



LIVELLO 3

Scendiamo in profondità

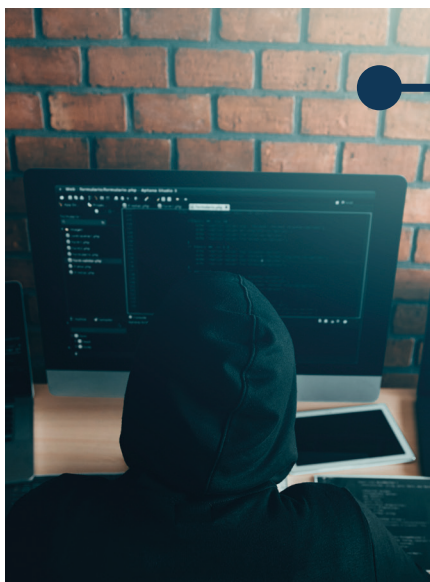
DESCRIZIONE DEL LIVELLO

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

Nel terzo livello di questo corso si parla più approfonditamente del come difendersi dalle minacce precedentemente descritte negli altri livelli. In particolare si approfondisce il tema degli attacchi all'internet delle cose, della sicurezza informatica parlando anche dei rischi delle operazioni online, tra cui i pagamenti, lo shopping e la banca online.

ATTACCHI ALL'INTERNET DELLE COSE (IoT)

L'IoT crea connessioni tra più dispositivi o cose. Questa connettività consente di fornire i dati a Internet, consentendo una maggiore efficienza e uno sforzo umano ridotto. Ma sfortunatamente ci sono aspetti negativi, come minacce alla sicurezza e attacchi informatici. Questo corso ti aiuterà a identificare questi rischi e ti consiglierà come migliorare le tue misure di sicurezza per prevenire gli attacchi.



DEEP E DARK WEB

il Deep web rappresenta l'ecosistema all'interno del quale si annidano i cybercriminali. Ma di cosa si tratta? E quanto è grande? In questo modulo lo andremo a scoprire insieme

BLOCKCHAIN E CRIPTOVALUTE

Sentiamo sempre più spesso parlare di Blockchain e BITCOIN come se fossero entità clandestine provenienti da un universo parallelo. In realtà sono tecnologie che possono esserci molto utili. Quindi in questo modulo cercheremo di spiegare nel modo più semplice possibile il mondo delle criptovalute e le applicazioni della blockchain.



ATTACCHI AI SISTEMI INDUSTRIALI

Gli attacchi non colpiscono solo i computer privati o aziendali ma anche i sistemi industriali e infrastrutturali che controllano una serie di servizi tra cui alcuni servizi essenziali per i cittadini e la società. Questi attacchi rappresentano un rischio ben più grave perché mettono a rischio i servizi ai cittadini. La storia recente, e gli incidenti già accaduti ci dimostrano quanto siano reali questi rischi. In questo modulo andiamo a scoprire meglio di cosa si tratta.



CRITTOGRAFIA

Ci sono diversi modi per archiviare le informazioni in modo che solo alcune persone siano in grado di accedervi. Uno di questi è la crittografia. Ne abbiamo sentito parlare quando abbiamo trattato il ransomware. Questa volta però vediamo come la crittografia può trasformarsi da incubo a prezioso alleato.

SHOPPING ONLINE

Acquistare online è un'esperienza incredibile! Tantissimi prodotti a portata di click e poterli ricevere dopo poche ore dall'ordine è bellissimo. Ma anche in questo caso sono presenti dei rischi. In questo modulo andremo a vedere quali sono e come diffenderci



ONLINE BANKING

L'Internet Banking o Home Banking e il Mobile Banking sono servizi bancari fruibili dai clienti attraverso una connessione internet. Quali sono i rischi nell'uso di questi servizi? Vediamolo in questo modulo



GEOLOCALIZZAZIONE

I servizi di Geolocalizzazione sono così presenti nella nostra vita quotidiana che non ci facciamo più caso. Google MAP è un servizio eccezionale. Mai più in ritardo e mai più domande ai passanti per sapere dov'è quella via piuttosto che quel ristorante o un parcheggio. I benefici sono noti ma quali sono i rischi?



SIM SWAP

Continuano a ripeterci che l'autenticazione a 2 fattori garantisce sicurezza. sappiamo anche che attraverso il meccanismo del SIM-SWAP, anche questo tipo di precauzioni vengono spesso violate. Ma come è possibile? E soprattutto... come possiamo difenderci?

