C

Email Thread Hijacking: Detection and Payment-Fraud Response

Email thread hijacking occurs when an attacker uses or copies a real conversation to make malicious payment, credential, or attachment requests convincing.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 How conversation interception works
02 Thread hijacking versus spoofing
03 Warning signs
04 Controls that stop payment fraud
05 If a fraudulent transfer was sent
06 Mailbox incident response
07 For recipients of a suspicious reply
08 Source

Quick answer: Email thread hijacking, or conversation interception, occurs when an attacker uses a compromised mailbox or copied conversation to insert a malicious request into a real business exchange. The attacker may change bank details, send malware, request credentials, or redirect replies. Verify consequential changes through a separate trusted channel.

01 How conversation interception works

An attacker compromises the mailbox of an employee, supplier, customer, real-estate professional, or other participant. They read messages, calendars, contacts, signatures, invoices, and timing until a valuable transaction appears. They may reply from the genuine account, create a look-alike domain, or copy the thread into a new message that appears continuous.

Mailbox rules can hide the victim’s legitimate replies, mark messages as read, forward copies externally, or move correspondence to another folder. The attacker may delete sent items and wait quietly before changing payment instructions or introducing an attachment.

02 Thread hijacking versus spoofing

Simple spoofing forges the visible sender but does not require mailbox access. A look-alike domain uses a subtly different registered domain. Account compromise sends from the real mailbox and can expose authentic history. These methods can be combined, so a message appearing inside an existing thread is not proof that the sender remains in control.

03 Warning signs

- New bank, wallet, payment, delivery, or contact details introduced by email.
- A reply-to address or registered domain that differs from earlier messages.
- Unusual urgency, secrecy, changed tone, or a request to avoid normal approval.
- An unexpected archive, link, document, QR code, or request to sign in again.

- Missing messages, unfamiliar inbox rules, forwarding, delegates, OAuth grants, or login sessions.
- A supplier claiming not to have received replies that appear in your sent history.

04 Controls that stop payment fraud

1. Verify every new or changed payment instruction using a known phone number or established portal, never contact details from the change request.
2. Require two-person approval and record verification for beneficiary changes and high-value payments.
3. Use phishing-resistant MFA, disable legacy authentication, and restrict external forwarding and unapproved application consent.
4. Configure SPF, DKIM, and DMARC for owned domains. These reduce domain spoofing but cannot prevent mail sent from a compromised real account.
5. Monitor new inbox rules, forwarding, unusual locations, impossible travel, new MFA methods, and large mailbox searches or exports.

05 If a fraudulent transfer was sent

Contact the sending financial institution immediately through its official fraud channel and request recall or recovery action. Speed matters. Preserve the full messages with headers, payment records, account details, phone numbers, timestamps, and verification history. Report to local law enforcement and the appropriate national fraud service; in the United States, the FBI directs BEC reports to IC3.

06 Mailbox incident response

Do not only reset the password. Revoke sessions and tokens, remove unauthorized MFA and recovery methods, inspect forwarding, rules, delegates and application grants, and review sign-in and audit logs. Determine which conversations and attachments were accessed. Notify affected

partners through independently verified contacts, hunt for the same lure across the organization, and preserve evidence for legal or regulatory review.

07 For recipients of a suspicious reply

Do not use “reply” to verify the request because the attacker may control the conversation. Start a new contact through a known number or portal. If a file ran or credentials were entered, isolate the device and secure the account from a clean system.

08 Source

The attack patterns, payment examples, and response priorities align with the FBI’s Business Email Compromise guidance.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com