Business Email Compromise (BEC)

BEC is more than an email issue. It's an identity problem.

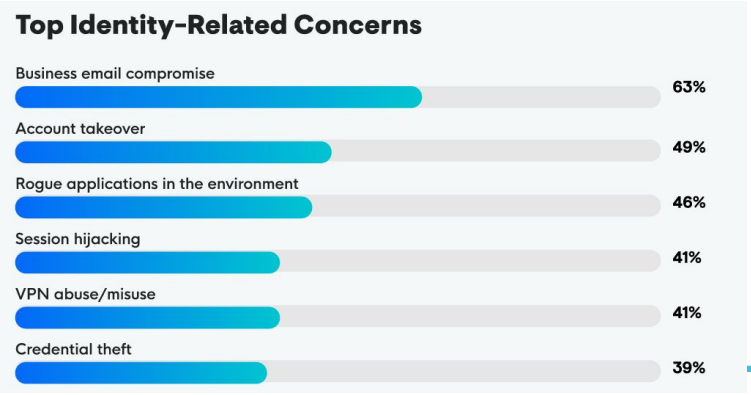
Overview

Just one compromised account is all it takes for attackers to pose as your company's leadership, reroute payments, and quietly drain your funds.

BEC attacks are a billion-dollar business because hackers exploit your weakest link: **identities and untrained users.**

Modern BEC bypasses secure email gateways, traditional filters, and MFA. Attackers just log in—not break in!—and exploit what most teams can't see: compromised sessions, rogue OAuth apps, inbox rule manipulation, and socially engineered employees.

Huntress stops takeovers before the fallout and trains users to spot Business Email Compromise red flags so you stay protected.



Key Outcomes

Stop account takeovers
Hackers know the jackpot starts with a compromised Microsoft 365 account. Once attackers compromise an identity, they forward rules, hijack sessions, and set up fraudulent payments. They move fast, but Managed ITDR moves faster. Our 3-minute MTTR stops attackers before a compromised inbox turns into a full-blown BEC incident.

Outsmart attackers
Your employees are your first line of defense—and attackers know it. That's why Huntress offers training built by the same experts who stop real-world BEC attacks every day to teach your workforce to recognize wire-fraud red flags, verify suspicious requests, and resist adversary tactics

Stay ahead 24/7
Most growing businesses can't afford 24/7 coverage—but attackers don't clock out. With Huntress, you're never alone in the fight against BEC. Our SOC, staffed by expert threat analysts, is ready to shut down attacks 24/7 to keep your business secure, your operations steady, and your peace of mind intact.

HUNTRESS

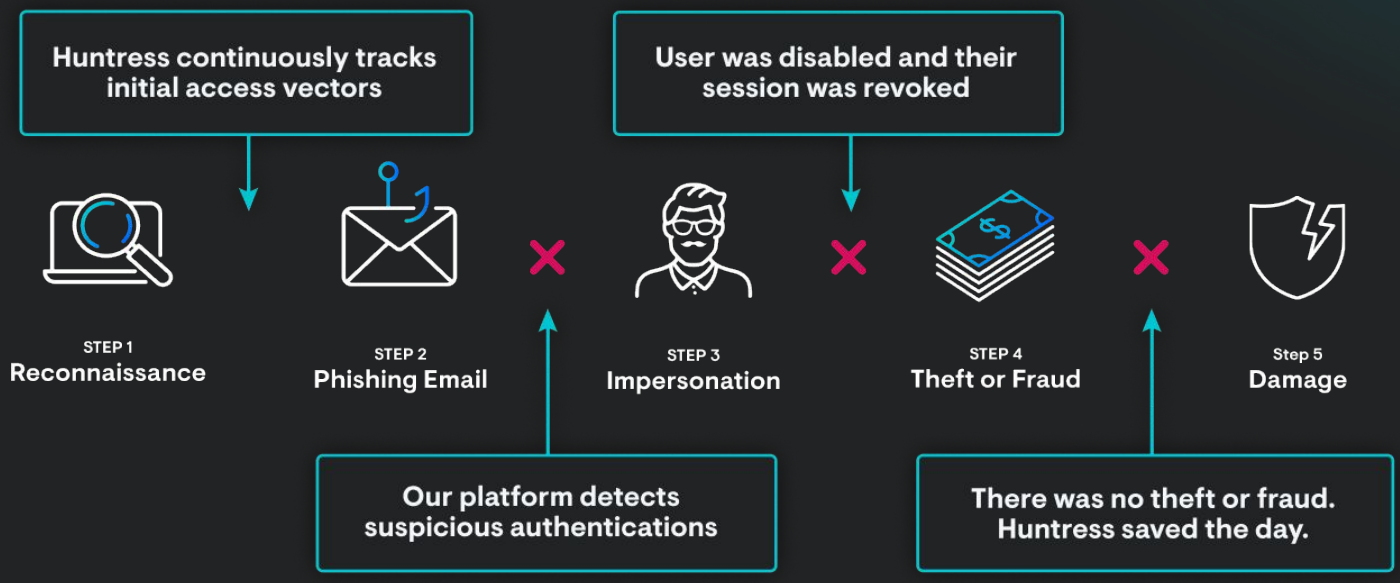
Filters stop bad emails.
Huntress stops financial damage.

Proven to stop BEC so you avoid manual, multi-hour incident response.

The sinking feeling of a user reporting a clicked phishing link quickly confirms a compromised account via an unusual datacenter IP login. This triggers a frantic scramble to assess the damage, determine responders, and contain the threat.

With the 24/7 human-led, AI-augmented Huntress SOC, that panic is gone. We contain threats within minutes, completing critical, time-sensitive steps before attackers can steal data or initiate wire fraud by:

- Disabling the compromised account
- Revoking the session
- Stopping the attacker before any business impact



Real threats demand real proof

24/7
Global threat analyst coverage

3 min
Mean Time to Respond (MTTR)

200k+
Organizations protected

9M+
Identities monitored

See how the Huntress Security Platform protects you from BEC.

Get started today at huntress.com/trial

HUNTRESS