



CYBER JAGROOKTA DIWAS - AUGUST 2026

BEC ATTACK

BUSINESS EMAIL COMPROMISE

A single stolen email account can expose sensitive business information, customer records, financial documents, and internal communications.

Cyber criminals use compromised accounts to impersonate trusted employees, redirect payments, steal confidential data, and launch further attacks across the organization.

HOW BEC ATTACK HAPPENS



RED FLAGS



EMAIL GATEWAY CHECKS

Email gateway caution message for mails received from unknown sources.



CHANGES EMAIL CREDENTIALS

Sudden changes of account information without prior notice.



REQUESTS FOR SENSITIVE INFORMATION

Emails asking for confidential data, credentials, internal documents or urgent payments.

STAY SAFE



VERIFY BEFORE YOU ACT

Confirm requests through a trusted channel like a phone call or in-person.



ENABLE STRONG PROTECTIONS

Use Multi-Factor Authentication (MFA) and strong, unique passwords.



BE ALERT, REPORT EARLY

Be cautious of suspicious emails and report any doubt to IT/Security.

A COMPROMISED EMAIL ISN'T JUST AN INBOX AT RISK

IT CAN BECOME THE GATEWAY TO YOUR ORGANIZATION'S MOST VALUABLE INFORMATION.

