CORSO CYBER SECURITY

VISITA IL CORSO

Data la crescente applicazioni della tecnologia e dell'Internet of Things (IoT) sia in ambito lavorativo che in ambito privato e, soprattutto, vista la mole di dati sensibili ed informazioni riservate archiviate su supporti digitali, la cybersecurity è diventata un aspetto fondamentale per individui, aziende e organizzazioni di ogni settore. Il Corso Cyber Security offre una panoramica completa proprio sui principi fondamentali della sicurezza informatica introducendo tematiche come l'implementazione di politiche di sicurezza, l'uso di strumenti e tecnologie per rilevare e rispondere alle minacce digitali.

DOCENTE
Ing. Antonio Pellegrino

DURATA
Ore 5

MODALITÀ
e-Learning

L'obiettivo principale del corso è quello di fornire una solida base di conoscenze applicabili nella protezione dei dati sia a livello personale che professionale. Grande attenzione sarà data alla comprensione delle principali strategie di difesa e delle best practices da mettere in atto per incrementare la sicurezza dei propri sistemi informatici e creare una rete sicura. I discenti apprenderanno come riconoscere e comprendere le diverse tipologie di minacce informatiche e di cyber risk più diffusi, anche tramite l'utilizzo consapevole di strumenti come software di analisi o i più comuni AntiVirus.

1.
LA SICUREZZA INFORMATICA

1.1. Introduzione alla Cyber Security
1.2. Lo scopo degli attacchi informatici
1.3. IoT: Internet of Things
1.4. Gli attacchi più famosi
1.5. Le conseguenze di un attacco informatico
1.6. Anonymous

2.
CYBER RISK

2.1. I pericoli del Web: quali sono e come riconoscerli
2.2. I rischi informatici più comuni (Parte 1)
2.3. I rischi informatici più comuni (Parte 2)
2.4. I pericoli derivanti dalle mail
2.5. Social Media: come evitare di esporre l'azienda e se stessi ai rischi
2.6. Social Engineering
2.7. Cosa sono i Cookies
2.8. I Cookies in azione

3.
IL FATTORE UMANO E AZIENDALE

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

4.
PASSWORD SICURE: TRUCCHI E CONSIGLI

4.1. Creare una Password Efficace
4.2. Autenticazione a due Fattori su Google e Facebook
4.3. Riepilogo sulle Password

5.
POSTAZIONE SICURA

5.1. Profili Utenti
5.2. Processi e Servizi
5.3. Software di Analisi
5.4. Scanner Wi-Fi
5.5. Monitoraggio delle risorse
5.6. AntiVirus

6.
RETE SICURA

6.1. Principali protocolli di comunicazione
6.2. Consigli su creazione di una rete sicura
6.3. Creare una rete ospite (Wi-Fi)
6.4. Network-Attached Storage (NAS)
6.5. Virtual Private Network (VPN)
6.6. Port Scanner
6.7. Sniffing