ManageEngine
AD360

The anatomy of a high-profile social media breach

How a phone call and a stale insider account gave attackers the

keys to the world's most powerful megaphone

The numbers that shocked the social media industry

130+	$120K+	350M+
High-profile accounts hijacked	Crypto scam losses in hours	Reach of compromised accounts

The day verified voices were silenced

Help desk trusted an univerfied identity.

Overprivileged accounts gave unrestricted access.

Malicious changes looked like routine admin activity.

130 accounts hijacked. Global fallout.

Breach. Financial loss. Reputation damage.

What actually happened

STEP 1

Social engineering the help desk

In July 2020, attackers called a major social media platform's internal IT support, impersonating employees to obtain credentials for internal admin tools. They targeted employees with access to account management systems.

> **The vulnerability:** A convincing phone call was all it took — no technical exploit needed. Insider access was granted based on unverified identity.

STEP 2

Overprivileged and stale accounts exploited

With the stolen credentials, attackers accessed the platform's internal Agent Tools — a powerful admin panel. The compromised accounts carried far more privilege than their roles required, and some belonged to staff whose access had never been reviewed or scoped down.

> **The critical failure:** Over-provisioned accounts with unchecked privileges are indistinguishable from legitimate admin activity — no alerts triggered, no anomaly flagged.

STEP 3

Unauthorized changes made silently

Attackers changed recovery emails, disabled two-factor authentication, and locked real owners out — all through the admin panel, with no real-time monitoring in place to catch the activity as it happened.

> **The escalation:** Without change monitoring or audit trails, every malicious action looked like routine admin work. Security teams had no visibility until the damage was done.

STEP 4

Mass account takeover and public fallout

130 high-profile accounts — including Barack Obama, Elon Musk, Apple, and Jeff Bezos — were hijacked and used to broadcast a Bitcoin scam, stealing $120,000+ in hours.

The aftermath

- Global media panic
- Congressional hearings
- Arrest of a 17-year-old
- Permanent damage to platform trust and share price.

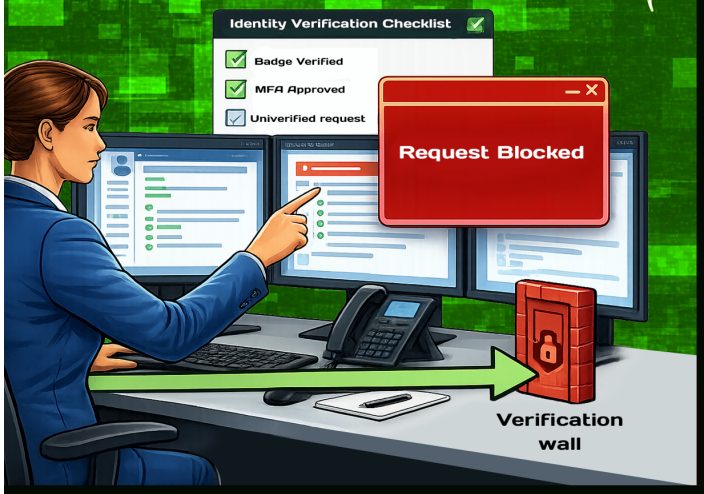
The root cause

130 high-profile accounts — including Barack Obama, Elon Musk, Apple, and Jeff Bezos — were hijacked and used to broadcast a Bitcoin scam, stealing $120,000+ in hours.

No malware. No hacking tools.
Just a phone call, invisible privilege, and nobody asking questions.

Keeping digital trust intact

Access is verified, scoped, and controlled.



Least privilege limits what any account can do.

Every critical change is tracked and alerted in real time.

Attack contained before it could spread.

No breach. No chaos. No headlines.

What if AD360 was deployed?

STEP 1

MFA and secure identity verification stop the phone call

AD360's security component, ADSelfService Plus, reduces reliance on help desk-based identity verification with MFA and secure self-service password reset. Sensitive access actions require verified authentication before credentials or permissions can be changed.

> **How it stops the attack:** Even if attackers successfully impersonated an employee over the phone, stolen credentials alone wouldn't grant access to internal admin systems.

STEP 2

Least privilege removes excessive access

AD360 enforces role-based access control and continuously identifies stale, inactive, and overprivileged accounts through automated access reviews and governance policies.

> **How it stops the attack:** Compromised accounts would have limited permissions instead of broad administrative control,dramatically reducing the attack surface.

STEP 3

Real-time AD change monitoring triggers instant alerts

Every change to account permissions, group memberships, recovery settings, and access roles is tracked and alerted on in real time — the moment it happens.

