Specops White Paper

Securing the Service Desk

How to close the verification gap in 2025
Risks, case studies, and defenses

Specops Software, an Outpost24 company, is the leading provider of identity management and authentication solutions.

SPECOPS
AN OUTPOST24 COMPANY

What's inside?

Executive summary

An impersonated phone call. That's all it took for attackers to infiltrate Marks & Spencer's systems in April 2025, triggering a ransomware attack that forced the British retail giant to shut down its operations and **lose $400M in profits**. The entry point? Not a sophisticated zero-day exploit or advanced persistent threat, but threat actors who impersonated an M&S employee to trick a third-party help desk into resetting a password.

Service desks have evolved from internal support functions into prime hunting grounds for cybercriminals. Armed with AI vishing technologies and carefully crafted social engineering scripts, attackers are systematically targeting the human element of cybersecurity. They're weaponizing people's instinct to help, turning IT staff into accidental accomplices who hand over password resets, disable multi-factor authentication, and grant privileged access. Unfortunately, too many organizations are leaving their staff open to these threats.

Traditional technical defenses that cost thousands to implement can be bypassed with a convincing voice, a few publicly available details, and exploitation of predictable human psychology. It's a simple but effective attack methodology that demands immediate attention.

Through forensic analysis of recent high-profile breaches, we'll show you exactly how verification failures cascade into operational disasters. We'll also share the defenses you need to have in place: verification protocols, phishing-resistant MFA implementations, and vendor controls.

Whether you're aiming to safeguard identity workflows, manage service desk operations, or evaluate security tools, this paper will help turn your service desk from a vulnerability into a defensive asset. Make sure your service desk is prepared in case the phone rings and the caller has bad intentions.

Rise of social engineering against service desks

Today's attackers have abandoned the shotgun for the sniper rifle, trading mass email campaigns for precision strikes against the humans who control access to your most sensitive systems. Why hack through layered defenses when you can simply ask someone for a password?

The anatomy of modern social engineering

Picture this scenario: an attacker spends thirty minutes on LinkedIn, identifies your IT manager, then discovers she recently posted about working late on a system migration. They call your help desk at 11 PM claiming to be the manager, saying they're locked out and desperate to complete critical work before the morning deadline. The night-shift agent, eager to help a stressed colleague, bypasses normal verification procedures. Within minutes, the attacker has password resets, MFA tokens disabled, and a foothold in your network. Attackers have weaponized the desire to help, the pressure to work efficiently, and the assumption that people are who they claim to be.

Why service desks are vulnerable

Service desks exist in a perfect storm of conflicting pressures. Agents must move fast to maintain service levels, yet verify thoroughly to maintain security. They're often outsourced and handle requests from people they've never met. Performance metrics can conflict with rigorous security practices, if agents are measured on resolution speed and customer satisfaction.

Meanwhile, attackers have industrialized their approach. They harvest employee details from data breaches, social media, and corporate websites. They craft personas complete with insider knowledge, urgency-driven narratives, and emotional manipulation techniques refined through thousands of attempts. **AI-powered voice synthesis technology** even allows them to clone executives' voices from publicly available recordings (that don't be need to very long – less than a couple of minutes. **Microsoft claim a person's voice can be cloned in just three seconds with the right tools**.

In many situations, the playing field isn't level – it's tilted decisively toward the attacker.

How a threat campaign plays out

Modern social engineering operates like a sophisticated marketing campaign with distinct phases. They often run several campaigns at the same, with automation helping to create a mass operation:

1

Reconnaissance phase
Attackers gather intelligence about your organization from publicly available sources like social media sites and your company website. They identify recent hires, org structures, and vendor relationships that create natural cover stories.

2

Pretext development
Armed with intelligence, they craft believable scenarios. Stories like the executive traveling internationally who needs urgent access, the new employee whose credentials haven't activated, or the vendor requiring immediate system access for critical maintenance.

3

Multi-channel execution
The actual attack doesn't have to be restricted to a single phone call. An email could create the initial narrative, after which a phone call adds urgency and emotion. A live chat session can provide more details. Each channel reinforces the others, creating a sense of legitimacy.

4

Exploitation and escalation
Success means getting hold of a password while bypassing MFA. From there, attackers can escalate their privileges and establish persistent footholds that enable large-scale data theft or ransomware deployment.

