Barracuda

PARTNER LOGO

Who are You Really Talking to?

A business partner has been discussing a new project with you on email. In the latest message he required you to send along your bank information for drafting a contract. He also asked you to download and review an attached proposal before tomorrow's meeting. You did all that without hesitation. But in the next hour, a huge amount of money was taken from your bank account, and your company network was proven to be invaded!

Similar cases happen again and again. A latest research by Barracuda on 500,000 email attacks has already identified a shocking 400% rise in domain-impersonation attacks used for this kind of conversation hijacking!

Believe it or not, cybercriminals manage to infiltrate legitimate email threads based on information gathered from compromised email accounts or as part of an account-takeover attack. Through highly customized phishing techniques, they make the victims totally believe they are interacting with someone they trust, and get tricked into opening malicious attachments, clicking on a phishing link, or disclosing confidential information.

How to mitigate the risk?

While ensuring that conversation hijacking is part of your security awareness training for employees, it is equally important to deploy an effective scanning tool across the organization to spot the burgeoning threats hiding in your emails. A stitch in time saves nine. Action now to stop the invaders! **Try a free run of the Barracuda Email Threat Scanner.**

Scan Your Mailbox Now

Forward this to a colleague

Privacy Policy I Unsubscribe