www.pipelinepub.com
Volume 22, Issue 1

Always On Means Mobile Customers Are Always At Risk

By: Dan Carella

Today, mobile devices are where consumers bank, shop, work, socialize, and manage their most personal information. As a result, telecom providers find themselves in a unique position of digital trust — and that responsibility is shifting in a critical way. While device- and network-level security has never been stronger, fraudsters are sidestepping these defenses to target the weakest link: human behavior.

This pivot in fraud strategy is one telecom leaders should monitor because it has the potential to have an outsized impact on consumer trust and loyalty. Understanding the mechanics of attacks designed to manipulate customers and devastate operations is critical for providers looking to develop the next generation of risk management and consumer engagement.

Constant connection to attack surfaces

Recent data concerning Americans' use of mobile devices and networks clearly illustrates why it has become a preferred attack vector. Consider this:

- Nearly all (98%) Americans now own a smartphone
- They average more than five hours a day on their devices
- More than half (53%) of consumers report being targeted with email, text, phone or online scams — all of which are mobile channels

Cybercriminals now have an ever-expanding attack surface with a highly engaged user base—offering a steady stream of personal data that can be weaponized for fraud. Unlike other telecom security challenges, such as SIM swaps or number port-out fraud, today's new attacks don't require breaching a network's cybersecurity defenses at all. Instead, they rely on social engineering techniques designed to manipulate mobile users into willingly handing over data or granting approvals.

This change in tactics marks a significant shift. It means the most sophisticated security protocols and fraud detection solutions can potentially be bypassed by a single, well-crafted text message or convincingly spoofed call. For telecom providers, it raises significant questions about how to protect customers when the threats are social and psychological in nature — rather than technical.

Current mobile scams to watch

While scams targeting mobile users aren't new, the tools used by today's criminals are, and they're alarmingly effective. Fraudsters are leveraging advances in AI, automation, and data mining to launch attacks that are frighteningly personalized, realistic, and scalable — and often indistinguishable from legitimate communications.

The result? Anyone can fall victim to these increasingly complex and convincing scams.

There are behavioral reasons that make mobile users particularly attractive targets. Mobile engagement is frequently quick and driven by impulse. Compounding the issue, consumers often check their phones while on the go or multitasking, making them more likely to open a link or respond to a message with less scrutiny. And because mobile devices are increasingly used to approve financial transactions, reset passwords, and complete multi-factor authentication, if a fraudster successfully gains access, they typically have "the keys to the kingdom" of the victim's entire digital life.

The following are some of the new twists on mobile scam trends telecom professionals should monitor this year.

Voice cloning and deepfake vishing: Fraudsters can now use off-the-shelf, AI-powered deepfake technology to replicate a family member or other trusted figure's voice. Known as voice cloning, the fake audio can be used to trick targets into revealing sensitive information, changing account access requirements, or approving fraudulent financial transactions. Some examples of voice cloning scams have

involved impersonating a bank representative or a loved one in need — creating a sense of urgency that pressures the victim into taking quick action.

Spoofed caller ID and smishing: Unfortunately, spoofing technology has become a criminal commodity. As a result, fraudsters can easily make it seem as if their calls are coming from legitimate phone numbers — including customer service lines of the consumer's telecom provider. Combined with deceptive text messages called "smishing" (SMS phishing), they can quickly deliver a very convincing one-two punch that uses the spoofed phone number to build

trust and override any initial suspicions. Victims often don't realize they've been duped until well after their accounts have been compromised.

The "say yes" scam: This is a subtle but effective scheme where scammers open a call with a question designed to elicit a simple "yes" from the victim. Whether they start by asking "Can you hear me?" or verifying their name, they're preying on the human impulse to respond. And while it may seem harmless, the scammers are waiting to record your voice saying that single word — because they can then use the recording to authorize fraudulent transactions or misrepresent your consent on voice-authenticated systems.

Malicious QR codes: QR codes have increasingly become targets for malicious schemes — and for good reason: 73% of consumers scan them. Leveraging that trust, scammers now create fake QR codes and place them on public infrastructure where one might expect to see them, such as parking meters or restaurant menus. When an unsuspecting consumer scans it to make a parking payment or access a menu, they instead access a fraudulent website or inadvertently install malware onto their device.

