PROGRAMMA CyberSAFE CertNexus

4 ore, 3 moduli

1.0 Necessità di sicurezza informatica
2.0 Perseguire la sicurezza informatica
3.0 Navigare su Internet in sicurezza

1.0 Necessità di sicurezza informatica

1A Identificare i requisiti di conformità alla sicurezza informatica

- Privacy dei dati
- GDPR
- Principio di confidenzialità, integrità e disponibilità
- Autenticazione
  - a singolo fattore
  - a due fattori
- Password
  - Corretta gestione
  - Gestori di password
- Linee guida

1B Identificare i rischi di social engineering

- Definizione
- Obiettivi degli attacchi di social engineering
  - Furto/distruzione di dati
  - Profitto economico
  - Vendetta

- Risorse da difendere
    - Hardware/dispositivi dell'organizzazione
    - Dati e informazioni aziendali
    - Accesso alla rete
    - Accesso ai locali
    - Credenziali utente
- Principali tipologie di attacchi di social engineering
    - Phishing
    - Smishing
    - Spear fishing
    - Whailing
    - Vishing
    - Tailgating
    - Piggybacking
    - Shoulder surfer
    - Baiting
    - Pharming
    - Pretexting
    - Tailgating/piggybacking
    - Dumpster diving
- Esempi concreti di attacchi di social engineering
- Linee guida per mitigare gli attachi di social engineering

2.0 Perseguire la sicurezza informatica

2A Sicurezza fisica o passiva

- Definizione
- Risorse da difendere
- Dispositivi contenenti dati potenzialmente sensibili
    - Computer
    - Smartphone
    - Tablet

- Dispositivi di archiviazione removibile
- Requisiti per perseguire la sicurezza fisica o passiva

2B Identificare i malware, compresi i metodi di diffusione e di mitigazione

- Definizione
- Fonti dei malware
- Effetti dei malware
- Principali tipologie di malware
  - Virus
  - Worm
  - Ransomware
  - Spyware
  - Adware
  - Keylogger
  - Trojan horse
- Linee guida per prevenire i malware

2C Utilizzare i dispositivi wireless in modo sicuro

- Wireless: definizione
- Protocolli di sicurezza: WPA2
- Rete aperta e rete chiusa
- Fattori di rischio
  - Reti pubbliche
  - Reti wireless "memorizzate"
  - Evil twins
- Virtual Private Network (VPN)
- Linee guida
- Bluetooth

3.0 Navigare su Internet in sicurezza

3A Navigare sul Web in sicurezza

- Browser
  - Chrome
  - Internet Explorer
  - Edge
  - Firefox
  - Safari
- URL
  - Struttura dell'URL
  - HTTPS
  - URL sospetti
- Linee guida per navigare in sicurezza

3B Utilizzare la posta elettronica in modo sicuro

- Definizione
- Segnali di pericolo
  - Attacchi di social engineering
  - Spam
  - Programmi anti-virus fraudolenti
  - Offerte gratuite
  - Truffe monetarie
  - Richieste di informazioni
  - Grammatica ed ortografia
  - Allegati e link
- Esempi pratici di attacchi alla posta elettronica
- Linee guida per un corretto utilizzo della posta elettronica

3C Utilizzare i social network in modo sicuro

- Sicurezza dei social network
    - Condivisione di informazioni sensibili
    - Attacchi di social engineering
    - Diffusione di malware
    - Diffusione di dati personali dei dipendenti
- Linee guida per un corretto utilizzo dei social network