Conversation Interception: What it is, warning signs, and how to stop email thread hijacks

Gridinsoft Help Center

What it is

Conversation interception is when attackers sneak into an email thread-by hacking a mailbox or buying stolen archives-and quietly read along. Once they know the context, they can impersonate one side (e.g., a supplier or buyer) to reroute payments, change delivery details, or derail deals.

How it works

- Access: stolen passwords, malware on a device, or purchased mail archives.
- Eavesdrop: attacker learns names, amounts, timelines, tone, and signatures.
- Impersonate: they reply in-thread from the real account or a look-alike domain to change banking details or send booby-trapped files.

Red flags

- Sudden banking changes or "urgent" updates mid-thread
- Subtle domain look-alikes (vendor-pay.com vs vendorpay.com)
- Odd tone, spelling, or new contacts CC’d without reason
- Attachments or links replacing previously shared docs

If you suspect it (fast steps)

- Stop payments/shipments and verify by phone using known numbers.
- From a clean device, change email passwords and turn on MFA.
- Review mail rules/forwarders and remove anything unfamiliar.
- Check recent login history; sign out of other sessions.
- Inform partners and finance; preserve logs for investigation.

Prevent it

- MFA on all mailboxes; block legacy, password-only protocols.
- Train teams: never accept banking changes by email alone-verify out-of-band.
- Use allowlists for payee accounts; require a second approver for changes.
- Monitor for auto-forward rules, impossible travel logins, and look-alike domains.
- Keep endpoints protected (EDR/AV) and patched.