EXECUTIVE OVERVIEW

The Attack Surface in Your Pocket—and How Scattered Spider Socially Engineers Their Way Inside

Explore how financial institutions can protect themselves from the growing threat of mobile-first attacks

iVerify.

The Rise of Mobile-First Threats

Mobile Exploitation

E-criminals have shifted tactics to focus on the least protected endpoint: mobile. They leverage identity, SMS, SIM swap, and voice as primary attack vectors.

No Barrier to Entry

Low cost and effective social engineering attacks have overtaken costly and difficult-to-obtain remote exploit chains.

Impersonation Increasing

Scattered Spider has achieved a staggering 67% success rate in impersonating help desks to execute their attacks.

> The rise of mobile-first threats has fundamentally shifted the cybersecurity landscape, requiring financial institutions to rethink their security strategies and prioritize the protection of their mobile-enabled workforce and infrastructure.

iVerify.

The Attack Surface Shifted to Your Employees' Pockets

- Employees approve transactions, reset MFA, and access systems on personal devices
- 82% of organizations use BYOD, yet most devices have no enterprise security
- SMS, messaging apps, and voice bypass traditional endpoint defenses
- Identity flows replaced endpoints as the primary attack path
- SIM swaps and MFA spoofing collapsed SMS-based trust models

iVerify.

Personal & Corporate Security: The Boundary Dissolved

94%

of Fortune 50 companies have employee identity data exposed as a consequence of phishing attacks.

78%

of employees have had their corporate credentials exposed in a breach or leakage

67%

of employees use personal devices for work

THE GAP

Traditional controls still center on desktops and work email.
Attackers follow the path of least resistance.

iVerify.

Financial Institutions Are In the Crosshairs

Financial institutions are prime targets for cybercriminals due to the significant financial impact of data breaches in the industry. With average breach costs reaching $6.08 million and over $16.6 billion in losses reported to the IC3 in a single year, the financial services sector faces substantial risks.

iVerify.

The Evolving Criminal Landscape

Criminal Federation:
Scattered Spider + LAPSUS$ + ShinyHunters

An alliance of cybercriminal groups that have banded together, dividing labor between access, data theft, and extortion.

Division of Labor:
Access → Data Theft → Extortion

This federation streamlined their attack chains, becoming faster, polished, and repeatable.

Threat Shift:
Scattered Spider Leverages Mobile-First Tactics

Scattered Spider built their playbooks around mobile-first exploitation, leveraging identity, SMS, and voice as primary attack vectors.

> The emerging criminal federation between Scattered Spider, LAPSUS$, and ShinyHunters represents a formidable threat to financial institutions, with their division of labor, faster attack chains, and mobile-first tactics.

iVerify.

SIM Swaps & SMS: Your Front Door is Open

>$100M

FBI-tracked SIM-swap losses since 2022
United States Only

1,055%

increase in unauthorized SIM swaps
UK: 289 cases (2023) → 3,000 cases (2024)

THE REALITY

If you rely on SMS for critical authentication or recovery, you've made telecom call centers part of your security perimeter.

iVerify.

Why This Matters Now

Social Engineering at Scale

Threat actors automate vishing, smishing, and impersonation to compromise accounts.

Phones Extend the Attack Surface

Employees approve transactions, reset MFA, and access systems on personal devices.

Identity as an Entry Point

Attackers bypass devices entirely by exploiting MFA resets and access flows.

BYOD Visibility

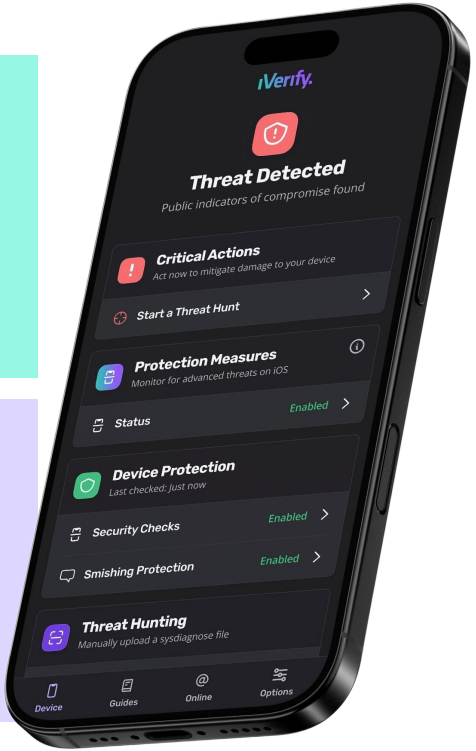
Most personal devices have little to no enterprise security.

Endpoint Exposure

SMS, messaging apps, and voice sit outside email and endpoint defenses.

SMS Trust is Fragile

SIM swaps and spoofed MFA break SMS-based authentication.



iVerify.

CISO Checklist: Securing the Mobile-First Frontier

- [x] **Retire old perimeter thinking**

  Shift security focus from outdated perimeter-based approaches to address the mobile-first reality

- [x] **Remove/monitor SMS**

  Minimize reliance on SMS for authentication and monitor for SIM-swap indicators

- [x] **Refresh training & IR playbooks**

  Update security awareness training & incident response plans to address the unique challenges posed by mobile-first exploitation

- [x] **Lock down identity flows**

  Implement stronger authentication and access controls for help desk agents to prevent impersonation

- [x] **Protect all employees**

  Extend mobile security measures beyond just executives to encompass admins, help desk, and other privileged users.

- [x] **FS-ISAC peer collaboration**

  Engage with industry groups like FS-ISAC to stay informed on the latest mobile-first threats and best practices

iVerify.

Contact iVerify for a Custom Threat Briefing

Stay ahead of the evolving mobile-first threats posed by cyber criminal groups like the Scattered Spider federation.

EMAIL: info@iverify.io WEBSITE: iverify.io

iVerify.