> **How it stops the attack:** The instant an attacker used stolen credentials to modify account settings, IT would receive an alert, flagging the unauthorized change before 130 accounts could be touched.

STEP 4

Access audits expose the problem before attackers do

ADManager Plus generates detailed access audit reports, showing who has access to what, when it was granted, and whether it's still justified. Routine audits would have surfaced the overprivileged support accounts and triggered a privilege review.

How it stops the attack: The structural vulnerability — over-provisioned accounts with unchecked access to admin tools — would have been identified and remediated during a standard audit cycle, well before any social engineering attempt.

The result:

- ✓ No social engineering loophole
- ✓ No over privileged accounts to exploit
- ✓ No silent unauthorized changes
- ✓ No mass account takeover
- ✓ No Bitcoin scam. No congressional hearing.

The business case

Without AD360 (The social media platform's reality)

- ⓘ 130 high-profile accounts hijacked
- ⓘ $120,000+ scammed from the public
- ⓘ Congressional inquiry and regulatory scrutiny
- ⓘ Permanent erosion of user trust
- ⓘ Share price drop and reputational fallout

With AD360 (The alternate timeline)

- ✓ Overprivileged accounts never exist
- ✓ Stale accounts auto-detected and disabled
- ✓ Real-time alerts catch unauthorized changes instantly
- ✓ Attack surface eliminated before exploitation
- ✓ Platform trust and brand integrity intact

ROI insight

The social media platform hack cost millions in crisis management, legal exposure, and lost market value — all traceable to accounts that should never have had that level of access.

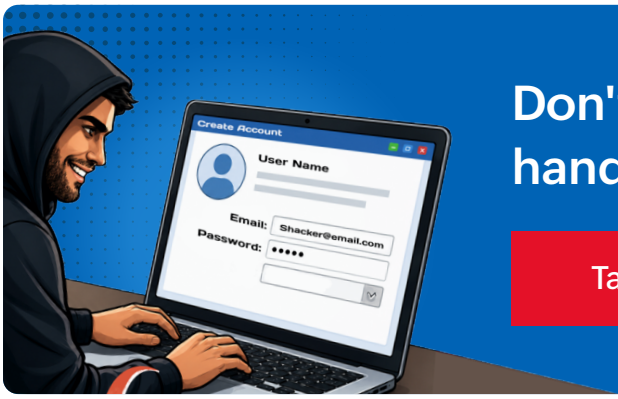
- ✓ $120K+ stolen + millions in damage vs. fractional IAM deployment cost
- ✓ Massive reputational damage vs. proactive access governance
- ✓ Congressional testimony vs. a clean access audit report

Lessons from the social media platform hijacking

Compromised, overprivileged accounts' actions are harder to track	Malicious activity blends into legitimate admin behavior
Stale accounts are loaded guns	Unused but powerful accounts are prime targets for social engineering
Access without audit is trust without verification	No visibility into who has what access means no ability to detect abuse
Privilege creep compounds over time	Roles change, but access often doesn't, creating dangerous gaps
Real-time monitoring is non-negotiable	By the time the breach was noticed, 130 accounts had already been taken
Social engineering bypasses technical controls	Identity governance must account for human-layer attacks, not just technical ones

Best practices to defend against insider access abuse

Enforce least privilege access	Limit admin capabilities to only what's necessary
Implement role-based delegation	Avoid giving full control to individual accounts
Monitor and audit all administrative actions	Detect anomalies instantly
Restrict and control privileged account usage	Protect high-risk access points
Automate policy enforcement	Ensure consistency across all accounts
Enable real-time alerts for suspicious activity	Respond before escalation
Regularly review and clean up access rights	Eliminate privilege creep



Don't let an unchecked account hand attackers your entire platform

Talk to an expert

Our Products

ADManager Plus | ADAudit Plus | ADSelfService Plus | Exchange Reporter Plus | RecoveryManager Plus

AD360 | Log360 | EventLog Analyzer | DataSecurity Plus | M365 Manager Plus

ManageEngine
AD360

ManageEngine AD360 is a unified identity platform that seamlessly connects people, technology, and experiences while giving enterprises full visibility and control over their identity infrastructure. It offers automated life cycle management; secure SSO; adaptive MFA; and risk-based governance, auditing, compliance, and identity analytics—all from a single, intuitive console. With extensive out-of-the-box integrations and support for custom connectors, AD360 easily integrates into existing IT ecosystems to enhance security and streamline identity operations. Trusted by leading enterprises across healthcare, finance, education, and government, AD360 simplifies identity management, fortifies security, and ensures compliance with evolving regulatory standards. For more information, please visit https://www.manageengine.com/active-directory-360/.

$ Get Quote Download