

THE HIDDEN THREAT IN YOUR HELPDESK AND HOW TO STOP IT



YOUR HELPDESK IS A PRIME TARGET

There's a hidden threat lurking in your helpdesk: cybercriminals exploiting phone-based impersonation and social engineering to gain privileged access. Once inside, they can launch ransomware, steal sensitive data, or move money undetected until it is too late to recover. And it all starts with a seemingly routine phone call.

THE ATTACK: SIMPLE, EFFECTIVE, AND DEVASTATING

- A cybercriminal calls the IT helpdesk pretending to be an employee.
- They claim they have an urgent need—like a password reset or MFA bypass.
- The agent, eager to assist, processes the request after verifying employee details—many of which the attacker easily sourced from social media or data breaches.
- The attacker now has legitimate access to the employee's account—and potentially, the entire network.

With access in hand, the attacker can elevate privileges, exfiltrate data, disrupt operations, or unleash ransomware. This isn't hypothetical—it's one of the most common entry points for major security incidents.

BEYOND THE BREACH: THE REAL CONSEQUENCES OF ATTACKS



MGM Resorts lost over \$100 million in 2023 after a single impersonation call to their helpdesk triggered a ransomware. The breach caused a 9-day outage across 30 properties and the exfiltration of over 35M customers' PII.



Clorox suffered a major breach in 2023 after attackers tricked a helpdesk agent into granting access. Operations were disrupted and manufacturing halted — total impact of \$49M in remediation and \$380M in total damages.



SHORTER CALLS • BETTER SECURITY • EASIER BANKING

MAKE YOUR HELPDESK YOUR FIRST LINE OF DEFENSE

Authenticate callers by voice—passively and invisibly during the conversation.

HOW ILLUMASHIELD™ WORKS



The agent answers the call as usual.



The IllumaSHIELD™ system analyzes the caller's voice in the background.



If it matches the voiceprint, access is allowed.



If it doesn't match, or detects anomalies, the system flags or blocks the request.

NO PINS. NO CODES. NO SECURITY QUESTIONS. JUST THE VOICE.

SECURITY WITHOUT FRICTION

- Removes identity validation burden from agents
- Stops attackers—even if they spoof numbers or steal credentials
- Seamlessly integrates into existing helpdesk workflows
- Enables fast, secure, and confident resolution

THE HELPDESK AS A CRITICAL SECURITY CHECKPOINT

IT leaders must rethink the role of the helpdesk—from a support hub to a frontline security checkpoint.

IllumaSHIELD™ empowers your team to:

- Block voice-based social engineering attacks
- Eliminate reliance on guessable or public information
- Maintain employee satisfaction without sacrificing security

ABOUT ILLUMA

Illuma, based 100% in the US, is the leader in voice authentication and fraud prevention. Its flagship solution, IllumaSHIELD™, uses AI-driven voice biometrics to provide secure, seamless authentication—reducing fraud and boosting authentication efficiency. It has been featured at top FinTech events and has earned industry recognition, including back-to-back 'Best of Show' awards at Finovate.



SEE ILLUMASHIELD™ IN ACTION! BOOK A DEMO TODAY AT [ILLUMA.CX](https://illumacx.com)