Corso Security Awareness

Gestire in maniera corretta il sistema informativo è una condizione essenziale per qualsiasi azienda, piccola o grande. Le apparecchiature informatiche, infatti, si vedono sempre più fondamentali per l'accesso a servizi chiave, quali la gestione dei dati personali, la proprietà intellettuale e la gestione dei flussi finanziari.

L'integrità di tale sistema viene senza dubbio affidata agli strumenti preposti a questa funzione, quali software antivirus, sistemi di backup, firewall, accortamente configurati e gestiti dai tecnici informatici. **Purtroppo, alle volte questo non è sufficiente**, in quanto i malintenzionati, consapevoli che gli odierni sistemi di gestione sono difficilmente attaccabili, prendono di mira l'anello debole del sistema: l'utente.

Gli utilizzatori spesso non vengono debitamente istruiti riguardo le minacce che fanno sempre più spesso uso di tecniche di ingegneria sociale, non gestibili dai sistemi di sicurezza automatizzati.

Formare gli utenti diventa quindi una delle misure di prevenzione più efficaci di Data Breach, e più in generale dei problemi di sicurezza informatica e non solo.

Durata 8 h

Parte Prima

- Introduzione
  - Cos'è il crimine informatico o cybercrime
  - Cos'è la sicurezza digitale o cybersecurity
  - La triade CIA e la data security
  - Perché è necessario proteggere i dati
  - Conseguenze degli attacchi e impatto economico
  - Ruolo degli Utenti nel processo di Sicurezza Digitale dell'organizzazione

Parte Seconda

- GDPR
  - Il diritto di protezione dei dati personali
  - Il contesto normativo
  - Dati personali e proprietari
  - Diritti dei proprietari

Alpsolution Sas di Cesare Carli & C.
cesare.carli@alpsolution.eu
Tel. 3401834067

alpsolution
assistenza hardware e software

- Trattamento dei dati, titolari e incaricati
- Impatto sull'organizzazione
- Data Breach e obblighi delle organizzazioni

Parte Terza

- Sistemi informativi e utenti
  - Sistemi informativi e approccio del castello
  - Utenti e Account
  - Credenziali di autenticazione
  - Compromissione dei dati aziendali
  - Come vengono usati i nostri dati nel Dark-Web
  - Buone pratiche di gestione delle password
  - Password managers e autenticazione a più fattori
  - l'approccio Zero Trust ed il suo impatto presente e futuro.

Parte Quarta

- Ingegneria sociale
  - Come funziona l'ingegneria sociale e principali meccanismi.
  - Casi di studio
  - Come identificare un link malevolo o una mail malevola.

Parte Quinta

- Tipologie di minacce
  - La truffa nigeriana
  - Il Phishing e le sue declinazioni
  - Spear Phishing e Whaling
  - Vishing e Smishing
  - Attacchi via app di messaggistica e social network
  - Cripto-Virus e Ransomware
  - Altre tipologie di Malware
  - Compromissione di mail aziendali e conseguenze
  - Altre modalità di attacco, fake antivirus, chiavette, ecc.
  - Protezione mobile e implicazioni
  - Smart Working in sicurezza, indicazioni.

Come tutti i corsi forniti da Alpsolution l'erogazione può avvenire da remoto utilizzando la piattaforma Microsoft Teams o in presenza.