

# Cybersecurity: mitigare gli attacchi in azienda. L'importanza del fattore umano nelle strategie di difesa.

Masterclass in diretta online il 24 e 31 maggio 2023

# Il web è diventato un luogo pericoloso? Come possiamo difenderci?

I dati aziendali sono quotidianamente esposti a minacce esterne di ogni tipo, i ransomware, i cosiddetti virus "sequestra PC" che criptano l'intero contenuto dell'hard disk e poi chiedono il pagamento di un riscatto per decifrarlo, ne sono un esempio eclatante.

I mezzi per difenderci esistono, quello che manca è la consapevolezza del problema e la conoscenza degli strumenti e delle misure quotidiane da adottare per proteggerci.



# Il corso: Mitigare gli attacchi in azienda

## Obiettivi

Obiettivo del corso è di mitigare i rischi di cyber attack causati dagli errori umani.

L'errore umano è ancora oggi la causa principale del 95% della violazione della sicurezza informatica e ciò è determinato dalla mancanza delle conoscenze necessarie da parte degli utenti.

La finalità prioritaria del corso è pertanto di garantire che tutti gli utenti finali, e non solo gli IT Specialist, conoscano le misure e i protocolli per mantenere se stessi e l'azienda al sicuro.

## Target

Il corso è rivolto ad aziende, studi professionali, associazioni, enti pubblici e in genere a tutti i soggetti che hanno necessità di proteggere i propri dati



# Il Programma

**Mercoledì 24 maggio 2023 – Ore 16.30 – 19.30**

## L'Evoluzione del Cybercrime

- I dati del crimine informatico in Italia: il rapporto CLUSIT
- Cyberwarfare, la guerra cibernetica: casi famosi
- I danni economici generati alle aziende.

## Social Engineering e Phishing

- Cos'è il Social Engineering e come si attirano gli utenti nella rete dei cybercriminali
- Le varie tipologie di Phishing

## I Ransomware: la minaccia oggi più temuta

- Come attaccano i Ransomware : i vettori d'infezione
- Come difendersi: le misure di prevenzione

**Mercoledì 31 maggio 2023 – Ore 16.30 – 19.30**

## I rischi e le vulnerabilità delle mail

- Gli attacchi attraverso la posta elettronica
- La Business Email Compromise: che cos'è e quanti danni sta creando alle aziende
- PEC e posta crittografia

## Gli attacchi verso i dispositivi mobili

- Come vengono attaccati i devices mobili
- La prevenzione del mobile malware

## Imparare ad utilizzare le password

## Mettere in pratica la Cyber Security

- L'importanza del Backup: Backup Strategy
- La sicurezza informatica come gioco di squadra

## Il Docente

Ing. Giorgio Sbaraglia

Giorgio Sbaraglia, ingegnere, è Information & Cyber Security Advisor.

È membro del Comitato Direttivo CLUSIT (Associazione Italiana per la Sicurezza Informatica) e certificato "Innovation Manager" da RINA.

Coordinatore scientifico del Master "Cybersecurity e Data Protection" della 24Ore Business School

È autore dei libri:

- "GDPR kit di sopravvivenza" Editore goWare,
- "Cybersecurity kit di sopravvivenza. Il web è un luogo pericoloso. Dobbiamo difenderci!" Editore goWare,

Collabora con CYBERSECURITY360 testata specialistica del gruppo Digital360 per la sicurezza informatica.



## **Costi di Partecipazione**

**€ 200,00 + IVA**

**Per iscrizioni superiori a n. 2**

**€ 150,00 + IVA**

## **Contatti**

**Referente**

**Francesca Sorrentino**

**E-mail**

**[fsorrentino@democonsulting.it](mailto:fsorrentino@democonsulting.it)**

**Mobile**

**+39 3456838558**