Digital Security Academy

Corso di Cybersecurity Awareness

Obiettivi del corso:

Fornire ai frequentatori una formazione completa sulla sicurezza informatica per prevenire attacchi e proteggere i dati aziendali.

Introduzione al Corso

Modulo 1: Fondamenti della Cybersecurity

- **Definizione di Cybersecurity e Importanza**
- **I tre pilastri della sicurezza: Confidenzialità, Integrità, Disponibilità (CIA Triad)**
- **Tipologie di dati aziendali e loro valore**
- **Normative e regolamenti (GDPR, NIST, ISO 27001, ecc.)**

Modulo 2: Minacce Informatiche e Tipologie di Attacchi

- **Minacce interne vs esterne**
- **Malware (virus, worm, trojan, ransomware, spyware, adware, rootkit)**
- **Phishing, Smishing e Vishing**
- **Attacchi Man-in-the-Middle (MitM)**
- **SQL Injection, XSS, attacchi a siti web**
- **Attacchi DDoS e botnet**
- **Zero-day exploit e vulnerabilità software**

Modulo 3: Tecniche di Protezione e Difesa

- **Autenticazione e gestione delle password**
  - MFA (Autenticazione a più fattori)
  - Gestori di password
- **Cifratura dei dati e protocolli di sicurezza**
- **Aggiornamenti e patch management**
- **Backup e Disaster Recovery**
- **Firewall e sistemi di rilevamento delle intrusioni (IDS/IPS)**

Modulo 4: Sicurezza dei Dispositivi e della Rete

- Protezione dei dispositivi aziendali (PC, smartphone, IoT)
- BYOD (Bring Your Own Device) e rischi associati
- Wi-Fi security e reti sicure (VPN, WPA3, segmentazione di rete)
- Accesso remoto sicuro e telelavoro

Modulo 5: Ingegneria Sociale e Sicurezza Umana

- Cos'è l'ingegneria sociale e perché è pericolosa?
- Tecniche di manipolazione psicologica usate dagli hacker
- Esercizi pratici: simulazione di phishing e attacchi di social engineering

Modulo 6: Sicurezza delle Applicazioni e del Cloud

- Sicurezza delle applicazioni web e mobile
- DevSecOps: Integrare la sicurezza nello sviluppo software
- Rischi del Cloud Computing e strategie di mitigazione
- Modelli di sicurezza cloud (IaaS, PaaS, SaaS)
- Identità e accesso nel cloud (IAM)

Modulo 7: Incident Response e Gestione delle Crisi

- Piani di risposta agli incidenti informatici
- Identificazione e contenimento delle minacce
- Notifica e comunicazione durante una violazione
- Analisi forense e recovery post-attacco
- Ruolo del CERT (Computer Emergency Response Team)

Modulo 8: Conformità, Privacy e Aspetti Legali

- Regolamenti di sicurezza (GDPR, CCPA, HIPAA, PCI-DSS)
- Responsabilità legale in caso di data breach
- Politiche di sicurezza e codice di condotta aziendale
- Protezione della privacy aziendale e personale