Conversation Hijacking

Spotting the Threat

Did you know that a Barracuda analysis of 500,000 email attacks revealed a 400% increase in conversation hijacking related activity? Here we take a closer look so you can spot the threat.

With conversation hijacking, cybercriminals insert themselves into existing business conversations or initiate new ones based on information they've gathered from compromised email accounts.

Their main goal is to use this information to steal money or personal data.

By blending in, conversation hijackers leverage familiarity to catch victims off guard. A typical email exchange may be an informal request to verify bank information while the sender is out of town, or an urgent demand to download a report.

How to avoid becoming a victim of Conversation Hijacking:

- Verify the identity of the email sender with a phone call.
- Be skeptical of requests that involve the transfer of money or financial information.
- Have a manager weigh in if you're unsure of the sender, request or overall email.
- Alert your IT team if you suspect anything suspicious as it could be part of a larger attack.

Example

Hello {email:firstName},

◀ Conversation hijackers inject themselves into existing email threads by seamlessly blending in, using first names and leveraging the situation to elicit a response.

Did you receive my last email?

Your gift card order is pending until we can process the transaction. Please visit the link here by end of day to confirm we have the right card on file.

▲ A tight deadline to respond adds a sense of urgency.

Once confirmed your order will be processed. Please allow five to seven business days for delivery. Thanks, {email:firstName}, for taking care of this!

▲ Using the first name again in the close extends the illusion that this is coming from a familiar source.

Sincerely,

Ben Argos
Rewards Card Services