Corso Cyber Security

Durata: 1 giornata

A chi è rivolto: personale aziendale, professionisti, collaboratori e a coloro che si occupano di sicurezza informatica

Scopo del corso:

Il corso è pensato per accompagnare i partecipanti in un percorso di consapevolezza e responsabilizzazione rispetto ai rischi legati all'uso quotidiano delle tecnologie digitali. In un contesto in cui le minacce informatiche sono sempre più sofisticate e pervasive, è fondamentale acquisire conoscenze aggiornate e sviluppare buone abitudini che permettano di proteggere i propri dispositivi, le proprie informazioni personali e i dati aziendali. La giornata di formazione rappresenta un'occasione per comprendere le dinamiche degli attacchi informatici, riconoscere i segnali di pericolo e apprendere strategie concrete per ridurre la propria esposizione alle minacce, migliorando nel contempo l'efficacia e la sicurezza delle attività online.

Contenuti

Durante il corso verranno introdotti i principi fondamentali della sicurezza informatica, con particolare attenzione agli aspetti pratici della protezione dei dati e della prevenzione degli attacchi. Si parlerà di come riconoscere software dannosi, truffe digitali e tentativi di manipolazione psicologica, imparando a distinguere comportamenti rischiosi da pratiche sicure. Verrà dato spazio alla gestione efficace delle credenziali, alla protezione delle reti domestiche e aziendali, all'uso corretto di internet e dei dispositivi mobili. Il corso si propone anche di sfatare falsi miti, promuovere senso critico e fornire strumenti concreti per affrontare in modo più sicuro le sfide del mondo digitale.

Introduzione alla Sicurezza Informatica

- Cos'è la sicurezza informatica
- Principi fondamentali: confidenzialità, integrità, disponibilità, autenticazione, controllo accessi, non ripudio, privacy
- Sicurezza come processo e non come prodotto

Cybersecurity: Difensiva e Offensiva

- Definizione di cybersecurity
- Approccio difensivo: firewall, IDS/IPS, antivirus, crittografia, backup, formazione
- Approccio offensivo: penetration test, ethical hacking, red team

Tipologie di Attacchi Informatici

- Malware: definizione, diffusione e sintomi
- Tipi di malware: trojan, spyware, ransomware, adware, rootkit, keylogger, botnet
- Tecniche di attacco: phishing, spoofing, DoS/DDoS, privilege escalation, buffer overflow

Social Engineering e Ingegneria Sociale

- Cos'è l'ingegneria sociale e come si manifesta
- Phishing, sextortion, bin-raiding, contatti indesiderati, skimming
- Prevenzione e riconoscimento degli attacchi

Reti e Comunicazioni Sicure

- Rischi dei Wi-Fi pubblici
- Tecniche di attacco alle reti: MitM, DNS Spoofing, Evil Twin
- Uso sicuro della rete: VPN, DNS sicuri, HTTPS

Autenticazione e Password

- Creazione e gestione di password sicure
- Autenticazione a due o più fattori (2FA/MFA)
- Autenticazione senza password: panoramica e vantaggi

Sicurezza dei Dispositivi e Supporti

- Sicurezza fisica dei dispositivi
- Rischi legati ai supporti rimovibili (USB, pendrive, BadUSB)
- Juice jacking e contromisure

Sicurezza Operativa e Collaborazione

- Aggiornamenti software e patching
- Politiche di accesso e controllo degli utenti
- Sicurezza nella condivisione dei file e nella collaborazione

Simulazioni e Casi Reali

- Analisi di email di phishing
- Esercitazioni su riconoscimento di minacce
- Simulazioni di attacco e risposta

Piano di Risposta agli Incidenti

- Come reagire in caso di attacco
- Procedure di isolamento e comunicazione
- Ripristino e prevenzione futura