L'Ordine degli Ingegneri della Provincia di Forlì-Cesena

organizza:

Il SEMINARIO GRATUITO

EVENTO FORMAZIONE FAD SINCRONA CIRC. CNI. 537/2020

"USARE LO SMARTPHONE IN SICUREZZA MESSAGGISTICA ISTANTANEA: CI POSSIAMO FIDARE?"

Finalità del seminario

In questo seminario verranno esaminati i maggiori rischi nell'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. Gli spyware sono

sempre più diffusi, usati talvolta in modo legale (si parla in questo caso di “captatori informatici”), ma molto spesso per fini illeciti.
“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.

QUANDO
GIOVEDI’ 20 GENNAIO 2022 ore 14.30 -18.30

DOVE
Evento Webinar Online con la Piattaforma GoToWebinar
Iscrizione attraverso il portale *www.iscrizioneformazione.it* .In seguito all’iscrizione verrà inviato due giorni prima dell’evento un Link di registrazione alla piattaforma Go ToWebinar sulla mail indicata nel portale Iscrizione Formazione al momento della registrazione. L’utilizzo del Link consentirà l’accesso alla stanza virtuale.

PROGRAMMA DEL CORSO

14.30: Collegamento alla piattaforma virtuale e Apertura dei lavori del Presidente Ordine degli Ingegneri di Forlì-Cesena

14:35 – 16.30 Inizio momento formativo:

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.

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)

16.30 – 16.40: Pausa

16.40 – 18.30:

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 e le regole per un backup sicuro

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.
- Come trattano i nostri dati personali? Le "etichette privacy".
- 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.

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 (https://www.24orebs.com/docenti/giorgio-sbaraglia).
Coordinatore scientifico del **Master "Cybersecurity e Data Protection"** della 24Ore Business School.

È membro del Comitato Scientifico 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.
È autore dei libri:

- **“GDPR kit di sopravvivenza”** (Editore goWare),
- **“Cybersecurity kit di sopravvivenza. Il web è un luogo pericoloso. Dobbiamo difenderci!”** (Editore goWare),
- **“iPhone. Come usarlo al meglio. Scopriamo insieme tutte le funzioni e le app migliori”** (Editore goWare).

Collabora con **CYBERSECURITY360** https://www.cybersecurity360.it/about testata specialistica del gruppo Digital360 per la **cyber security.**
Scrive anche per ICT Security Magazine https://www.ictsecuritymagazine.com e per www.agendadigitale.eu/ e per la rivista **CLASS**.

Il seminario è riservato ai soli iscritti all’Ordine Ingegneri della Provincia di Forlì-Cesena e riconoscerà ai partecipanti n. 4 CFP