CYBER SECURITY AWARENESS

Workshop in videoconferenza (Webinar)

Milano, 28 giugno 2021

Dalle 9.00 alle 13.00

*Il corso, indirizzato a personale non IT, è concepito per trasmettere consapevolezza e competenze di base per ridurre l'esposizione ai **Rischi Cyber**.*
*Le minacce informatiche possono avere un impatto elevato sul business aziendale con danni importanti sia a livello economico che di reputazione. La collaborazione di dipendenti e manager di ogni grado nell'adozione di un comportamento responsabile ed attento nella gestione delle informazioni e degli strumenti informatici, aziendali e personali, rappresenta una sfida importante ed indispensabile per migliorare il livello di sicurezza e la resilienza ad attacchi sempre più sofisticati. Seppure responsabili IT, Cyber e personale addetto alla gestione operativa della Cyber Security possano sforzarsi di adottare i migliori standard, procedure e tecnologie sofisticate per la difesa da attacchi Cyber, **tutto il personale aziendale è esposto** ad errori involontari o ad attacchi mirati che possono spesso compromettere e rendere vane le misure di sicurezza.*

*Il corso si propone di contribuire a diffondere la consapevolezza dell'importanza della Cyber Security per ogni ruolo aziendale, fornisce competenze di base e strumenti operativi per evitare comportamenti non appropriati o difendersi da attacchi quali **Phishing**, **Vishing**, **Social Engineering**, avere una gestione responsabile di dispositivi aziendali e personali quali **Smartphone**, utilizzare con consapevolezza i **Social Media**, comprendere cosa sono e quali rischi comportano gli attacchi **Ransomware**. Il corso non si propone di trasformare un dipendente o un manager in un esperto di Cyber Security ma di migliorare la sua gestione quotidiana di informazioni e strumenti informatici, la sua responsabilità come parte dell'azienda nella difesa dalle minacce Cyber.*

Introduzione

L'importanza della Cyber Security e la necessaria collaborazione di ciascuno nella difesa delle informazioni e degli strumenti informatici. Esempi di attacchi informatici e conseguenze.

Phishing, Vishing, Smishing, Social Engineering

Metodologie di attacco, come è possibile riconoscerle, norme di comportamento e di difesa.

Dispositivi Mobili Aziendali e Personali

Rischi nell'uso di Smartphones, Mobile App, Connessioni non sicure, chiavette USB e dispositivi esterni.

Password e protezione degli Accessi

Perché è importante scegliere Password robuste per uso Aziendale e Personale. L'autenticazione a 2 fattori.

Social Media

Rischi aziendali e personali nell'utilizzo non appropriato dei canali Social. Tecniche di attacco e norme di comportamento.

Ransomware

Casi reali di attacchi Ransomware, tipologie di rischio per l'azienda. Business Interruption, Danni Reputazionali, Esfiltrazione di Informazioni.

Alla fine del corso, attraverso un portale Web dedicato, i partecipanti potranno effettuare un test di verifica delle conoscenze acquisite ed avranno accesso ad ulteriore materiale di approfondimento.

Relatori

Massimiliano Rijllo, CEO - Coinnect SA

(Questo convegno è finanziabile attraverso i vouchers del Fondo Banche e Assicurazioni)

Quota di partecipazione Euro 350 + IVA 22% a partecipante

Sono previste scontistiche per piu' partecipanti della medesima azienda
I webinar saranno fruibili sulla piattaforma Zoom

Ulteriori informazioni al numero 02.80016480 e segreteriagenerale@iside.it o www.iside.info

ISIDE srl
Via Dante n.4 - 20121 Milano
Tel 02.80016480 - Fax 02.80016481

Azienda certificata ISO 9001
Certificato n° IT20-24804A