

CORSO ONLINE CYBER SECURITY



Docente
Ing. Antonio
Pellegrino



Durata
5 ore



Crediti
5 CFP



Modalità
E-learning

ISCRIVITI ORA 

CHIAMA IL NUMERO
(+39)092445834



VISITA IL SITO
www.pedago.it





Il Programma del Corso

Descrizione

Il Corso di Cyber Security Online, della durata di 5 ore in e-learning, fornisce le basi teoriche e operative della sicurezza informatica per proteggere dati, reti e infrastrutture digitali. Il percorso approfondisce le principali minacce (phishing, malware, social engineering, data breach) e le relative misure di prevenzione, con focus su protezione dei dati, sicurezza delle reti e conformità al GDPR. Le competenze acquisite sono applicabili sia in ambito professionale sia personale.

Obiettivi

- Comprendere i principi della sicurezza informatica e le principali minacce digitali;
- Valutare e gestire i rischi informatici con strategie di prevenzione efficaci;
- Applicare buone pratiche per la protezione dei dati e la sicurezza delle reti;
- Utilizzare strumenti di sicurezza come antivirus e autenticazione a due fattori;
- Garantire la sicurezza informatica in azienda tramite formazione e monitoraggio;
- Operare nel rispetto delle normative sulla privacy e sulla protezione dei dati.

Perché sceglierci



Docenti Qualificati

Professionisti selezionati tra i più qualificati esperti di ogni settore



Contenuti tecnici, ma chiari

Approccio pratico e comprensibile, anche su temi complessi.



Massima Flessibilità

Possibilità di gestire la formazione in autonomia da pc o smartphone



Risorse Aggiuntive

Ogni corso dispone di materiale didattico, documenti e utility gratuite



Tutoring e Assistenza

Team sempre pronto a gestire esigenze di natura tecnica o didattica



Rilascio di Attestato

Al superamento del corso è previsto il rilascio dell'Attestato

1.

LA SICUREZZA INFORMATICA

- Introduzione alla Cyber Security
- Lo scopo degli attacchi informatici
- IoT: Internet of Things
- Gli attacchi più famosi
- Le conseguenze di un attacco informatico
- Anonymous

2.

CYBER RISK

- I pericoli del Web: quali sono e come riconoscerli
- I rischi informatici più comuni (Parte 1)
- I rischi informatici più comuni (Parte 2)
- I pericoli derivanti dalle mail
- Social Media: come evitare di esporre l'azienda e se stessi ai rischi
- Social Engineering
- Cosa sono i Cookies
- I Cookies in azione arichi

3.

IL FATTORE UMANO E AZIENDALE

- Il fattore umano nella cyber security
- La postazione di lavoro nell'era dello "Smart Working"
- Come evitare di esporsi a furti di dati e di informazioni
- Strumenti Aziendali
- Il GDPR e la Gestione dei Dati
- Ho subito un attacco! E adesso?

5.

POSTAZIONE SICURA

- Profili Utenti
- Processi e Servizi
- Software di Analisi
- Scanner Wi-Fi
- Monitoraggio delle risorse
- AntiVirus

4.

PASSWORD SICURE: TRUCCHI E CONSIGLI

- Creare una Password Efficace
- Autenticazione a due Fattori su Google e Facebook
- Riepilogo sulle Password

6.

RETE SICURA

- Principali protocolli di comunicazione
- Consigli su creazione di una rete sicura
- Creare una rete ospite (Wi-Fi)
- Network-Attached Storage (NAS)
- Virtual Private Network (VPN)
- Port Scanner
- Sniffing