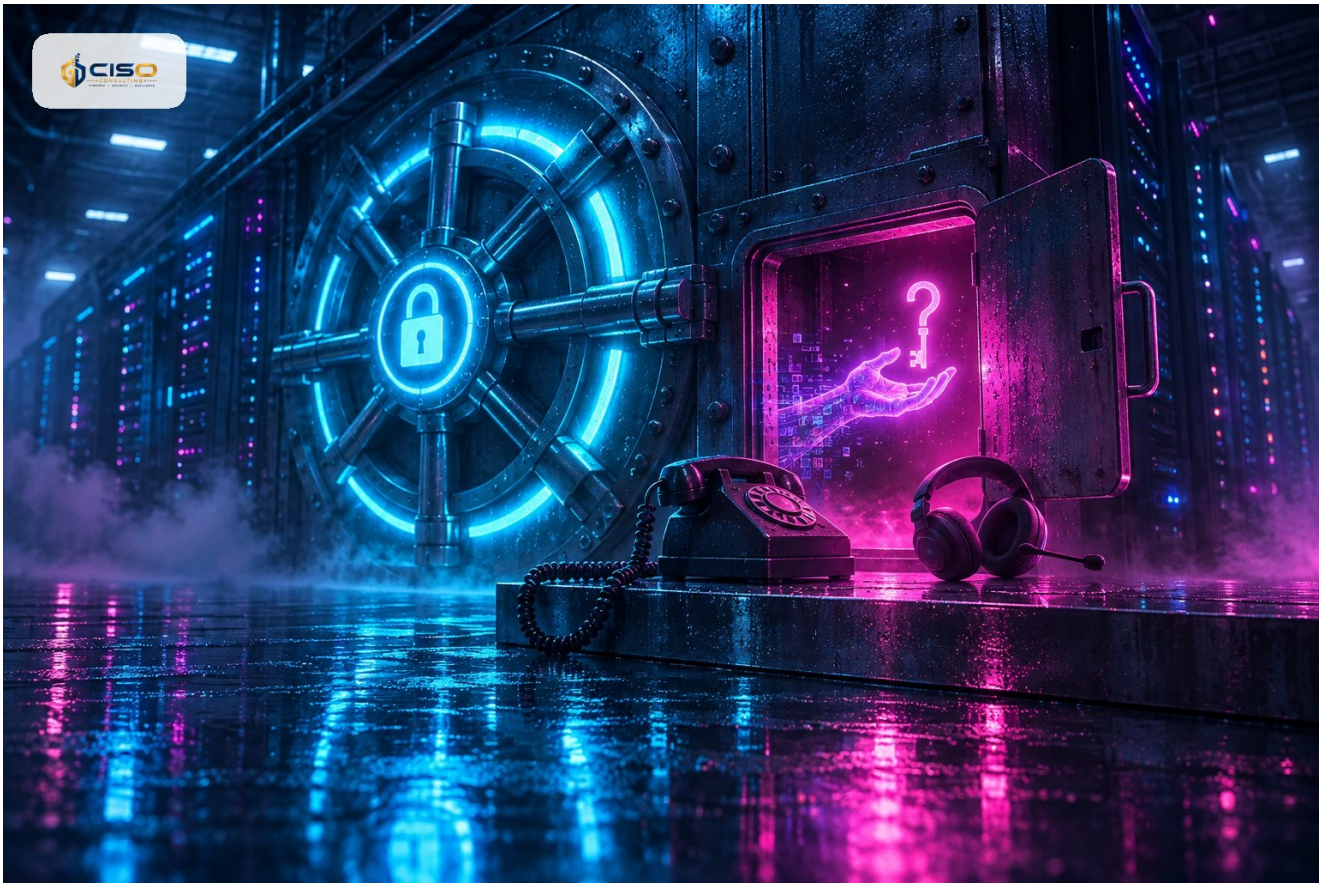
Service desk password resets: close the gap that bypasses MFA



A sponsored article argues that knowledge-based checks at the service desk undermine strong login controls. It says social engineering and AI make account recovery a prime target and calls for consistent verification.

- Account recovery at the service desk can bypass MFA and conditional access if it relies on questions such as a manager's name or department.
- Attackers can collect answers from LinkedIn, company sites, social media and leaked data.
- Groups such as Scattered Spider impersonate employees to obtain password resets or new MFA device registrations.
- The article cites a 2025 Gartner survey (62% of organizations hit by a deepfake social engineering attack) and Verizon's 2026 DBIR (voice and text social engineering 40% more successful than email

phishing).

- It recommends mandatory verification before sensitive changes, agent training and secure self-service recovery. Note that the article is sponsored by Specops Software.

The gap

Many organizations have strengthened employee logins with multi-factor authentication (MFA) and conditional access. A sponsored article from Specops Software points out that these controls lose value when the route for recovering access is weaker than the login itself. At many service desks, agents still confirm identity with knowledge-based questions, such as the name of the employee's manager or their department.

The article notes that such details are easy to collect from professional profiles, company websites, social media and leaked data. It also observes that NIST's digital identity guidelines no longer accept security questions as an authentication method.

Why it is getting worse

The article says groups such as Scattered Spider target the service desk, impersonating employees to obtain password resets or the registration of new MFA devices. Generative AI can make the stories more believable and even imitate voices. It cites a 2025 Gartner survey in which 62% of organizations reported a deepfake attack involving social engineering or automated processes, and Verizon's 2026 DBIR, which found texts and voice calls 40% more successful than email phishing.

The conclusion is that agents should not be asked to judge how convincing a caller sounds. Verification should be a required step in the workflow, with training and clear permission to refuse or escalate.

Reading the source

The piece promotes the vendor's own product, so its claims should be weighed accordingly. The underlying control principle, however, is sound and independent of any product: recovery must be as strong as authentication.

What to do now

1. Review how your service desk verifies callers before password resets and MFA device registration, and stop using manager or department questions as proof of identity.
2. Make verification a mandatory, logged step in the workflow, using a channel the attacker cannot easily reach, not the agent's judgment.
3. Require additional approval or escalation for high-privilege accounts and for any request to register a new MFA device.
4. Train service desk staff on voice-impersonation and AI-assisted social engineering, and authorize them to

refuse or escalate.

5. Consider secure self-service recovery to reduce call volume, and test recovery procedures through internal social engineering exercises.