Wrong number engagement scams: This kind of scam starts with a seemingly harmless wrong number text. By replying, however, the victim confirms to an attacker that a mobile number is active and tied to a person willing to engage. These scams then escalate when the attacker starts preying upon the victim's instinct to be polite or helpful. Ultimately, the scammer's goal is to steer the interaction into an opportunity for financial exploitation — whether gathering enough information to commit identity theft, asking for money, or presenting a fake investment ploy.

Realigning customer protection approaches

As central enablers of consumers' mobile experiences, telecom companies play a key role in reducing risks that come with them. If customers cannot feel safe on their devices, their trust in their telecom providers can be quickly eroded.

Telecom providers should evaluate their customer protection efforts across three key areas to ensure they align with today's mobile risk trends.

1. Consumer empowerment: Turning customers into the first line of defense

As threat actors increasingly target human behavior rather than network infrastructure, consumer education moves to the forefront as a powerful security layer. Telecom providers no longer have the option to wait until a cyber event occurs. Instead, they must engage customers proactively with practical and timely resources that help them recognize suspicious activity — thereby cultivating them as allies in the fight against scammers.

What does this engagement look like? It could be push notifications that alert customers to active scam campaigns; easy-to-consume educational articles regarding mobile threat awareness; and tools that enable customers to report and blocksuspicious calls as they happen. The goal is to transform consumers from passive recipients of fraud protection into active participants in their own security.

Self-service tools can go a long way in supporting this goal by empowering customers to quickly lock SIM cards, change passwords, or verify account activity from a convenient dashboard. A key consideration is to remove friction when it matters most. A combination of education and control builds loyalty by showing customers investment in their digital safety.

2. Systemic enhancement: Making security a visible value-add

Security shouldn't always be a back-end function. In fact, making it a visible part of the customer experience sends a strong signal about a telecom's priorities.

Call verification tools, advanced spam call blocking, and fraud alerts are all examples of how a telecom can evolve from a mere service provider into a customer's trusted digital partner. This visibility reinforces the idea that a telecom's true value extends beyond connectivity to include safeguarding the experience.

Providers can bundle these protections as part of a premium service package or loyalty program, turning security into a differentiator that increases the perceived value of the relationship. As mobile scams become more sophisticated, the ability to authentically promote consumer-focused protections becomes a competitive advantage, especially for those security-minded prospects who are concerned about digital safety.

3. Partner alignment: Strengthening standards and credibility

In today's world, technical capabilities and price can no longer be the only considerations when evaluating potential vendors and partners. Cybersecurity practices and reputation are key factors telecom providers should weigh heavily when assessing vendors. Such an approach requires digging more deeply into their cybersecurity practices, understanding how potential partners handle customer data, and knowing exactly what their incident response plans entail. When telecom providers hold partners to their same security standards, they're better prepared to respond to situations where supply chain vulnerabilities impact customer safety.

When telecoms work with partners known for reliability and security, it strengthens their positioning as a trustworthy provider. In an environment where consumers and small businesses are increasingly aware of their need for cyber protection, earning a reputation for guarding customer data can be a differentiator that works in your favor.

At the same time, a brand's reputation can be quickly damaged when an event happens — and customers won't necessarily differentiate between their telecom providers and their telecom providers' vendors. Sound partner due diligence not only protects telecom customers but also the organization's brand and long-term credibility.

Protecting the mobile future

Today's reliance on mobile devices means they're only becoming more central to consumers' lives — and therefore, they'll remain ever-more attractive targets for threat actors. Telecom providers that empower consumers, strengthen systemic defenses, and build secure partner ecosystems will not just reduce fraud losses but build deeper customer loyalty.

Today's consumers are always connected, and the telecom industry can play an important role in ensuring "always on" doesn't mean "always at risk." In a world where customer trust is a coveted competitive asset, providers that proactively protect customers will be best equipped to earn that trust.