Escape from Cybercrime

Obiettivi

Il corso di mira a fornire le conoscenze fondamentali sulla sicurezza informatica, affrontando le principali minacce come malware, phishing, e attacchi alla rete. Si concentra sulla gestione sicura delle password, l'uso protetto delle e-mail e dei social media, e le strategie per prevenire i rischi aziendali, come errori umani e data breach. Inoltre, esplora tecniche di protezione come aggiornamenti software, sicurezza Wi-Fi, backup e promuove una cultura aziendale di cybersecurity.

Programma

- Introduzione alla Cybersecurity: Importanza della sicurezza informatica e impatti del cybercrime
- Tipologie di Malware: Virus, worm, trojan, ransomware, spyware e altre minacce
- Attacchi basati sull'inganno: Phishing, smishing, vishing, social engineering e sim swap
- Attacchi alla rete e ai dispositivi: DDoS, exploit, botnet e pericoli del Dark Web
- Errori umani e sicurezza aziendale: Comportamenti a rischio e data breach reali
- Protezione dei dispositivi e delle reti – Aggiornamenti software, sicurezza Wi-Fi e backup
- Gestione sicura delle password: Creazione di password robuste e autenticazione a più fattori
- Uso sicuro delle e-mail: Riconoscere e prevenire attacchi via e-mail e file dannosi: social media e cybersecurity: Rischi della condivisione di dati aziendali online
- Navigazione sicura in Internet: Evitare siti malevoli, download rischiosi e truffe online
- Messaggistica aziendale e sicurezza: Pericoli di WhatsApp e altri strumenti di comunicazione
- Protezione delle informazioni aziendali: Strategie per prevenire il furto di dati sensibili
- Conclusioni e Best Practices: Creazione di una cultura aziendale di cybersecurity

Durata: 1h 20m

Valido ai fini: IVASS