From Network to Trust Platform:

How Telcos Win by Embedding Scam Protection

Turning scam defense into stronger app engagement, lower churn, and premium growth in 2026

norton™

From connectivity provider to trusted digital safety platform

Telecom operators are under pressure to prove value beyond connectivity. Faster networks, better bundles, and sharper pricing still matter — but they do not fully solve the churn problem. Customers rely on their telco every day, yet many only engage when they receive a bill, need support, or consider switching.

That relationship is too thin for the next phase of competition. In 2026, the operators that embed scam protection directly into their platforms — not as a bolt-on feature, but as a visible, everyday trust layer — will begin to redefine what a telco relationship actually means.

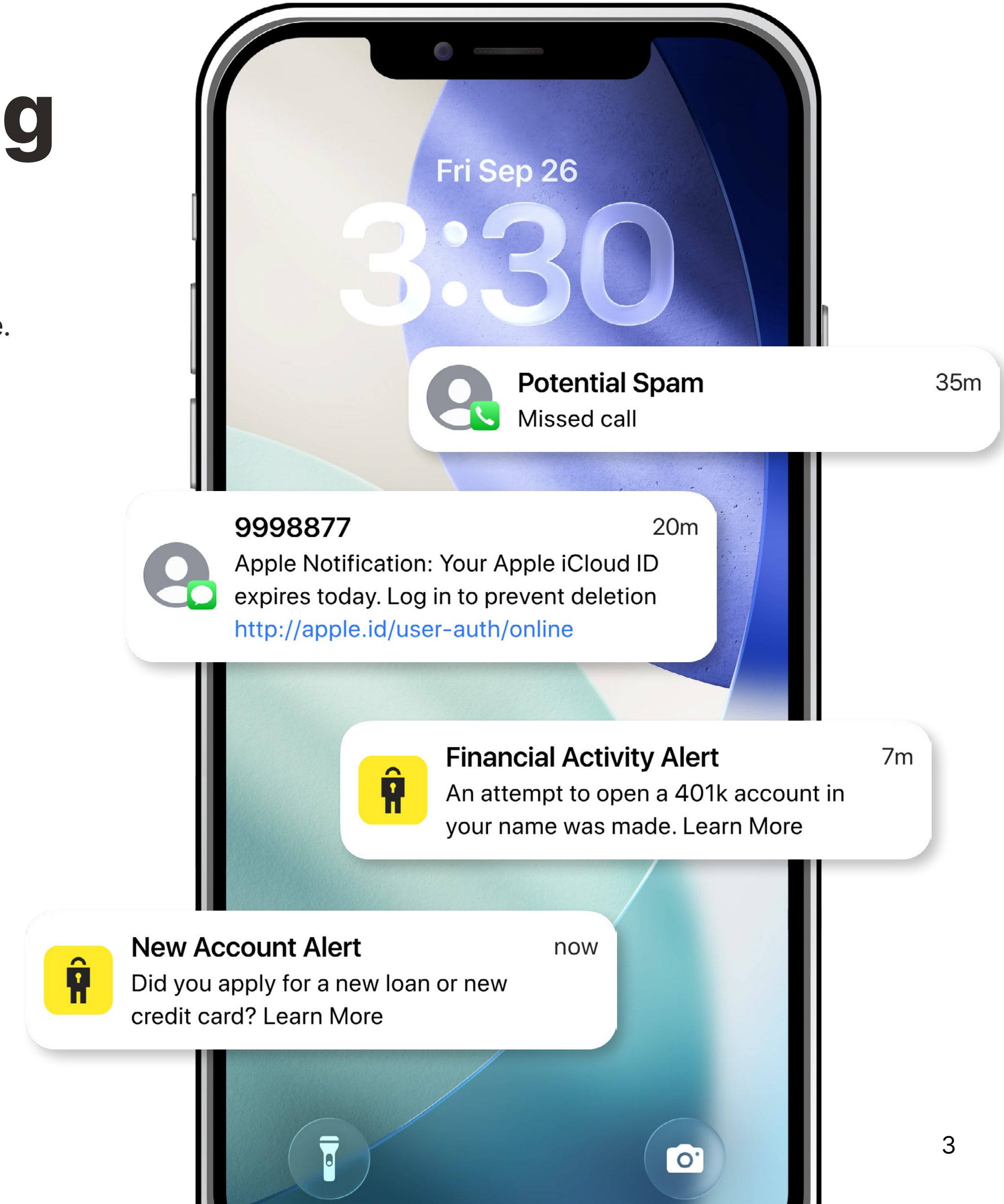
> **The strategic shift is clear: telcos are moving from connectivity providers to trusted digital safety platforms.**

The telco value problem is becoming a trust problem

Connectivity is essential, but increasingly hard to differentiate. When the network works, it fades into the background. That creates a difficult engagement dynamic: the telco is critical to daily life, but customers may not feel active value from the relationship very often.

