**Commissione Industria 4.0 – Commissione Ingegneria dell'informazione – Commissione Innovazione Tecnologica**

## Seminario


# CYBERCRIME: I PERICOLI DEL WEB

# Che cosa possiamo fare per difenderci?

La Commissione Industria 4.0 in collaborazione con le Commissioni Ingegneria dell'Informazione e Innovazione Tecnologica dell'Ordine degli Ingegneri di Modena, organizza un seminario, al fine di trattare e mettere a fuoco una tematica di particolare interesse ingegneristico, quale la Sicurezza Informatica. In questo seminario verranno trattati i temi con particolare attenzione agli attacchi del Cyber Crime, alla protezione dei propri dati e dei propri account. Spiegheremo perché oggi la Cyber Security riguarda tutti noi e perché nessuno può considerarsi al sicuro: ritenere di non essere un obiettivo interessante per i cyber criminali è il miglior presupposto per essere attaccati. Gli strumenti informatici sono importanti, ma il punto debole è sempre l'uomo (il fattore "H") che con il suo comportamento può rendere inefficace qualsiasi strumento di difesa. L'uso di password

deboli è una delle principali cause (63%) della violazione e del furto dei nostri dati: cosa fare per proteggerci meglio? Non serve essere dei "geni" dell'informatica per riuscire a difendersi: basta acquisire la consapevolezza dei rischi e saperli riconoscere. In una parola: "usare la testa".

**Programma:**

- **Sabato 10 Novembre 2018**

## *IL CYBERCRIME E GLI ATTACCHI NEL WEB*

09:00 – 09:15 **Benvenuto e presentazione della giornata.**

09:15 – 12:45 **Argomenti trattati**:

**Introduzione: l'evoluzione del Cybercrime**

- I dati del crimine informatico nell'Italia e nel mondo.
- Il rapporto CLUSIT 2018.
- Cyberwarfare, la guerra cibernetica: alcuni casi famosi.
- Il Deep Web, il Dark Web, i black market, la rete TOR e il Bitcoin: cosa sono e come vengono usati.
- I danni economici generati alle aziende.

**Panoramica sulle principali tecniche di attacco**

- Gli attacchi DDoS e le Botnet.
- APT (Advanced Persistent Threat).
- Attacchi "man-in-the-middle".
- I Keylogger.

**Social Engineering, Phishing e Ransomware**

- Cos'è il Social Engineering.
- La crescita esponenziale del phishing e lo Spear phishing: come riconoscerlo e come difendersi.
- I Ransomware: cosa sono e come ci attaccano.
- Alcuni casi famosi: da WannaCry a NotPetya.
- Come difendersi dai Ransomware: la prevenzione.
- Sono stato colpito da un Ransomware: cosa fare ora?
- Implicazioni giuridiche per le vittime dei ransomware.

12.45 - 13.00 **Domande aperte**

13:00 **Fine Lavori**

**Crediti Formativi e Attestati**

Agli ingegneri che parteciperanno all'intera durata del seminario verranno rilasciati N.**4** CFP.

**Relatore:**

Il seminario è tenuto dall' Ing. Giorgio Sbaraglia

**Giorgio Sbaraglia**, ingegnere, è appassionato da sempre ai temi della sicurezza informatica. Dopo esser stato per molti anni dirigente in una grande società di costruzioni italiana, svolge oggi attività di consulenza e formazione per la sicurezza informatica e per il GDPR. Ha pubblicato il libro "GDPR kit di sopravvivenza" per la casa editrice GoWare. Tiene corsi su questi temi per molte importanti società italiane di formazioni, tra le quali la Business School de Il Sole 24 Ore. È membro del CLUSIT (Associazione Italiana per la Sicurezza Informatica) e certificato "Innovation Manager" da RINA.

www.giorgiosbaraglia.it

**Sede del seminario:**

Sala Master (edificio MO 27) del Dipartimento di Ingegneria E. Ferrari, Via Pietro Vivarelli, 10 - Modena

**Modalità di partecipazione:**

Quota d'iscrizione: **€ 25,00 + iva**

Iscrizione attraverso il portale *www.iscrizioneformazione.it*