AI-PACT Tempo Innovation Source

neverbefore.it

Livello Base (24 ore)

CORSO DI CYBERSECURITY

Premessa

Questo corso è progettato per chi è nuovo alla **cybersecurity** e desidera comprendere i **concetti fondamentali della sicurezza informatica**. Fornirà una panoramica delle principali minacce e vulnerabilità, oltre a introdurre le pratiche di base per proteggere dispositivi, reti e dati personali. Al termine del corso, i partecipanti avranno una solida base per comprendere e applicare misure di sicurezza essenziali nel mondo digitale.

A chi è rivolto?

Questo corso è rivolto a studenti, principianti, e professionisti che non hanno esperienza o hanno una conoscenza limitata della cybersecurity. È ideale per chiunque desideri **comprendere i principi fondamentali** della sicurezza informatica e apprendere come **proteggere le proprie informazioni e dispositivi** da minacce comuni. Non sono richiesti requisiti di conoscenza tecnica specifica.

Obiettivi

- Comprendere i **concetti fondamentali** della cybersecurity e l'importanza della sicurezza informatica.
- Riconoscere le **principali minacce e vulnerabilità** nel mondo digitale.
- Imparare le pratiche di base per la **protezione di dispositivi, reti e dati personali**.
- Applicare misure di sicurezza elementari per **prevenire attacchi comuni** come malware e phishing.
- Sviluppare consapevolezza della **privacy online** e della **gestione sicura** delle informazioni personali.

Programma didattico

Modulo 1: introduzione alla cybersecurity (6 ore)

- cos'è la cybersecurity e perché è importante;
- minacce e vulnerabilità comuni;
- concetti di base di sicurezza: confidenzialità, integrità, disponibilità (CIA Triad);
- panoramica delle principali minacce: malware, phishing, attacchi DoS.

Modulo 2: concetti di rete e sicurezza (8 ore)

- fondamenti di rete (protocollo TCP/IP, DNS, HTTP/HTTPS);
- nozioni base di firewall, proxy, e VPN;
- sicurezza delle reti Wi-Fi;
- pratiche di base per la sicurezza delle reti.

Modulo 3: sicurezza dei dispositivi e delle applicazioni (6 ore)

- sicurezza dei sistemi operativi (Windows, Linux);
- sicurezza delle applicazioni: aggiornamenti e patching;
- utilizzo di antivirus e antimalware;
- configurazione sicura dei dispositivi mobili.

Modulo 4: introduzione alla sicurezza personale e alla privacy (4 ore)

- gestione delle password e autenticazione a due fattori (2FA);
- sicurezza dell'email e dei social media;
- introduzione alla crittografia (cifratura, SSL/TLS);
- pratiche di navigazione sicura e protezione della privacy online.