L'Ordine degli Ingegneri della Provincia di Ferrara
Organizza il Seminario

LO SMARTPHONE COME STRUMENTO DI LAVORO MESSAGGISTICA ISTANTANEA: CI POSSIAMO FIDARE?

Prima Parte:
Lunedì 29.03.2021 ORE 16.00 – 18.00

Seconda Parte:
Mercoledì 31.03.2021 ORE 16.00 – 18.00

ISCRIZIONE

L'evento si svolgerà in modalità FAD sincrona sulla piattaforma GoToWebinar previa iscrizione obbligatoria sulla piattaforma www.iscrizioneformazione.it
Qualche ora prima dell'inizio dell'evento verrà inviato via mail il link tramite il quale accedere al webinar.

CREDITI FORMATIVI PER GLI INGEGNERI

Il Seminario è valido ai fini dell'aggiornamento professionale con il riconoscimento di n**. 4 crediti CFP per gli ingegneri iscritti all'Ordine della Provincia di Ferrara.**

OBIETTI DEL SEMINARIO

Prima Parte

Verranno esaminati i maggiori rischi che si corrono nell'utilizzo dell'uso dei dispositivi mobili.
Oggi gli smartphone sono diventati un'appendice del nostro corpo, un oggetto che abbiamo sempre con noi, che usiamo in modo continuo e che contiene molte informazioni e quindi rappresentano un obbiettivo molto interessante per cybercriminali e per chi ci vuole spiare.
Per questo il "classico" phishing si è trasferito anche negli smartphone, attraverso i messaggi: si parla infatti di **smishing**, cioè SMS phishing.
Esamineremo le modalità con le quali i malware penetrano negli smartphone, con tecniche che sono diverse da quelle utilizzate per i computer e faremo un confronto tra i due principali sistemi operativi: Android e iOS.
Possiamo sicuramente affermare che oggigiorno può essere molto più utile spiare uno smartphone piuttosto che rubarlo.
Spiegheremo cosa sono gli **Spyware**, applicazioni appositamente create per compiere attività di spionaggio sui nostri smartphone.

Seconda Parte

"Te lo mando con WhatsApp…".
Quante volte, nella nostra vita diciamo o sentiamo dire una frase come questa?
Oggi le applicazioni di **Messaggistica istantanea** (Instant Messaging) sono in assoluto le applicazioni più usate e più scaricate negli smartphone di tutto il mondo ed hanno rivoluzionato il nostro modo di comunicare.
Oggi WhatsApp è l'applicazione di messaggistica istantanea più diffusa al mondo, ma non è la sola
È opportuno perciò domandarsi: quanto sono sicure le applicazioni di messaggistica istantanea che tanto usiamo?
E soprattutto: possiamo usarle anche per comunicazioni riservate?
Tratteremo anche la sicurezza delle reti Wi-Fi.
Ed in conclusione si parlerà delle best practices di utilizzo degli smartphone in ambito aziendale.

PROGRAMMA DEL CORSO

Prima Parte:

Lunedì 29.03.2021 ORE 16.00 – 18.00

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.

Seconda Parte:

Mercoledì 31.03.2021 ORE 16.00 – 18.00

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.). Ma quanto è sicura?
  - **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)

DOCENTE

Giorgio Sbaraglia, 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, tra le quali la 24Ore Business School de Il Sole 24 Ore.
È membro del CLUSIT (Associazione Italiana per la Sicurezza Informatica) e certificato "Innovation Manager" da RINA.
Ricopre incarichi di DPO (Data Protection Officer) presso aziende e Ordini Professionali.

Evento realizzato con il patrocinio della

RETE PROFESSIONI FERRARA