At the same time, consumers are facing more digital risk than ever — scam texts, fraudulent calls, impersonation attempts, AI-enabled social engineering, and marketplace fraud are now part of everyday life. These threats arrive through the same channels telcos help enable: calls, SMS, mobile apps, and browsers.

A telco that helps customers identify suspicious messages, avoid unsafe links, and respond to potential fraud is doing more than offering security. It is building a stronger, more trusted relationship. Trust is becoming a product experience.



The global scam economy: What the data reveals

Consumers lost an estimated **$442 billion to scams** in the past year[1]

Losses to investment scams **soared by 40% in a year**, to a new record high[2]

70% adults globally have had a scam experience in the last year, with exposure most common in Oceania, South America, and Africa[1]

Wire or bank transfer is the most common method of transferring money to scammers, particularly in South America, the Middle East, and Asia[1]

71% of fraud victims report emotional impact. More say scams hurt their mental health (60%) than their finances (50%) — making scams a wellbeing crisis, not just a financial one.[3]

Scams are now a customer experience issue

Scams are different from most digital threats because they are immediate, emotional, and personal. A suspicious message creates anxiety. A fake payment request triggers panic. A convincing impersonation attempt puts a vulnerable family member at risk.

For telcos, this makes scams more than a cybersecurity concern — they become a customer experience issue, a support issue, and a brand trust issue. When customers are confused or worried, they turn to the organization they already trust.

Embedded scam protection allows operators to help customers before confusion becomes harm. A scam check, safety alert, or suspicious link warning gives customers practical help in the moment they need it — turning reactive support into proactive protection.

Embedded protection changes app engagement

Many telco apps are still used primarily for account management — checking usage, paying bills, or contacting support. These interactions are useful, but they are not frequent, and they are rarely emotionally positive. Scam protection can change this entirely.

When protection is built into the app, it creates high-intent reasons for customers to return. Alerts, scan results, identity notifications, and safety guidance become visible proof that the telco is actively working for them — not just collecting a direct debit.

The new engagement loop

Risk appears
Scam, link, call

→

Customer opens app
Seeking guidance

→

Telco helps
Safe or not safe

→

Value proven
In the moment

→

Trust earned
Repeat

Over time, this reshapes how customers perceive the brand. The telco is no longer just the company that delivers connectivity and sends a bill. It becomes the company that helps protect their digital life.

From value-added service to core platform strategy

Historically, consumer cyber safety has been sold through telco channels as an optional add-on. That model still has a role — but it is no longer enough for the scale of the scam problem, or for the depth of relationship telcos need to build.

The stronger opportunity is protection that feels native. Telcos increasingly want safety capabilities to live inside their own customer experiences, with full brand control — not redirected to a third-party product.

Value-added service
"Would you like to buy protection?"

Core platform strategy
"Protection is part of what it means to be our customer."

That second message is more powerful. It supports differentiation, loyalty, and customer lifetime value — because it aligns with what consumers increasingly need: confidence, simplicity, and protection in the moments that matter.

Why 2026 is the inflection point

Several forces are converging to make embedded scam protection a strategic priority this year — not next year.

AI-powered scams

Fraudulent messages are becoming more convincing, impersonation more scalable, and social engineering more personalized.

Vulnerable audiences

Older customers, families, and small businesses need simple, accessible protection — not complex products.

Privacy expectations

Data sovereignty and responsible processing are increasingly central to platform decisions.

