BST
Consulting Group

BUSINESS EMAIL COMPROMISE (BEC)

Business Email Compromise (BEC) is a type of cyber attack where threat actors impersonate trusted individuals to deceive employees into sending money or sensitive information.

HOW BEC ATTACKS WORK

1 RESEARCH

Attackers research your organization and identify key personnel.

2 IMPERSONATE

They impersonate a trusted individual (e.g., CEO, vendor, partner) via email.

3 DECEIVE

They create a sense of urgency to bypass normal verification processes.

4 EXPLOIT

The victim is tricked into sending money or sharing sensitive information.

5 IMPACT

Attackers achieve financial gain and damage your organization's reputation.

PROTECT YOURSELF

Everyone plays a role in stopping BEC.

VERIFY REQUESTS

Always verify unusual requests via a trusted channel.

BE SUSPICIOUS

Look for red flags like urgent language, unusual payment instructions, or unknown senders.

FOLLOW POLICY

Follow your company's security policies and report anything suspicious.

STAY INFORMED

Regular training helps you recognize and avoid threats.

STOP. THINK. VERIFY. Don't let a fake email cost your organization.

nmassry@bstco.com