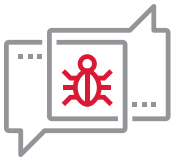
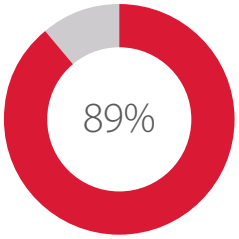


Fraud involving SMS interception is one of the most widespread attacks related to banking services. By intercepting incoming SMS confirmation messages and sending commands, attackers can easily obtain access to a client's online bank account. Research shows that ***in 89% of cases, an attacker can intercept SMS messages.***



Statistics: Primary Security Threats for SS7 Cellular Networks, Positive Technologies, 2016

Banks are racing to converge with other industries. In the digital economy, consumers need more than traditional financial providers can offer. Online banking and cloud services, personalized offers, AI-powered support—all these have become table stakes for banks trying to remain market leaders. At the same time, banks are performing radically new functions, such as acting as marketplaces for other companies (insurers, airlines, and media) and providing government services.

Telecom services are increasing in popularity: many banks are choosing to launch a mobile virtual network operator (MVNO) under their own brand and provide cellular services. Banks can choose from multiple MVNO models, from light MVNO to full MVNO, creating a virtual operator with its own rate plans, pool of subscriber numbers, and billing.

Creation of a bank-branded MVNO offers several major business opportunities.

+ **Improved client retention thanks to bundling.** Bundled services are much cheaper, easier to manage, and "stickier"—clients are reluctant to leave due to the difficulty of switching.
+ **More clients and per-client revenue.** A bank acting as MVNO can offer related financial services (such as better loan rates for clients who sign up for the bank's MVNO), which draws in new clients and drives existing ones to spend more.
+ **Savings on mobile for banks.** Rising rates for mobile services have forced many banks to look at reducing SMS notifications in favor of push notifications to clients. As a medium-term solution, creating an MVNO can offer substantial cost savings on sending SMS notifications.

But converging technologies can have downsides too. Every new service enlarges the attack surface vulnerable to hackers. **When launching MVNOs, banks must step up and become fully responsible for security, since they now face all the same risks as traditional telecom operators.** As described by the experts at Positive Technologies, these threats fall into three main categories:

+ **Fraud.** SMS messages can be intercepted in order to obtain full access to clients' online bank accounts, transfer client funds, apply for loans, create fictitious clients to withdraw money, and more.
+ **Information leaks.** Valuable client information (subscriber location, voice calls, SMS messages, banking history) can be disclosed or stolen. This information can be then sold or used to bypass bank anti-fraud systems.
+ **Downtime.** Service operability may be targeted in attacks on the operator network (such as DoS attacks on telecom systems and subscribers).

SECURING MOBILE VIRTUAL NETWORK OPERATORS:
THE POSITIVE TECHNOLOGIES SOLUTION

KEY BENEFITS:

Better awareness of the state of network security

Reduced fraud

Rapid incident investigation

Automation of the security management process

Regular reporting to strengthen decision-making and flexible risk management

Strong protection of client data

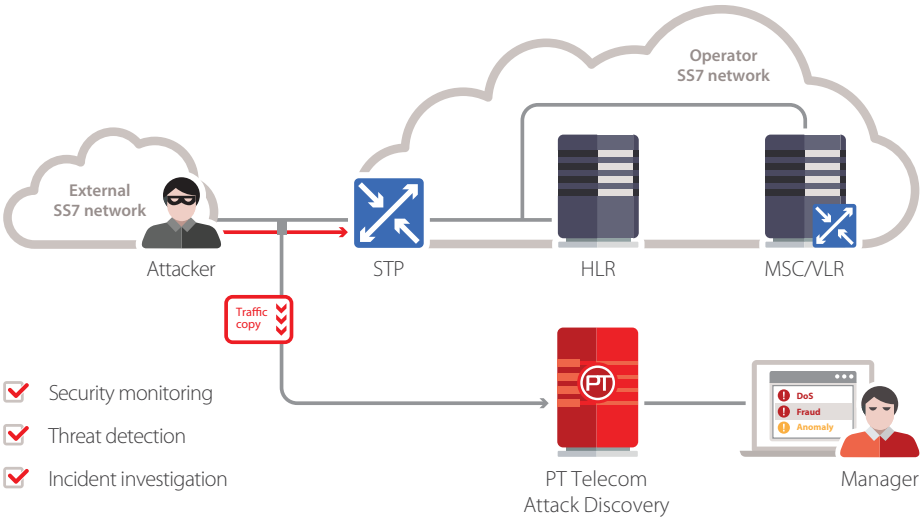
Cyberattacks on mobile operators, including virtual ones, are possible in large part due to flaws in the signaling networks that form the backbone of all of today's telecom infrastructure. The telecom industry may seem high-tech, but signaling networks—and especially the critical SS7 network—were designed over 30 years ago and have barely been changed since.

THE POSITIVE TECHNOLOGIES SOLUTION FOR MVNO CYBERSECURITY

When deploying an MVNO, banks must take note of these threats and make sure their networks are safe for clients' personal data and savings. This demands an in-depth approach: **regular audits** of network security are necessary in order to mitigate risks. For timely detection and prevention of attacks, it's important to use **additional protection solutions** for 24/7 traffic monitoring, attack blocking, and more.

To help its clients design a thoughtful strategy for combating telecom security threats, Positive Technologies offers **PT Telecom Security Assessment.** In this comprehensive assessment of operator network security, Positive Technologies experts identify critical security flaws in signaling networks, pinpoint potential attack vectors, and develop detailed recommendations for preventing possible intrusions.

Network operators can react to threats more effectively thanks to **PT Telecom Attack Discovery** (PT TAD). This system from Positive Technologies monitors and protects the perimeter of the signaling network, detecting anomalous activity in real time. PT TAD combines powerful attack detection capabilities with robust analytics, making it simple and intuitive to assess the current state of security. PT TAD aggregates security information and generates detailed reports for quick reactions to threats.



MVNOs can keep all their bases covered. By using PT Telecom Security Assessment and PT TAD in tandem, they can build out a vulnerability management process, minimize the risk of incidents, and defend the operator and subscribers from all types of cyberattacks.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com