Kaseya®

The rise of phishing: Why MSPs must outpace smarter cybercriminals

Phishing is no longer a numbers game. Today's cybercriminals rely on intelligence rather than volume. They use AI to craft precise, personalized and highly convincing attacks with near-perfect accuracy.

AI-generated phishing, impersonation and social engineering campaigns are evolving faster than end users can adapt. While even well-trained end users struggle to keep pace, the responsibility for stopping these attacks has shifted squarely to MSPs. **More than 60% of MSPs report that most or all clients rely on them for cybersecurity guidance.**

Read on to learn how to stay ahead of smarter cybercriminals and better protect clients with AI-powered security solutions.

The rising impact of cyberattacks on MSP clients

The threat isn't theoretical.

- In 2025, 44% of MSPs reported that at least 10% of their clients experienced a cyberattack.
- Even more concerning, 8% reported that between 41% and 80% of their client base was impacted.

As cyberthreats grow more sophisticated and frequent, clients want partners who can anticipate threats, automate defenses and eliminate blind spots before attackers exploit them.

Top client IT needs for 2026

- AI & automation services – 48%
- Security services – 42%
- Backup and recovery – 36%
- Endpoint and network management – 34%

The MSP revenue reality: Demand vs. delivery

While demand for AI and advanced security is rising rapidly, **AI and automation account for just 13% of MSP revenue in 2025**. Most MSP revenue remains concentrated in traditional services.

At the same time:

- Core services such as EDR, endpoint security, patch management and email security have become baseline expectations.
- Advanced services such as AI-driven detection, SIEM, SOC and compliance remain underadopted despite increasing demand.

This gap represents both risk and growth opportunity for MSPs.

Where AI changes the game for MSP security

In an era of AI-powered attacks, defending manually is no longer sustainable. AI-driven security enables MSPs to:

- Detect and respond at machine speed
- Identify anomalies traditional tools miss
- Gain visibility across the entire ticket and threat lifecycle
- Scale protection without scaling headcount

The opportunity ahead: From protection to differentiation

Rising interest in advanced detection and EDR indicates a broader market shift toward intelligent security.

Forward-thinking MSPs are:

- Packaging premium, AI-driven security offerings
- Expanding into advanced detection and response
- Increasing client retention through proactive protection
- Elevating their role from reactive support to strategic advisor

Staying ahead of smarter cybercriminals

Cybercriminals will continue to innovate, and end users will continue to face increasingly convincing deception. As an MSP, you must move faster than attackers. You need a proactive, AI-driven security approach to detect threats early, respond quickly and protect clients more effectively.

Equip your MSP with cutting-edge cybersecurity solutions to respond to AI-powered threats and unlock new growth opportunities.

Step into the next evolution of managed security.

Learn more