INDICE

CYBERSECURITY: Consapevolezza dei rischi e comportamenti corretti

INTRODUZIONE: CHI SONO GLI ATTACCANTI E COME AGISCONO

IDENTITA' DIGITALE E DATA BREACH

PRINCIPALI TIPOLOGIE DI MALWARE

PRINCIPALI DIFESE TECNICHE

TRUFFE, SOCIAL ENGINEERING E PHISHING

RISCHI OPERATIVI, REPUTAZIONALI E IMPATTI SU SOLVENCY II

CRITTOGRAFIA, GESTIONE PASSWORD E NAVIGAZIONE

CASE STUDY E BEST PRACTICES

Durata: 4 ore

Modalità svolgimento: asincrona/sincrona

Valido ai fini della formazione obbligatoria:

☒ **IVASS**

ESMA

COMPETENZE

Tecniche basse	Contenutistiche medie	Relazionali basse
🟢	🟡🟡	🟢

Descrizione del corso

- Il corso inizia con una descrizione dei diversi profili degli attaccanti e del modo in cui operano
- L'oggetto del furto: l'identità digitale e i data breach
- Alcuni riferimenti all'attualità: ransomware, truffa del CEO, truffa del cliente/fornitore
- Vengono presentate le principali forme di malware: virus, ransomware, backdoor e spyware
- Viene fornita una panoramica delle principali difese tecniche: antivirus, antispam e firewall
- Come funziona la crittografia, la gestione password e la navigazione internet
- Quali sono i comportamenti corretti per ridurre i rischi

Know how richiesto: conoscenza dei processi informatici in ambito bancario, finanziario assicurativo

- **Al termine del percorso** formativo è previsto un **test** volto a valutare le competenze dei discenti.
- Il test si fine corso si ritiene **superato** se è stata raggiunta la soglia del **60%** delle risposte corrette
- Emissione di **attestato di valutazione** delle conoscenze acquisite.

Destinatari: Le figure destinate ad erogare consulenza assicurativa, Organizzazione, Audit e Compliance

In caso di formazione Asincrona: Moduli formativi, suddivisi in pillole formative della durata di circa 15 minuti, intervallati da momenti di consolidamento e verifica dell'apprendimento (brevi test a risposta chiusa).