

[HOME](#) / [COME CI ATTACCANO - LA BUSINESS EMAIL COMPROMISE: METTIAMOCI ALLA PROVA CON CASI REALI](#)

COME CI ATTACCANO - LA BUSINESS EMAIL COMPROMISE: METTIAMOCI ALLA PROVA CON CASI REALI

Tipologia	Corsi E-Learning
Temi	Bancassicurazione, ICT, Organizzazione e Sicurezza, Controlli Interni
Tipologia e-Learning	Casi, multimediale
In sintesi	<p>Le varianti della Business Email Compromise (BEC): CEO Fraud, The Man In The Mail, Bogus Invoice Scheme, Supplier Swindle, Invoice Modification Scheme, Business Contacts through Compromised E-mail, Business Executive and Attorney Impersonation, Data Theft. Sono tante e tutte insidiose. L'analisi dei casi reali procede attraverso differenti chiavi di lettura: cosa è accaduto, le conseguenze dell'attacco, gli errori commessi; l'esercitazione si concentra sugli elementi ai quali prestare attenzione per riconoscere queste truffe e sulle le misure tecniche e organizzative da adottare contro la BEC.</p> <p>RILASCIO PREVISTO: NOVEMBRE</p>
Target	Operatori di filiale bancaria, di agenzia assicurativa, di help desk, di contact centre, di back office
Obiettivi	Descrivere le caratteristiche delle diverse tipologie di Business Email Compromise (BEC) e riconoscere gli errori più comuni commessi dalle vittime, le misure di prevenzione per evitarli e le azioni da intraprendere in caso di attacco subito
Durata	1 ora e 30 minuti di fruizione lineare

CONTENUTI

- Caso 1 – Una CEO Fraud successa davvero
- Caso 2 – La truffa alla Zecca
- Caso 3 – La BEC realizzata con il Deep Fake a Hong Kong
- Business E-mail Compromise (BEC): di che cosa si tratta e ultime frontiere degli attacchi

CONTATTI

Per informazioni Ufficio Gestione Clienti e Processi Informativi e Tecnologici

gestioneclienti@abiservizi.it

06.6767.640