ITALIACORSI

FORMAZIONE PROFESSIONALE CONTINUA

Tutorial
Cyber Security

Tutorial Cyber Security

Valido dal 13.01.2020 al 13.01.2021

Attestato ECM scaricabile direttamente al termine del corso, previo superamento del test, almeno il 75% della performance. Il corso dovrà essere terminato rispettando il periodo di validità. In caso di ritardo non sarà possibile rimborsare il corso e ricevere i crediti ECM.

DURATA: 3 ore

Provider accreditato FIPES

MODALITÀ: e-learning

OBIETTIVO GENERALE (ECM)
Linee guida – Protocolli – Procedure (2).

OBIETTIVI SPECIFICI
Uno dei pilastri della sicurezza logica è la formazione del personale. Infatti, gli attacchi più sofisticati richiedono sempre una componente di ingegneria sociale che sfrutta i comportamenti inappropriati del personale. Un piano di formazione completo e continuativo può correggere tali comportamenti con enorme beneficio per la sicurezza complessiva dell'azienda. La nostra offerta formativa è finalizzata sia al dipendente che al personale tecnico IT.

Nel corso affrontiamo tutti gli aspetti della Cyber Security: i tipi di hacker, gli attacchi e da dove provengono, le frodi, le tecniche utilizzate, gli scenari presenti e futuri, le statistiche. Affrontiamo tali argomenti sia sul piano aziendale che sul piano personale e famigliare (l'internet of things), come affrontare questo rischio sia dal punto di vista tecnico che culturale. Concludiamo con case history a nostro parere più interessanti della scena cyber italiana e internazionale.

DESTINATARI
Tutte le professioni sanitarie.

PROGRAMMA

Cyber Security: cos'è - Presentazione della Sicurezza attiva (sicurezza logica), tecniche e gli strumenti mediante i quali le informazioni ed i dati di natura riservata sono resi intrinsecamente sicuri.

Gli attaccanti - Chi sono gli hacker? Come vengono classificati a seconda delle tecniche e degli obiettivi.

I rischi e le minacce - Le aziende tecnologicamente più avanzate, condizione imprescindibile per mantenersi competitivi nel mercato globale, sono gli obiettivi maggiormente attaccabili. Quali rischi corrono?

Gli esempi e le Storie - Gli esempi più eclatanti del mondo Cyber: gli attacchi già avvenuti.

Il Deep Web - Che cos'è il Web Sommerso? Leggende, miti e realtà.

Criptoloker e i suoi fratelli -Cosa sono i Malware? Meritano un approfondimento specifico.

IoT Internet of Things - Cyber e oggetti quotidiani: gli hackers possono entrare anche nella nostra sfera domestica?

Le Difese - Come difendersi in azienda e in famiglia. Le 3 regole d'oro. Proteggersi da virus e malware. Riconoscere le truffe. Controllare i social media

Cyber Security in sanità - Rapporto 2018. Trend cyber attacco. Gestione del rischio. Data bridge. Quadro normativo di riferimento. Scenari percorribili.