USARE LO SMARTPHONE IN SICUREZZA

MESSAGGISTICA ISTANTANEA: CI POSSIAMO FIDARE?

OBIETTIVI

Offrire le conoscenze per identificare i maggiori rischi nell'uso dei dispositivi mobili, in particolare nella messaggistica istantanea, e gli strumenti per utilizzarli in sicurezza, anche nel contesto aziendale.

CONTENUTI

I malware sui dispositivi mobili: come attaccano

- Android e iOS, i due principali sistemi operativi: caratteristiche e differenze per la sicurezza.
- I tanti Android: quale scegliere?
- I rischi nell'uso delle app: quali attenzioni dobbiamo adottare prima di scaricarle.
- I Ransomware su mobile.

Phishing e Smishing

- Cosa è lo smishing: alcuni esempi.
- Attenzione allo spoofing su sms e WhatsApp.
- Come usare WhatsApp in modo sicuro.
- I Social Network come mezzo di attacco sempre più usato.

Gli Spyware

- Gli Spyware negli smartphone; alcuni attacchi famosi: cosa sono e come operano gli spyware.
- Spyware... per tutte le occasioni.
- I sintomi: come capire se c'è uno spyware nel nostro smartphone.
- Come difendersi dagli spyware.

Gli strumenti per violare gli smartphone

- La vulnerabilità delle reti WI-FI.
- Come viene fatta l'estrazione dei dati da un dispositivo.
- L'acquisizione dei dati attraverso il backup.

Messaggistica istantanea (IM): ci possiamo fidare?

- WhatsApp e sistemi di chat: quanto sono sicuri?
- La crittografia end-to-end (E2E).
- Aspetti critici da valutare: i Metadati, il Backup delle chat.
- Le principali applicazioni di Messaggistica: caratteristiche e differenze.
- WhatsApp, la più diffusa; Facebook Messenger; Telegram: non solo messaggi, anche molti altri servizi (Bot, canali, ecc.); iMessage di Apple; Signal; altre applicazioni meno note: Wire, Threema, Wickr, Confide, ecc.

La prevenzione del mobile malware

- Nove regole per usare gli smartphone in sicurezza.
- Best practices di utilizzo degli smartphone in ambito aziendale.
- I sistemi MDM (Mobile Device Management).

Quota di iscrizione per persona: Eu 190,00+IVA

Info e iscrizioni: iscrizioni@tacktmi.it

www.tacktmi.it

CALENDARIO

MODULO 1 – 12 ottobre 2021 – dalle 16.00 alle 18.00

MODULO 2 – 14 ottobre 2021 - dalle 16.00 alle 18.00

La formazione è condotta in un ambiente virtuale progettato per simulare una vera classe e fornire un'esperienza di apprendimento reale.

DOCENTE

Giorgio Sbaraglia è ingegnere, svolge attività di consulenza e formazione per la sicurezza informatica e per il GDPR. Tiene corsi su questi temi per molte importanti società italiane di formazione, ricopre incarichi di DPO (Data Protection Officer) presso aziende e Ordini Professionali. E' autore di libri: "GDPR kit di sopravvivenza"; "Cybersecurity kit di sopravvivenza. Il web è un luogo pericoloso, dobbiamo difenderci!" "iPhone. Come usarlo al meglio. Scopriamo insieme tutte le funzioni e le app migliori".