



# Suite Cybersecurity: cosa c'è di nuovo





# Suite Cybersecurity – Cosa c'è di nuovo

---



## CONTENUTI

Abbiamo realizzato una **suite di 5 nuovi corsi** multimediali e interattivi, per un totale di **6 ore**, dedicata alle **ultime pericolose evoluzioni del cybercrime**.

Recenti ed emblematici attacchi di tipo ransomware e truffe business email compromise (BEC) sono il contesto dal quale si sviluppano **esercitazioni che hanno l'obiettivo di favorire negli allievi la consapevolezza dei rischi, la capacità di riconoscerli e di applicare le precauzioni e i mezzi di difesa più opportuni**.

**L'analisi dei casi è condotta per tipologie di attacco** e, concentrandosi sugli gli errori commessi dalle vittime, **consente di accrescere in modo interattivo l'attitudine alla costante attenzione agli elementi di rischio e di sviluppare buone prassi di "cyber hygiene"**.

I contenuti sono a cura dell'Ing. Giorgio Sbaraglia, Cybersecurity Consultant e socio Clusit.

**I corsi rispondono agli standard del Regolamento IVASS 40/2018.**



# Suite Cybersecurity – Cosa c'è di nuovo



La suite è articolata nei seguenti corsi:

<b>La cybersecurity nell'era digitale: un focus sul settore finanziario</b>	IVASS	Tutoriale multimediale	1 ora	Rilascio metà ottobre
<b>Come si è evoluto il cybercrime e le più recenti tecniche di attacco. La criticità del «fattore umano»</b>	IVASS	Videolezione	1 ora	Disponibile
<b>Ransomware 2.0: come sono cambiati gli attacchi negli ultimi anni</b>	IVASS	Videolezione	1 ora	Disponibile
<b>Come ci attaccano - La minaccia ransomware: mettiamoci alla prova con casi reali</b>	IVASS	Casi multimediale	1 ora e 30 minuti	Rilascio fine ottobre
<b>Come ci attaccano - Business email compromise e phishing via PEC: mettiamoci alla prova con casi reali</b>	IVASS	Casi multimediale	1 ora e 30 minuti	Rilascio novembre



# Suite Cybersecurity – Cosa c'è di nuovo

---



## DESTINATARI

Operatori di filiale bancaria, di agenzia assicurativa, di help desk, di contact centre, di back office



## DURATA

6 ore



## FORMAT

Corsi multimediali e interattivi, orientati a modelli di coinvolgimento attivo dell'utente



## IL TRACCIAMENTO

I corsi fruiti tramite **LMS di ABIFormazione**, indipendentemente dai formati, inviano alla piattaforma i dati di tracciamento utili per la produzione della reportistica, compresa quella **richiesta da FBA**, conforme alla **Circolare ANPAL n. 4 del 28.12.2020**. I corsi predisposti per le piattaforme LMS delle aziende clienti sono realizzati secondo lo **standard SCORM 1.2**

# La cybersecurity nell'era digitale: un focus sul settore finanziario



# La cybersecurity nell'era digitale: un focus sul settore finanziario

---



## CONTENUTI

Negli ultimi anni abbiamo assistito a una crescita continua degli attacchi informatici a tutti i livelli: il settore finanziario è stato tra i più colpiti nel mondo, assieme a quello manifatturiero. Parallelamente, molte nuove norme sono state emanate, italiane ma soprattutto europee, focalizzate sulla cybersecurity. Un numero di direttive e regolamenti come mai accaduto negli anni precedenti



## OBIETTIVO

Descrivere l'importanza strategica della cybersecurity nell'attuale era digitale e la normativa di riferimento riguardante il settore finanziario



## DURATA

1 ora di fruizione lineare



# La cybersecurity nell'era digitale: un focus sul settore finanziario

---



## INDICE

Come si è evoluto il cybercrime: quali sono gli obiettivi e chi sono gli attori

Il cybercrime nel settore finanziario

Normativa in materia cybersecurity con focus sul settore finanziario



**Come si è evoluto il cybercrime  
e le più recenti tecniche di attacco.  
La criticità del «fattore umano»**



## Come si è evoluto il cybercrime e le più recenti tecniche di attacco. La criticità del «fattore umano»

---



### CONTENUTI

Oggi il cybercrime rappresenta una minaccia concreta da non sottovalutare e i nostri avversari sono sempre più temibili. Cosa possiamo fare per difenderci? Quanto incide il fattore umano sugli attacchi informatici? Nessuno oggi può prescindere dal considerare la cybersecurity come elemento strategico per la difesa dei propri dati, aziendali o personali. Impariamo a proteggerci dagli attacchi informatici



