“Can you reset my password?” How a simple service desk attack cost Clorox $400 million

By Marcus White

Published: 2025-07-28 · Archived: 2026-04-12 02:20:43 UTC

Table of Contents

- “Can you reset my password?” How a simple service desk attack cost Clorox $400 million
- Clorox breach: Attack summary
- Clorox hack: How the service desk social engineering played out
- Specops analysis: What can we learn from the Clorox hack?


Hand holding a Clorox spray bottle

Table of Contents

- “Can you reset my password?” How a simple service desk attack cost Clorox $400 million
- Clorox breach: Attack summary
- Clorox hack: How the service desk social engineering played out
- Specops analysis: What can we learn from the Clorox hack?


picture of author marcus white

Last week, cleaning products giant Clorox took the unusual step of suing its IT services partner Cognizant for gross negligence. Clorox are alleging that the August 2023 ransomware attack they suffered came about thanks to an incredibly simple piece of human error. According to the complaint, hackers tied to the “Scattered Spider” group simply phoned Cognizant’s service desk and requested a password reset – and were given one.

We’ll walk through how this basic lapse led to serious consequences and share some practical hardening measures you can put into place.

Clorox breach: Attack summary

- **Who was targeted**: Clorox
- **Attack type**: Ransomware
- **Entry technique**: Service desk social engineering
- **Impact**: Operational disruption, $49 million in direct remediation expenses & $380 million in lost revenue
- **Who was responsible**: Hackers linked to the Scattered Spider group

On August 11th, 2023, attackers tied to the Scattered Spider group executed a social-engineering campaign against Cognizant’s Clorox service desk. They placed multiple calls in which they posed as locked-out employees

requesting password and MFA resets. Despite Clorox's clear, "straight-forward" reset procedures, the agent on the line bypassed the protocols. The caller wasn't verified, and they were given a new password.

Crucially, no notification emails were sent to either the impersonated employee or their manager. This basic alert could have tipped off Clorox's security team about the unauthorized changes. Worse still, the attackers repeated the same trick to compromise a second account belonging to an IT-security employee, instantly elevating themselves to domain-admin privileges and granting unfettered access to Clorox's core Active Directory environment.

Ransomware deployment

With valid high-level credentials in hand, the intruders disabled critical security controls, swept through the network to escalate privileges further, and deployed ransomware across key servers. This silently encrypted data and severed links between manufacturing, distribution, and IT systems. By the time Clorox detected anomalous activity and pulled the plug on affected systems, production lines were halted and order fulfilment ground to a standstill.

In the immediate aftermath, Clorox claimed there were delays in containment and a failure to shut down compromised accounts, compounding the damage during the critical first hours. Recovery efforts stretched for weeks, encompassing forensic analysis, credential resets, system restores, and vendor-led process overhauls.

In total, Clorox reports $49 million in direct remediation costs and $380 million in overall losses, including lost revenue from shuttered factories and disrupted supply chains.

Specops analysis: What can we learn from the Clorox hack?

Darren James, Senior Product Manager at Specops, said: "Ultimately, this lawsuit should be a wakeup call for all MSPs that provide IT help desk services to their customers. They need to take ownership of the user verification process, particularly regarding password or MFA resets. They should provide their customers with secure and flexible self-service solutions that can be used from any device, at any time, and from any location so there can be no exceptions made.

"For all other service desk calls, there should also be a mandatory verification process put in place. Having written procedures is one thing, but is the technology there to enforce a process? Or can the process be circumvented with a simple social engineering strategy? Failure to provide such services could leave an MSP open to similar litigation and reputational as well as financial penalties."

Is outsourcing the service desk risky?

It's estimated 50% of organizations outsource at least part of their service desk function. Outsourcing critical support functions can deliver cost savings and 24/7 coverage, but it can introduce risk too. Earlier this year, UK retailer Marks and Spencer's suffered a similar incident. Attackers phoned in posing as M&S employees and tricked staff at Tata Consultancy Services (M&S's long term IT helpdesk contractor) into resetting privileged credentials, gaining them unfettered access to the retailer's Active Directory environment.

To mitigate these risks, it's important to maintain strict SLAs that codify verification protocols, conduct frequent red team exercises on outsourced processes, and require transparent, real-time reporting of all high-risk activities. Only by enforcing strong verification processes at your service desk (even when it's run by a partner) can you ensure that your "frontline" defense remains a strength, not a vulnerability.

The key lesson here is the vulnerability of service desk agents to social engineering. It's vital to lock down service-desk permissions so that agents cannot reset credentials for admin or IT-privileged accounts without a secondary approval workflow.

To lock down your service desk against social-engineering threats like those used by Scattered Spider, try Specops Secure Service Desk for secure verification, granular reset controls, and full audit trails. Give your agents the support they need – book a live demo.

Last updated on **November 11, 2025**

 picture of author marcus white

Written by

Marcus White

Marcus is a cybersecurity product specialist based in the UK, with 8+ years experience in the tech and cyber sectors. He writes about authentication, identity and access management, and compliance.

Related Articles

- **Securing the service desk: Interview with an OffSec expert**

  Securing the service desk has become a priority for many organizations, especially after the spate of social engineering attacks in the UK linked to Scattered Spider. Attackers know the service desk can be an easy way to bypass MFA and gain initial entry to a network, as agents without the right security tools are vulnerable…

  Read More

- **Scattered Spider service desk attacks: How to defend your organization**

  Scattered Spider is a disparate hacking collective that has surged to prominence by using sophisticated social engineering tactics. One of their key tactics is exploiting people – specifically, corporate service desks. They recently hit the headlines by allegedly carrying out a crippling ransomware hack on UK retailer Marks & Spencer (M&S). M&S Chairman Archie Norman…

  Read More

- **M&S ransomware hack: Service Desk & Active Directory security lessons**

  M&S (Marks and Spencers) are a cornerstone of British retail with over 64,000 employees – so it was a shock for many to see them laid low by a ransomware attack in April 2025. The retail giant fell victim to a significant cyber-attack attributed to the hacking group known as Scattered Spider. Attackers reportedly infiltrated…

  Read More