Service desk attacks: *Real-world case studies*

These incidents show the range of social-engineering outcomes and demonstrate that attackers don't need zero-day exploits when human processes are weak.

Marks & Spencer: *Active Directory exfiltration and ransomware*

What happened: In April 2025, attackers impersonated an employee and contacted a third-party service desk to obtain credential resets. With those credentials as a launchpad, they exfiltrated the AD database (NTDS.dit) and **deployed ransomware across M&S systems**, causing major disruption to online and in-store services and prompting multi-month remediation. **Scattered Spider are also rumored to have been responsible** for this attack and similar operations against other major UK retailers: Harrods and The Co-Op.

Techniques and failure points: The attackers used a credible pretext (possession of internal details and a local accent) to get a third-party help desk to reset privileged credentials. Key failures include reliance on easily discoverable directory attributes for verification, lack of enforced callback/corporate directory confirmation, and insufficient segmentation/AD protections to prevent NTDS.dit extraction once credentials were compromised.

Business impact: M&S disclosed major operational disruption with long recovery timelines. Public reporting estimated material profit impact and a drop in stock prices. There has been a protracted restoration of services (e.g., click & collect remained affected for weeks). The attack also raised regulatory and insurance complexity for the retailer.

Clorox: *"They just asked for the password"*

What happened: The 2023 intrusion that struck **Clorox has hit the news again in 2025**. The cleaning giant is seeking roughly $380M in damages, alleging that an outsourced help-desk vendor (Cognizant) gave attackers access by failing to verify callers, handing over passwords, and resetting MFA. Reporting includes quoted transcripts and the company's claims that simple verification failures enabled the cyber-attack. ▸

Techniques and failure points: According to the complaint and media coverage, attackers bypassed technical defenses by convincing help-desk agents to reset credentials and remove or re-enroll MFA. These actions were possible because identity checks were inadequate, and agents were permitted to perform sensitive operations without authenticated callbacks or multi-factor confirmation. The alleged route required minimal technical sophistication but exploited procedural gaps.

Business impact: The lawsuit describes halted manufacturing, supply-chain disruption, and hundreds of millions in lost sales and remediation costs. Beyond direct financial claims, the case highlights vendor management risk: third-party help desks can become single points of failure. Especially outsourcing service desks to vendors who don't have strong verification controls.

In many situations, the playing field isn't level – it's tilted decisively toward the attacker.

Third-party CRM breaches: *Google, Chanel, Air France, and KLM*

In mid-2025, several high-profile brands (**including Google, Chanel, and the Air France–KLM group**) fell victim to a coordinated series of breaches originating from a common source: third-party CRM and customer support platforms as part of a wider Salesforce-focused vishing/social engineering campaign.

- At Chanel, attackers used vishing and malicious OAuth apps to trick staff into linking a rogue application to the company's Salesforce environment. That access exposed U.S.-based customer names, emails, phone numbers, and mailing addresses, though no financial or highly sensitive data was compromised.
- Meanwhile, Google's internal threat intelligence revealed that attackers posing as IT support impersonated helpdesk staff, convinced employees to verify login credentials, and thus gained unauthorized access to customer data stored in Google's CRM systems.
- Around the same time, Air France and KLM disclosed a data breach caused by attackers compromising a third-party customer service platform. The attackers accessed personal customer data (such as names, contact details, loyalty numbers, and communication subjects) though credit cards, travel details, and passwords were not impacted.

MGM Resorts: *Service-desk call to full outage*

What happened: In September 2023, attackers used social engineering to gain a foothold that quickly cascaded into **widespread outages across MGM's properties**, affecting reservations, casino systems and guest services for days. Phone-based social engineering against support personnel was a key early step.

Techniques and failure points: The Scattered Spider group mixed reconnaissance (harvesting employee and vendor details), targeted phishing, and a live voice call that relied on weak caller verification. Agents were exposed to a convincing pretext and once credentials were obtained, attackers moved laterally into operational systems. The chain was short because human trust and routine support flows provided the path of least resistance.

Business impact: The breach produced multi-day service interruptions across casino operations and guest services, directly affecting revenue, bookings and customer experience. Even short outages in hospitality have outsized costs (lost revenue, chargebacks, remediation and PR) and long tail brand damage. MGM Resorts said it suffered a $100 million hit to its 2023 third-quarter results due to the cyber-attack.

