time, which leaves very little space to intervene once money has moved. By the time a transfer is completed, the opportunity to prevent damage has often passed.

That is why scam protection has to start earlier by recognizing when someone's decision has been influenced, not just when a transaction looks unusual. We use AI to analyze behavioral patterns alongside digital activity, identifying when an action does not match the person behind it, and intervening before damage is done.

The entire Bitdefender Scam Protection portfolio is built for this reality. Rather than expecting people to recognize every red flag on their own, the portfolio works quietly across the channels people use every day:

- ↳ Scamio Pro – An AI-powered assistant that helps users evaluate suspicious messages, links, and conversations before they act.
- ↳ Scam Radar – Notifies users when scam outbreaks are detected in their region, giving them context before they engage.
- ↳ Web Scam Protection – Monitors browsing activity and identifies emerging scam patterns in real time.
- ↳ Email Protection – Continuously analyzes Gmail, Outlook, and local Windows email clients, marking messages as safe or unsafe.*
- ↳ Remote Access Scam Protection – Detects behavioral patterns associated with scammers attempting to gain remote

control of a device.**

- ↳ SMS Protection – Uses AI to identify scam messages and malicious links in text conversations.***
- ↳ Scam Notification Protection – Extends detection to suspicious push notifications.****
- ↳ Chat Protection – Identifies scam attempts across popular messaging platforms such as WhatsApp, Facebook Messenger, Telegram, and Discord.****
- ↳ Calendar Invites Protection – Detects malicious links and deceptive content embedded in calendar invitations.*****

This layered approach extends protection beyond transactions and into the behavioral space where manipulation begins.

And local email clients on Windows
** Windows only
*** Android and iOS only
**** Android only
***** iOS only

By integrating Bitdefender Scam Protection into the services you offer, you stand beside your customers when they are most vulnerable, helping prevent harm instead of explaining it afterward.

For you, this translates into stronger trust, lower support and reimbursement costs, and a differentiated offer in a market where customers increasingly expect proactive protection. Scams will continue to evolve. So must the institutions people rely on. Those who build AI-powered protection into their core offering today will define the standard for tomorrow.

Key Takeaways

- ↳ **Scams move faster than traditional defenses.** Criminal networks use AI, data, and coordination to scale manipulation in real time.
- ↳ **The critical moment happens before the money moves.** Once a transaction is authorized, recovery becomes harder and more costly.
- ↳ **Behavioral insight is the new frontline.** Effective protection requires detecting when a decision has been influenced — not just when a transaction looks unusual.
- ↳ **Protection must follow the user, not just the payment.** Scam detection needs to operate across messages, calls, browsing, and apps — where manipulation actually begins.

Why Choose Bitdefender as Your Trusted Partner?

We have been using AI in our security solutions long before it became a buzzword. For us, it has been a practical tool to detect threats earlier, understand behavior more clearly, and build protection that works reliably at scale.

Bitdefender Scam Protection continues to evolve as scams evolve. In 2026, we are expanding our capabilities to address voice-based scams, strengthen fake-shop detection, and defend against deepfake-enabled attacks, building on technologies we are already testing in real-world environments.

For more than two decades, we have protected individuals, businesses, and governments against increasingly sophisticated cyber threats. Our AI-driven technologies and security expertise have made us a long-term partner for organizations that need protection they can trust.

Today, we safeguard millions of users across 170 countries. We also work closely with global law enforcement to disrupt criminal networks, expose emerging threats, and help make the digital world safer, not only by reacting to attacks, but by anticipating them.

Key Takeaways

- ↳ **AI is not new to us** – It has been part of our security foundation long before it became a trend.
- ↳ **Protection evolves with the threat** – Scam Protection is continuously expanding to address voice scams, deepfakes, and fake-shop networks.
- ↳ **We act beyond prevention** – Through collaboration with global law enforcement, we help disrupt criminal networks and reduce threats at their source.
- ↳ **We don't just react to scams** – we build defenses ahead of them.

Sources:
* Global State of Scams 2025 Report. Bitdefender is actively involved in fight against scams as a board member of GASA, and the data referenced in this white paper reflects findings from its most recent global report.

(1)

(2)

(3)

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com

Bitdefender-SPP-whitepaper-TLC_CS_SCAM-brand343-en_EN
CD-07/30/24 • MD-March 3, 2026 11:13 am