# Sicurezza informatica per utenti: rischi e comportamenti nell’era dell’intelligenza artificiale

| | |
|---|---|
| CODICE | **DT0117** |
| DURATA | **1 gg** |
| PREZZO | **490,00 €** |
| EXAM | |

## DESCRIZIONE

Dalla consapevolezza all’azione: formare utenti capaci di riconoscere e prevenire le minacce digitali, anche nell’era dell’intelligenza artificiale.

Il corso fornisce agli utenti una visione chiara e aggiornata dei principali rischi legati all’utilizzo di strumenti informatici e digitali, con un focus sui comportamenti da adottare per prevenire incidenti di sicurezza.

Partendo dai concetti fondamentali della cybersecurity, il percorso affronta le minacce più diffuse (malware, phishing, furto di credenziali) e ne analizza l’evoluzione nel contesto attuale, caratterizzato da attacchi sempre più sofisticati e supportati dall’intelligenza artificiale.

Il corso integra aspetti teorici e indicazioni operative, consentendo ai partecipanti di riconoscere situazioni a rischio, utilizzare in modo sicuro strumenti digitali e comprendere il proprio ruolo nella protezione dei dati aziendali.

## OBIETTIVI RAGGIUNTI

Al termine del corso, i partecipanti saranno in grado di:

- identificare le principali minacce informatiche
- adottare comportamenti sicuri nell’uso quotidiano di strumenti digitali
- riconoscere attacchi evoluti (phishing avanzato, social engineering, deepfake)
- utilizzare in modo consapevole strumenti di intelligenza artificiale
- contribuire attivamente alla riduzione del rischio informatico aziendale

## TARGET

Utenti, dipendenti aziendali e manager

## PREREQUISTI

Conoscenze di base sull’utilizzo di sistemi operativi e strumenti digitali

**CONTENUTI**

# Introduzione alla sicurezza informatica

- Concetti base di cybersecurity
- Il ruolo dell’utente nella sicurezza aziendale
- Evoluzione delle minacce informatiche

# Minacce informatiche e tecniche di attacco

- Malware: virus, ransomware, trojan e backdoor
- Furto di credenziali e accessi non autorizzati
- Siti web malevoli e software dannoso
- SPAM e diffusione delle minacce

# Phishing e social engineering

- Phishing e spear phishing
- Smishing (SMS) e vishing (telefonate)
- Tecniche di manipolazione e ingegneria sociale
- Riconoscimento di comunicazioni sospette

# Minacce emergenti e intelligenza artificiale

- Introduzione all’uso dell’AI negli attacchi informatici
- Phishing avanzato e personalizzato
- Deepfake e impersonificazione (voce e video)
- Limiti dei metodi tradizionali di riconoscimento

# Uso sicuro degli strumenti digitali

- Navigazione sicura
- Gestione di email, allegati e link
- Password e autenticazione multifattore (MFA)
- Sicurezza nella condivisione dei dati (cloud e strumenti collaborativi)

# Uso consapevole dell’intelligenza artificiale

- Rischi legati all’uso di chatbot e assistenti virtuali
- Protezione dei dati sensibili
- Buone pratiche nell’utilizzo degli strumenti AI

# Comportamenti corretti e gestione delle minacce

- Come prevenire gli incidenti di sicurezza
- Cosa fare in caso di attacco o sospetto
- Segnalazione e gestione degli eventi di sicurezza

# Normativa e responsabilità

- Principi fondamentali del GDPR
- Protezione dei dati personali
- Cenni al D.Lgs. 231/2001 e reati informatici