Attackers don't need zero-day exploits when human processes are weak

How to defend the service desk

The challenge is clear: attackers have turned service desks into an initial entry point. But this same understanding reveals the solution. By transforming your service desk from a soft target into a hardened control point, you can flip the economics of social engineering attacks. What currently takes attackers minutes can be turned into weeks of preparation and multiple failed attempts – then giving up. Some will move on as soon as they realise strong security measures are in place.

A three-pillar defense strategy

Pillar 1: Process and policy

Your first line of defense isn't technology: it's process design that removes dangerous decisions from individual agents. This means establishing non-negotiable verification requirements for any action affecting credentials or multi-factor authentication. No exceptions, no shortcuts, no matter how convincing the caller or urgent the request.

Central to this approach is the authenticated callback protocol: agents must call back using phone numbers sourced directly from your corporate directory, never numbers provided by the caller. This single requirement neutralizes most social engineering attempts, as attackers cannot control your corporate phone system.

Equally critical are scripted workflows that agents see in real-time, with explicit confirmation checkpoints before any sensitive action. These scripts remove improvisation from high-risk decisions, ensuring consistent security posture regardless of which agent handles the call or how persuasive the caller might be.

Pillar 2: People and training

The best policies fail without proper implementation. Your agents need regular, realistic training that goes beyond generic phishing awareness to address the specific techniques targeting service desks. This means role-specific exercises featuring executive impersonation, urgent financial requests, and vendor emergency scenarios – the actual pretexts attackers use.

Effective training programs include recorded call reviews and post-exercise debriefs that transform mistakes into learning opportunities. The goal isn't to blame agents for falling for sophisticated attacks, but to build organizational muscle memory that makes suspicious requests immediately recognizable.

However, training doesn't solve the problem alone, and it's not fair to put the whole responsibility on the shoulders of service desk agents. They need help from their organizations.

Pillar 3: The right technology: Enforced verification

Technical controls eliminate the guesswork that attackers exploit. Integration between your phone system and identity directory allows agents to see authoritative contact information and recent authentication history instantly. Caller ID spoof detection and risk scoring for inbound channels flag suspicious calls before agents even begin interaction. Automation is crucial for consistency and speed. When verification workflows are built into agent tools and require explicit confirmation before proceeding, you eliminate the human tendency to take shortcuts under pressure. Failed verification should automatically trigger escalation, removing the option for agents to override security protocols.

Traditional knowledge-based questions (mother's maiden name, last four digits of Social Security number) should never be primary verification methods. This information is often available in data breaches or can be discovered through social engineering. Even SMS message are vulnerable to exploitation. Phishing-resistant multi-factor authentication should be mandatory. This might include hardware tokens, push notifications to registered devices, or corporate app confirmations that prove device possession – methods that cannot be easily bypassed through social manipulation. Requiring several factors in combination is the most secure tactic.

Securely verify your password resets — every time.

Specops Secure Service Desk transforms a vulnerable touchpoint into a layer of reliable security. By enforcing multi-factor authentication through trusted providers like Duo, Okta, and PingID, our solution ensures that every password reset and account unlock requires genuine user verification. Never knowledge that can be easily researched online. Your agents gain the confidence to handle high-risk calls securely, while maintaining fast resolution times through streamlined verification processes.

Don't let your service desk become the weak link that costs your organization millions in ransomware damage and recovery. **Schedule a live demo today** and see how Specops Secure Service Desk can protect your agents, secure your users, and safeguard your organization from the social engineering attacks that are targeting service desks worldwide. Your cybersecurity is only as strong as your most vulnerable process – make sure this one is secure.

Try Secure Service Desk

Don't let your service desk become the weak link that costs your organization millions in ransomware damage and recovery.

Five takeaway actions

As part of putting the three-pillar strategy into place, these five steps will materially reduce the likelihood that a single social-engineering call becomes a full-scale breach.

1. Make verified callbacks mandatory for all credential and MFA changes — source the callback number from your directory, not caller ID.
2. Standardize and display scripted verification flows for agents; force escalation when verification fails.
3. Require phishing-resistant MFA for account recovery and all high-risk tasks.
4. Run role-specific vishing simulations quarterly and use recordings for remediation and coaching.
5. Enforce vendor parity: require third parties to implement identical verification controls such as **Specops Secure Service Desk** and audit them regularly.

Try Secure Service Desk