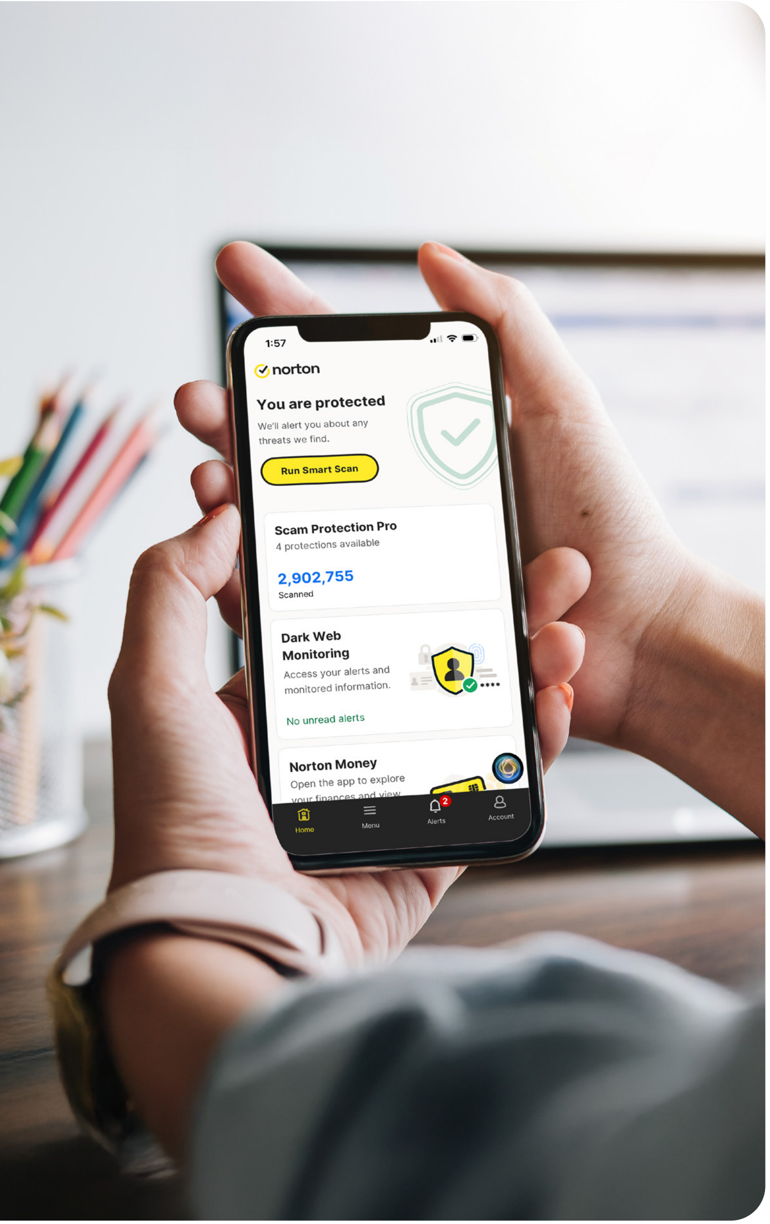
Local fraud trends

Scams now mirror local banks, delivery services, and government agencies — requiring localized, timely intelligence.

Digital engagement gap

Operators need more recurring reasons for customers to open their apps. Safety moments fill that gap.

The operators that move first will establish the association between their brand and digital safety — and that association is difficult for later movers to displace.



What embedded scam protection should deliver

Effective scam protection feels native to the telco experience — easy to find, easy to understand, and genuinely useful in the moment. The best implementations share six qualities.

- **Native**
  Lives inside the telco app. Customers never need to leave the ecosystem to get help.
- **Contextual**
  Responds to real moments: suspicious texts, unsafe links, unknown callers, local fraud trends.
- **Scalable**
  Flexible integration via SDK, API, white-label UI, or widget — meeting operators where they are.
- **Visible**
  Customers see protection working — alerts, scans, safety status, recommendations.
- **Simple**
  One clear answer: is this safe? What do I do next? Who can help me?
- **Extensible**
  A foundation for identity, privacy, device security, parental controls, and AI-assisted support.

The right platform lets telcos start with scam protection and grow into a broader digital safety proposition — without rebuilding the experience from scratch at each stage.

The commercial case: Retention, ARPU, and differentiation

Embedded scam protection is not just a customer experience investment — it has a clear commercial logic.

Stronger retention
Visible, ongoing value beyond connectivity gives customers a reason to stay — and a story to tell others.

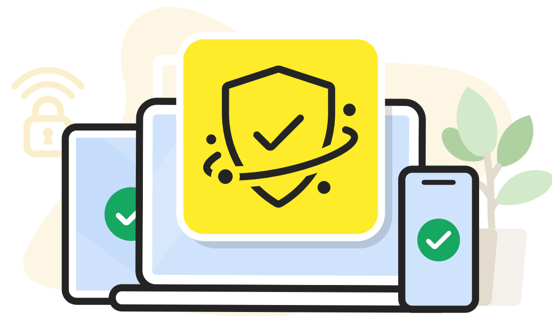
Reduced support pressure
Helping customers earlier in their journey — before panic becomes a call — can reduce care costs.

Increased app engagement
Safety moments create recurring, high-intent reasons to open the telco app beyond bill payment.

Brand differentiation
The telco that becomes known as the safe network earns an advantage that pricing alone cannot replicate.

ARPU growth
Premium tiers, family safety plans, and bundled protection help create natural upsell opportunities.

