



# Tecniche pratiche di hacking per dipendenti

## Obiettivi del corso

Un'azienda può dotarsi di tutti i firewall più moderni e sicuri del mondo, ma se non istruisce i propri dipendenti sulle regole basilari di un qualsiasi attacco di hacking o di ingegneria sociale, non potrà mai definirsi sicura. Le pratiche di hacking diventano sempre più frequenti all'interno delle organizzazioni, dunque diventa necessario attrezzarsi per difendersi da tali attacchi anche attraverso la formazione del proprio personale per riconoscere tali tipologie di attacchi e segnalare prontamente a per rimediare alle azioni lesive.

Attraverso questo corso di base, i discenti acquisiranno familiarità con diverse minacce alla sicurezza del computer e della rete, come: il furto di identità, le frodi con carta di credito, il phishing sui sistemi di home banking, i virus e le backdoor, le truffe via email, la perdita di informazioni confidenziali, gli attacchi da parte di hackers e il social engineering.

Il corso di formazione è rivolto a tutti i dipendenti di un'organizzazione che tratta dati sensibili e riservati.

### Requisiti d'accesso

Il Fondo Nuove Competenze 2022-2023 dà ampio spazio al potenziamento delle competenze digital e green all'interno delle aziende, in piena linea con le indicazioni inserite nel PNRR.

### Modalità di formazione

FAD asincrona

### Durata

30

## FONDO NUOVE COMPETENZE

Il fondo finanzia il costo delle ore destinate alla formazione dei propri dipendenti: rimborsa infatti i costi sostenuti dall'azienda in relazione alle ore di lavoro destinate alla frequenza dei percorsi:

- del 100% dei contributi previdenziali ed assistenziali
- del 60% della retribuzione oraria delle ore destinate alla formazione.