CSAW-1 - CYBER SECURITY AWARENESS

Categoria: **Cyber Security Awareness**

INFORMAZIONI SUL CORSO

Durata:	Categoria:	Qualifica Istruttore:	Dedicato a:	Produttore:
1 Giorni	Cyber Security Awareness	Docente Senior (min. 5 anni)	Utente	PCSNET

OBIETTIVI

In questo corso di consapevolezza (awareness) verranno trattati i temi di Sicurezza Informatica, con particolare attenzione agli attacchi del Cybercrime e alla protezione dei propri dati e dei propri account.
Oggi la Cyber Security riguarda tutti noi e nessuno può considerarsi al sicuro: ritenere di non essere un obbiettivo interessante per i cyber criminali è il miglior presupposto per essere attaccati, quindi la sicurezza informatica è diventata un elemento strategico per la difesa dei dati della propria azienda o del proprio studio professionale. Se un'azienda perde i propri dati non è più nulla.
L'evoluzione del cybercrime ha sostituito l'hacker con vere e proprie organizzazioni criminali dotate di grandi mezzi e in grado di portare attacchi a chiunque. Il problema non è sapere se verremo attaccati ma solo quando saremo attaccati, non importa se siamo grandi o piccoli, prima o poi ci attaccheranno.
I mezzi per difenderci esistono, quello che manca è la consapevolezza del problema e la conoscenza degli strumenti più idonei da adottare per proteggerci. Oggi le Aziende non possono più ignorare il rischio ("perché dovrebbero attaccare proprio me?"), ma anzi cogliere l'opportunità (e gli obblighi) derivanti dal GDPR (Regolamento Europeo sulla Privacy) per ripensare e riorganizzare la propria sicurezza informatica a difesa dell'asset "immateriale" più importante, i PROPRI DATI!
Gli strumenti informatici sono importanti, ma il punto debole è sempre l'uomo (il fattore "H") che con il suo comportamento può rendere inefficace qualsiasi difesa.
Questo corso rappresenta un utile strumento per fornire a tutti la formazione di base per difendersi dagli attacchi informatici, formazione prevista anche dal nuovo Regolamento Europeo Privacy (GDPR).

PREREQUISITI

Nessun prerequisito.

CONTENUTI

Modulo 1 - L'evoluzione del Cybercrime

- -I dati del crimine informatico nell'Italia e nel mondo: il rapporto CLUSIT
- -Cyberwarfare, la guerra cibernetica: casi famosi
- -Deep Web, Dark Web, rete TOR e Bitcoin: cosa sono e perché ci riguardano
- -I danni economici generati alle aziende

Modulo 2 - Social Engineering e Phishing

- -Cos'è il Social Engineering

-Le varianti del Phishing: whaling, smishing, vishing e QRishing
-Phishing e lo Spear phishing: le tecniche d'attacco
-Casi pratici e come riconoscerli
-Individuare i siti di phishing: il typosquatting

Modulo 3 - I Ransomware: la minaccia oggi più temuta

-I Ransomware: cosa sono
-Come ci attaccano: i vettori d'infezione
-Alcuni attacchi famosi: da WannaCry a Petya
-Come difendersi dai Ransomware: le misure di prevenzione
-Sono stato colpito da un Ransomware: cosa fare ora? Quali sono le possibili opzioni
-Implicazioni giuridiche per le vittime dei ransomware: profili di responsabilità derivanti dal pagamento di riscatti

Modulo 4 - I rischi e le vulnerabilità delle email

-Gli attacchi attraverso la posta elettronica
-La Business Email Compromise (BEC): che cosa è e quanti danni sta causando nelle aziende
-Le truffe "The Man in the Mail" e "CEO fraud"
-L'email non è uno strumento sicuro: lo spoofing
-PEC e posta crittografata: caratteristiche, utilizzi e differenze

Modulo 5 - I malware su dispositivi mobili

-I rischi nei devices mobili: come vengono attaccati
-Cosa è lo Smishing e come riconoscerlo
-La prevenzione del mobile malware: una corretta policy aziendale
-La vulnerabilità delle reti WI-FI

Modulo 6 - Imparare a usare le Password

-Gli strumenti (sempre più potenti) degli hackers: alcuni famosi casi di attacchi e "data breach"
-La sicurezza di un Account dipende dalla forza della password
-Le regole per una Password sicura e gli errori da evitare
-Le "domande di (in)sicurezza"
-I Password Manager

Modulo 7 - La Sicurezza nelle Piattaforme Microsoft

-Cosa è la Zero Trust Architecture (ZTA)
-Windows Defender
-Sicurezza in Microsoft 365
-Protezione dell'identità e delle informazioni: Azure Entra ID e Azure Information Protection
-L'autenticazione a più fattori (MFA - Multi Factor Authentication)

Modulo 8 - I pericoli generati dallo Smart Working

-Il desktop remoto (RDP): quando serve e come utilizzarlo
-Le VPN (Virtual Private Network): quali scegliere e come impostarle
-Proteggere la privacy nelle riunioni online: le misure da adottare nell'uso delle piattaforme di Web meeting

INFO

Materiale didattico: Materiale didattico e relativo prezzo da concordare

Costo materiale didattico: NON incluso nel prezzo del corso
Natura del corso: Dimostrativo