> **Scam protection can help telcos turn safety into engagement, engagement into trust, and trust into loyalty.**



What telco leaders should do now

Five priorities for operators preparing to embed scam protection in 2026

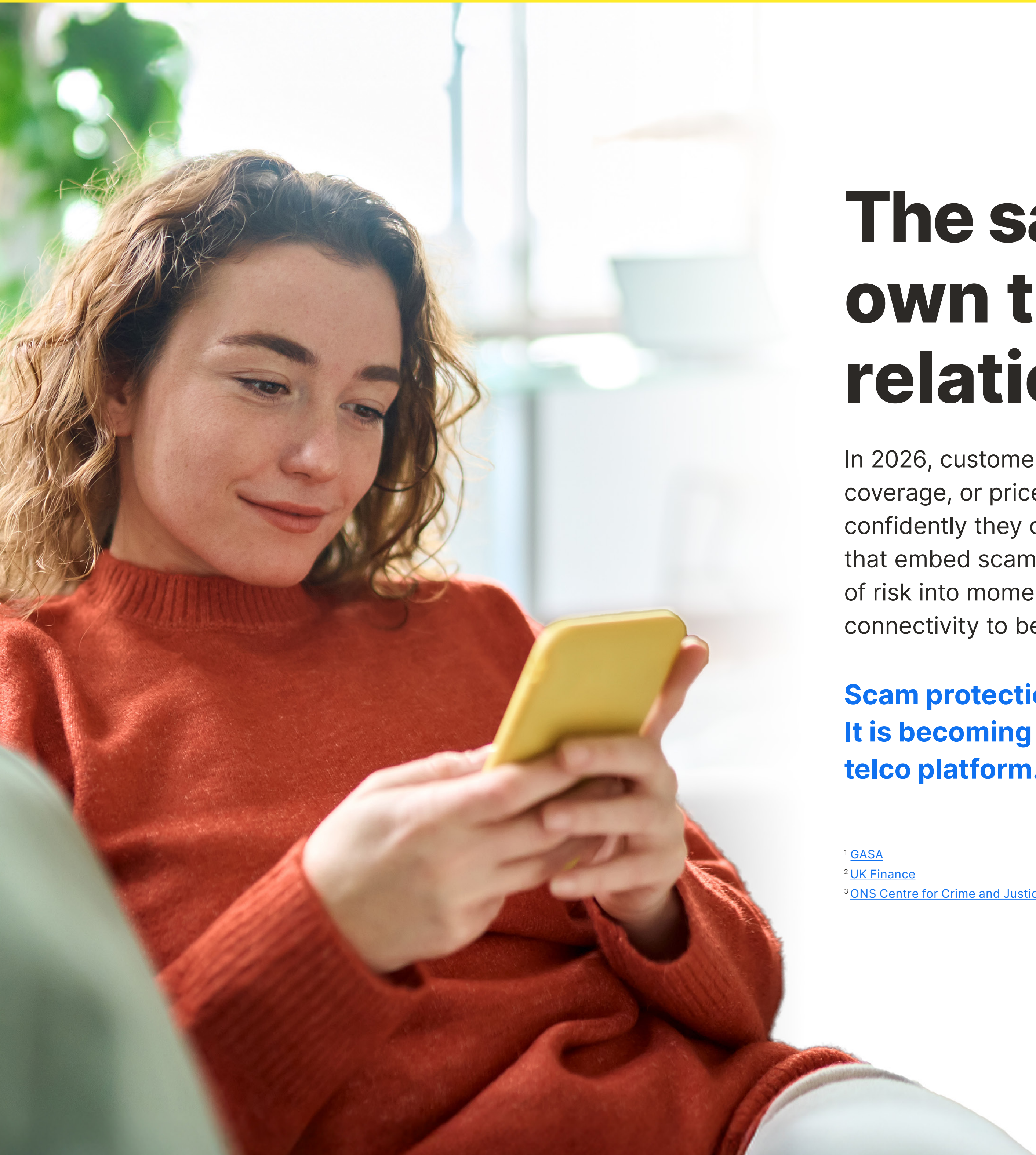
1. **Reframe protection as a trust proposition**
   Connect scam protection to the brand promise — safer customers, safer families, safer digital lives — not just another security add-on.

2. **Embed protection into the app**
   Make the telco app the place customers go for safety guidance, not only account management.

3. **Design around real scam moments**
   Build experiences around the questions customers actually ask: Is this message a scam? Has my data been exposed? What do I do next?

4. **Localize the experience**
   Use local scam trends, language, and threat intelligence to make protection feel timely and personally relevant.

5. **Choose flexible integration paths**
   Balance speed to market with long-term platform control — through SDKs, APIs, white-label UI, widgets, or single-page applications.



The safest telco will own the stronger relationship

In 2026, customers will not judge telcos only by speed, coverage, or price. They will judge them by how confidently they can live their digital lives. The operators that embed scam protection can help turn moments of risk into moments of trust — and move beyond connectivity to become trusted digital safety partners.

Scam protection is not just another feature. It is becoming the trust layer of the modern telco platform.

[1] GASA
[2] UK Finance
[3] ONS Centre for Crime and Justice

norton™