

CASE STUDY · SEPTEMBER 2024

Business Email Compromise: How Invoice Fraud Diverted Over \$500,000

An anonymized incident case study tracing a fraudulent file-sharing request, stolen Microsoft 365 credentials, hidden inbox conversations, and a wire transfer exceeding \$500,000.



Conceptual illustration only; not the customer's production environment.

Incident snapshot

Detail	Summary
Organization	A large enterprise (customer anonymized)
Initial lure	A fraudulent SharePoint-style file-sharing email targeting accounting personnel
Compromised service	A Microsoft 365 mailbox
Fraud mechanism	Hidden executive correspondence and a modified vendor invoice
Reported loss	Over \$500,000 transferred to attacker-controlled banking details
Case study date	September 2024

This anonymized incident case study is adapted from the supplied account. Identifying workforce details and the precise loss amount are omitted. The source names another investigator; this account does not attribute the investigation or remediation to Massive IT. Recovery of transferred funds is not documented.

The background: public information made the lure credible

The attacker used an enterprise's publicly available employee directory to research roles, departments, and contact information. That reconnaissance helped identify accounting personnel and construct a targeted message rather than a generic phishing email.

The email imitated a SharePoint file-sharing request. A link led to a fraudulent page designed to capture Microsoft 365 credentials. When the targeted employee encountered an error after attempting access, the issue was not reported, delaying the opportunity to investigate the suspicious request.

From stolen credentials to mailbox surveillance

With the captured credentials, the attacker accessed the employee's mailbox and monitored business conversations. Inbox rules redirected correspondence from the chief financial officer into the RSS Feeds folder, reducing the likelihood that the employee would see the messages in their normal inbox.

This mailbox access exposed the timing, content, and approval context of genuine payment activity. The attacker did not need to invent an entire transaction: a legitimate invoice and an existing executive authorization provided a convincing foundation for the fraud.

The invoice substitution

The attacker identified a vendor invoice that had been forwarded with authorization to process a wire transfer. Using a compromised third-party host, the attacker relayed messages spoofing the executive's email address and supplied a modified invoice containing attacker-controlled banking details.

The accounting employee recognized the vendor, invoice format, and apparent authorization. The payment was processed, and more than \$500,000 was transferred to the attacker's account according to the supplied incident account.

The attack chain

Stage	Observed tactic	Operational lesson
Reconnaissance	Research of public staff and contact details	Review the information exposed in public directories
Credential theft	Fraudulent file-sharing page	Report unexpected sign-in prompts and failed sharing requests promptly
Mailbox access	Use of captured Microsoft 365 credentials	Strengthen identity controls and review sign-in evidence
Concealment	Inbox rules moved executive messages out of view	Include mailbox-rule review in compromise investigations
Payment redirection	Spoofed executive message and altered banking details	Independently verify payment changes using trusted contact channels

Investigation findings

The source reports that MFA was not in use and that legacy IMAP and POP3 access remained enabled broadly. Where basic authentication is permitted, password-only access can undermine an MFA strategy; enabling MFA without reviewing authentication methods and exceptions is not enough.

Protocol names alone do not prove an MFA bypass, because supported modern authentication behavior depends on the client and configuration. This case study describes the incident findings rather than treating all IMAP or POP3 access as inherently password-only.

Reported remediation

The supplied account describes implementation of a layered set of identity and email protections:

- **Microsoft MFA:** Add another authentication factor for user access.

- **Safe Links and Safe Attachments:** Strengthen malicious-link and attachment inspection, subject to licensing and configuration.
- **Impersonation protection:** Improve detection of messages imitating executives or trusted senders.
- **SPF and DKIM:** Establish email authentication records and signing controls.
- **DMARC monitoring and reporting:** Improve visibility into domain spoofing and authentication results.
- **External sender tagging:** Provide an additional visible signal when messages originate outside the organization.

DMARC monitoring is not the same as an enforced rejection policy, and email authentication does not prevent every form of impersonation or account compromise. These controls should be understood as layers of protection, not a guarantee against future fraud.

Business process controls matter too

This incident illustrates why payment authorization and payment destination must be checked separately. A familiar invoice and an apparently genuine approval can still contain altered banking instructions.

Organizations should independently verify new or changed bank details through a previously trusted contact method, use appropriate dual approval for sensitive transfers, train personnel to report suspicious file-sharing requests, and include mailbox rules in incident response checks. These are lessons from the incident, not additional deliverables claimed by the supplied account.

What the account establishes—and what it does not

The reported outcome was discovery of the compromise and implementation of stronger identity and email controls. The source does not document recovery of the transferred funds, a measured reduction in subsequent attacks, or independent validation of every remediation control. No such outcome is claimed here.

Why this case matters

Business email compromise combines technical access with knowledge of normal business processes. In this incident, public employee information, credential theft, mailbox rules, and invoice manipulation worked together to make a fraudulent payment appear routine.

Reducing that risk requires coordinated identity security, email protection, employee reporting, and payment verification—not reliance on a single product or warning banner.

Review your email and identity defenses

Massive IT helps organizations assess Microsoft 365 identity controls, email security, and incident readiness. Schedule a consultation or call (813) 518-5454.