Corso Online: SICUREZZA E CONSAPEVOLEZZA DIGITALE. DIFENDERSI DALLE MINACCE IN UN MONDO CHE CAMBIA.

L'obiettivo del percorso è trasformare gli utenti da potenziali **"anelli deboli"** a **"difensori consapevoli"** del sistema informativo aziendale. Il corso fornisce gli strumenti concettuali e pratici per la protezione dei dati, la gestione sicura degli accessi e la neutralizzazione delle minacce più evolute, con particolare attenzione all'Ingegneria Sociale e alle nuove sfide dell'IA nel cybercrime.

Nota Bene: **Noi consigliamo di partecipare il percorso completo**, dato che gli argomenti sono collegati e seguono un percorso logico. **Ogni modulo è però pensato per essere anche un percorso a sé stante** e quindi è possibile scegliere di seguire solo i moduli di interesse. **Il corso verrà riproposto almeno un'altra volta durante l'anno solare**; quindi, è anche possibile seguire un modulo durane questa edizione e completare il percorso in quella successiva.

Obiettivi Formativi

Il percorso ha l'obiettivo di fornire una visione chiara del panorama attuale delle minacce informatiche, sensibilizzando i partecipanti sul loro ruolo attivo nella protezione del patrimonio informativo aziendale. Nello specifico, al termine del corso i partecipanti saranno in grado di:

- **Comprendere il valore dei dati e il contesto normativo:** acquisire consapevolezza sull'importanza della confidenzialità e integrità delle informazioni, in linea con i principi del GDPR e della privacy.
- **Imparare a proteggere le proprie credenziali:** applicare le *best practice* per la creazione di password robuste e comprendere la necessità critica dell'autenticazione a più fattori (MFA) per proteggere l'identità digitale.
- **Riconoscere l'Ingegneria Sociale e le trappole dell'IA:** identificare i tentativi di manipolazione (Phishing, Smishing) e le nuove minacce generate dall'Intelligenza Artificiale (come i Deepfake), distinguendoli dalle comunicazioni legittime.
- **Adottare comportamenti di difesa attiva:** operare in sicurezza sia in ufficio che in modalità Smart Working, riducendo i rischi legati all'uso di dispositivi mobili e alla navigazione web.

A Chi è Rivolto

Il corso è ideale per:

- **Tutti i dipendenti e collaboratori** che necessitano di una solida introduzione ai concetti di sicurezza digitale e protezione dei dati.
- **Responsabili e decisori** aziendali interessati a capire l'importanza strategica della formazione per prevenire i Data Breach.

Modalità di Partecipazione

Il corso sarà erogato in **diretta** tramite la piattaforma **Microsoft Teams** sotto forma di leziono frontali con anche esercizi pratici. Saranno previsti momenti dedicati in cui i discenti avranno spazio per porre domande e richiedere approfondimenti.

Modulo 1 - Fondamenti, Protezione degli Accessi e Contesto Normativo

Codice SEC-AW-01

Durata: Modulo da 3,5h con 15 min. di pausa

Questo primo modulo è la base imprescindibile per chiunque utilizzi strumenti digitali in ambito professionale. Verranno introdotte le nozioni fondamentali di cybersecurity, il ruolo cruciale dell'utente nel processo di sicurezza e le tecniche di base per proteggere l'accesso ai sistemi, in particolare attraverso la corretta gestione delle credenziali. Sarà fornito anche un inquadramento essenziale sul contesto normativo relativo alla privacy per comprendere l'impatto e gli obblighi relativi alla protezione dei dati.

Programma del Modulo:

- **Introduzione alla Sicurezza:**
  - Cos'è il crimine informatico (cybercrime) e la sicurezza digitale (cybersecurity).
  - La triade CIA (Confidenzialità, Integrità, Disponibilità) e la data security.
  - Il ruolo cruciale degli utenti nel processo di sicurezza digitale.
- **Gestione degli Accessi e Credenziali:**
  - Sistemi informativi e utenti/account.
  - I rischi di compromissione dei dati aziendali e l'uso dei dati nel Dark-Web.
  - Buone pratiche per la gestione delle password e l'uso dell'autenticazione a più fattori (MFA).
  - Cenni sull'approccio Zero Trust.
- **Contesto Normativo e Dati:**
  - Il diritto di protezione dei dati personali e i concetti base di GDPR.
  - Accenni ai Framework Normativi come NIS2 e DORA.
  - Data Breach e obblighi delle organizzazioni.
- **Considerazioni Finali.**

Modulo 2 – Ingegneria Sociale, Nuove Minacce e Difesa Attiva

Codice SEC-AW-02

Durata: 3,5h con pausa di 15 minuti.

Alla base di quasi tutte le principali minacce che cercano di colpire gli utenti esite l'**Ingegneria Sociale**, la tecnica prediletta dai malintenzionati per aggirare i sistemi di sicurezza automatizzati.

In questo modulo verranno esaminate le principali tipologie di minacce, dal Phishing al Ransomware, con un importante aggiornamento sulle nuove sfide portate dall'Intelligenza Artificiale (Deepfake, kit IA). L'obiettivo è fornire agli utenti le competenze per trasformare la consapevolezza in azione e contribuire attivamente ad aumentare la propria difesa personale e quella di tutta l'organizzazione.

Programma del Modulo:

- L'Arma dell'Inganno: Ingegneria Sociale:
  - Come funziona l'ingegneria sociale e i principali meccanismi.
  - Analisi di casi di studio.
- Riconoscere e Neutralizzare le Minacce (Parte I):
  - Il Phishing e le sue declinazioni: Spear Phishing e Whaling.
  - Vishing e Smishing.
  - Attacchi via app di messaggistica e social network.
  - Come identificare un link malevolo o una mail malevola.
  - BEC: Business Email Compromise, quando la minaccia arriva dall'interno.
- Minacce Avanzate e l'IA nel Cybercrime:
  - Introduzione all'uso dell'IA nel cybercrime: Deepfake, kit IA e bot malevoli per attacchi automatizzati.
  - Cripto-Virus e Ransomware.

- Altre tipologie di Malware e modalità di attacco (es. fake antivirus, chiavette USB, ecc.).

- Strategie di Difesa Attiva:
  - Protezione mobile e implicazioni.
  - Indicazioni per lo Smart Working in sicurezza.
  - Compromissione di mail aziendali e conseguenze.