### OBIETTIVO

Conoscere il fenomeno del cybercrime nelle sue dinamiche principali e riconoscere e sapersi difendere dal phishing



### DURATA

1 ora di fruizione lineare



# Come si è evoluto il cybercrime e le più recenti tecniche di attacco. La criticità del «fattore umano»

---



## INDICE

I dati del cybercrime nel mondo e in Italia

Perché i nostri avversari sono sempre più temibili

Il monitoraggio del cybercrime

La prima causa degli attacchi informatici: il fattore umano

Come riconoscere il phishing



# Ransomware 2.0: come sono cambiati gli attacchi negli ultimi anni



# Ransomware 2.0: come sono cambiati gli attacchi negli ultimi anni

---



## CONTENUTI

Il ransomware, la minaccia attuale più pericolosa in cui l'attaccante sequestra i file dell'utente e richiede un riscatto in criptovaluta, pena la pubblicazione e/o la vendita dei dati nel Dark Web. L'hacker non è più un personaggio isolato ma vere e proprie bande criminali organizzate come società, che effettuano attività di recruiting e hanno come clienti le proprie vittime. È importante saper riconoscere questa modalità di cyber attacco, applicando alcune regole di comportamento per potersi difendere



## OBIETTIVO

Conoscere il fenomeno del cybercrime nelle sue dinamiche principali e riconoscere e sapersi difendere dal ransomware



## DURATA

1ora



# Ransomware 2.0: come sono cambiati gli attacchi negli ultimi anni

---



## INDICE

I ransomware sono cambiati

Ransomware 2.0: nuove tecniche di attacco

Casi e bande ransomware famosi

Come difendersi dai ransomware 2.0

# Come ci attaccano - La minaccia ransomware: mettiamoci alla prova con casi reali





## Come ci attaccano - La minaccia ransomware: mettiamoci alla prova con casi reali



### CONTENUTI

Come un attacco ransomware può far cessare l'attività di grandi aziende o pubbliche amministrazioni, creando perdite economiche, disagi per i clienti ed enormi danni d'immagine. L'analisi dei casi reali procede attraverso differenti chiavi di lettura: cosa è accaduto, le conseguenze dell'attacco, gli errori commessi; l'esercitazione consente di far emergere focus di sicurezza contestualizzati



### OBIETTIVO

Descrivere le caratteristiche delle più recenti modalità di attacco ransomware e riconoscere gli errori più comuni che consentono ai malware di penetrare nelle reti delle organizzazioni, le misure di prevenzione per evitarli e le azioni da intraprendere in caso di attacco



### DURATA

1 ora e 30 minuti di fruizione lineare



# Come ci attaccano - La minaccia ransomware: mettiamoci alla prova con casi reali

---



## INDICE

Caso 1 – L'attacco a MGM Resorts
Caso 2 – L'attacco a Westpole-PA Digitale
Caso 3 – L'attacco a Synlab
Ransomware - La minaccia ancora oggi più grave e diffusa



# Come ci attaccano - Business email compromise e phishing via PEC: mettiamoci alla prova con casi reali



# Come ci attaccano – Business email compromise e phishing via PEC: mettiamoci alla prova con casi reali



## CONTENUTI

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. Anche le email PEC (che noi crediamo sicure!) possono essere usate per il phishing. 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 misure tecniche e organizzative da adottare contro la BEC e il phishing via PEC.



## OBIETTIVO

Descrivere le caratteristiche delle diverse tipologie di business email compromise (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



## DURATA

1 ora e 30 minuti di fruizione lineare



# Come ci attaccano – Business email compromise e phishing via PEC: mettiamoci alla prova con casi reali

---



## INDICE

Caso 1 – La truffa alla multinazionale passa per il chief financial officer

Caso 2 – Truffa da 3 milioni di euro alla Zecca dello Stato

Caso 3 – I falsi indirizzi PEC e l'attacco con PEC compromesse

Business email compromise (BEC): di che cosa si tratta e ultime frontiere degli attacchi

Anche le email PEC possono essere usate per il phishing

PEC e REM: cosa sono e come funzionano

abiformazione.it  
abilearning.it

UNI EN ISO 9001:2015  
per i Settori IAF 37, 35, 08

# Oltre 20 anni insieme.

Un viaggio nel mondo della formazione, orientato allo sviluppo delle competenze di migliaia di persone nelle banche, negli intermediari finanziari e assicurativi, nelle aziende e negli enti pubblici.

## CONTATTI:

gestioneclienti@abisevizi.it

06.6767.640

Piazza del Gesù, 49 00186 – Roma

**ABISERVIZI**  **ABI  
FORMAZIONE**