LIVELLO 1

Come ci attaccano e perché

DESCRIZIONE DEL LIVELLO

Ogni modulo è auto-consistente, ma tra i singoli moduli formativi sono stati inseriti dei " naturali" richiami ad argomentazioni affrontate nelle differenti lezioni, rafforzando in questo modo il livello di apprendimento e memorizzazione dei contenuti.

In questo primo livello verranno affrontati argomenti che riguardano i rischi per le aziende, partendo in primis dalla gestione delle password per poi approfondire il pericolo di virus e malware, che portano inevitabilmente a capire il perchè bisogna proteggere i propri dati.

Inoltre quello che scoprirai durante queste lezioni è che ognuno di noi è una straordinaria risorsa e una ricca fonte di informazioni e quindi ognuno di noi è soggetto ad attacchi da parte di hacker.

INTRODUZIONE

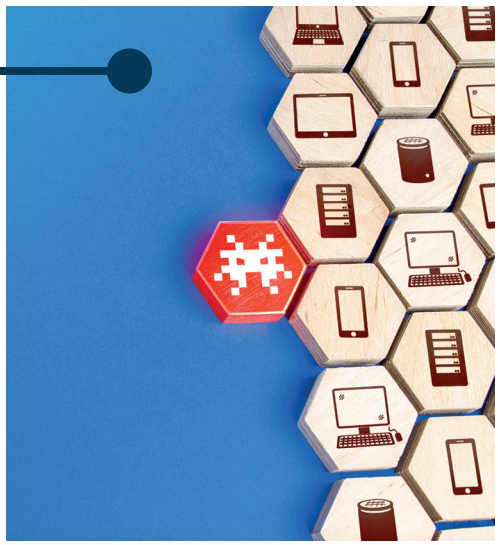
Questo modulo serve per introdurre l'utente nell'ambiente della cyber security. Esso fornisce delle informazioni generali sul corso specificando alcuni termini tecnici ricorrenti nei vari moduli.

GESTIONE DELLE PASSWORD

La gestione delle proprie **PASSWORD** è un elemento basilare delle strategie difensive. Questo modulo formativo fornisce gli elementi necessari per una **PASSWORD SICURA**, proteggendola da tentativi di violazione da parte di hacker che potrebbero livelarsi molto pericolosi.

VIRUS E MALWARE

Virus e Malware sono una delle minacce principali alle quali prestare attenzione. Questo modulo formativo fornisce gli elementi base per ridurre il rischio di cadere vittima di questi software e per limitare le conseguenze negative in caso di attacco.



PERCHÈ PROTEGGERE I DATI

I tuoi dati sono un **BENE PREZIOSO.** Nelle mani sbagliate, i tuoi dati potrebbero causare molti danni. Molte persone non si rendono conto che ovunque tu vada su Internet lasci sempre un'impronta digitale. Quindi non dare per scontata la sicurezza dei dati. Questo modulo fornisce gli elementi necessari per comprendere l'importanza dei dati.

PHISHING E ANTISPAM

Il **PHISHING** è una delle forme più comuni di attacco informatico e utilizza l'email come principale veicolo di diffusione. È particolarmente subdola perché basata su un inganno, i criminali fingono di provenire da organizzazioni autorizzate per indurti a fornire informazioni sensibili.
In questo modulo vengono fornite le informazioni necessarie per potersi difendere da attacchi provenienti da email di phishing e si parla anche del software anti-spam per bloccare le email sospette.

FURTO D'IDENTITÀ

La rivoluzione digitale ha amplificato il rischio di subire il **FURTO D'IDENTITÀ**, ovvero la possibilità che un cybercriminale usi i nostri dati personali, i dati anagrafici identificativi, i codici bancari le nostre foto per utilizzarli per commettere reati o per spiarci, per venderli ad altri e per molti altri scopi malevoli. In questa lezione vengono fornite le informazioni utili per difendersi dal "furto di Identità" e per saper cosa fare nel caso di furto.

USO DEI DISPOSITIVI RIMOVIBILI

Le **MEMORIE USB**, sono estremamente utili quando è necessario archiviare file personali o per spostare i file fra PC non connessi in rete. Le chiavette USB però sono anche potenziali vettori di malware. Quando abbiamo in mano una chiavetta USB dobbiamo riflettere bene prima di utilizzarla. In questo modulo viene mostrato come difendersi da questa tipologia di rischio.

RISCHIO RANSOMWARE

Tutti abbiamo sentito parlare di criminali che chiedono un riscatto per qualcosa, o per qualcuno che stanno tenendo in ostaggio.
Nell'era digitale, i riscatti sono usciti fuori dal grande schermo e sono entrati nella vita reale. L'ostaggio sono i tuoi dati. Questo modulo fornisce le informazioni necessare per di aiutarti a comprendere questo rischio e insegnarti a proteggerti dal temibile **RANSOMWARE.**