Barracuda

PARTNER LOGO

Who is Behind the Mask... Do You Know?

Your boss sent you an email asking you to perform an urgent but confidential wire transfer. You got this done in no time. But in the following day, you found that the money has gone to a fraudulent account resulting in a big loss of the company!

This kind of phishing attack, the so called “business email compromise” (BEC) or “man-in-the-email attack”, occurs frequently in many parts of the world causing US$1.7 billion losses last year according to the FBI. It has also become one of the most financially damaging cybercrimes in Asia with the potential to cause catastrophic disruption. Right, the nightmare has come true!

In most cases, BEC scammers pretend to be a high-level executive tricking a colleague, customer or partner into transferring funds or participating in what appear to be legitimate transactions, while disclosing sensitive data. These attacks use social-engineering tactics and compromised accounts, which are difficult to identify because you even will not see any malicious attachments and links found in typical phishing emails. They can also take a variety of forms which are totally beyond prediction.

How to avoid falling victim to BEC?

It is of equal importance to enhance the security awareness of employees and deploy an effective scanning tool across the organization to uncover the ever-increasing threats hiding in your emails. Own the moment or the moment will own you. Action now to remove the mask of email fraudsters! **Try a free run of the Barracuda Email Threat Scanner.**

Scan Your Mailbox Now

Forward this to a colleague