BUSINESS E-MAIL COMPROMISE E PHISHING VIA PEC: METTIAMOCI ALLA PROVA CON CASI REALI

Tipologia	**Corsi on demand**
Temi	**Bancassicurazione, Organizzazione e sicurezza**
Tipologia e-Learning	**Corsi multimediali e interattivi, orientati a modelli di coinvolgimento attivo dell'utente**
In sintesi	Le varianti della business e-mail 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. Anche le e-mail PEC (che noi crediamo sicure!) possono essere usate per il phishing. Il corso descrivere le caratteristiche delle diverse tipologie di BEC e del phishing via PEC per riconoscere gli errori più comuni commessi dalle vittime, le misure di prevenzione per evitarli e le azioni da intraprendere in caso di attacco. Il corso risponde agli standard del Regolamento IVASS n. 40/2018.
Target	Operatori di filiale bancaria, di agenzia assicurativa, di help desk, di contact centre, di back office
Durata	1 ora e 30 minuti

PRESENTAZIONE

Il corso illustra le caratteristiche delle diverse tipologie di business e-mail compromise (BEC) e del phishing via posta elettronica certificata (PEC) attraverso il racconto di vicende eclatanti e realmente accadute.

L'analisi dei casi procede attraverso differenti chiavi di lettura: cosa è accaduto, le conseguenze delle truffe, gli errori commessi dalle vittime; le esercitazioni si concentrano sugli elementi ai quali prestare attenzione per riconoscere questi attacchi e sulle misure tecniche e organizzative da adottare per difendersi.

I contenuti, multimediali e interattivi, sono arricchiti da voci di glossario, contributi tematici e approfondimenti. Il corso è corredato da test in itinere e finale.

I materiali sono a cura di Giorgio Sbaraglia, Cybersecurity Consultant e socio Clusit.

REQUISITI TECNICI

RISOLUZIONE VIDEO E BROWSER

Risoluzione video minima: 1024x768

HTML5

Windows: Microsoft Edge (versione corrente), Google Chrome (versione corrente), Firefox (versione corrente)

Mac: Safari (versione corrente), Google Chrome (versione corrente), Firefox (versione corrente)

Mobile: Safari e Google Chrome per iOS 10 o superiore, Google Chrome per Android 4.4 o superiore

CONTENUTI

- Caso 1 - La truffa alla multinazionale passa per il CFO
- Caso 2 – Il deepfake di Hong Kong
- Caso 3 – Truffa alla Zecca dello Stato
- La business e-mail compromise (BEC)
- Caso 4 – La truffa passa anche per le PEC
- Phishing tramite PEC
- Test finale
- Attestato IVASS

CONTATTI

Per informazioni

gestioneclienti@abiservizi.it

06.6767.640