

 VIDEOCORSO ONLINE

CYBERSECURITY PER TUTTI

La sicurezza informatica,
spiegata in modo semplice.

 Videocorso online |  20 ore |  Livello base



La cybersecurity riguarda tutti

Ogni giorno utilizziamo email, password, smartphone, servizi cloud e strumenti digitali per lavorare. Basta però una distrazione, un link sbagliato o una richiesta apparentemente innocua per mettere a rischio dati e sistemi aziendali.

Cybersecurity per Tutti è un videocorso pensato per fornire le conoscenze fondamentali per riconoscere le principali minacce informatiche e adottare comportamenti più sicuri nella vita lavorativa quotidiana.

Il percorso parte dalle basi ed è adatto anche a chi non possiede competenze tecniche.



20 ore di formazione



100% online



Fruizione on-demand



Livello base



Nessuna competenza tecnica richiesta





Il programma

Moduli 01-04

01



Fondamenti di Cybersecurity

Cos'è la cybersecurity
Principali minacce informatiche
Cybercriminali e loro obiettivi
Malware, ransomware e furto di informazioni
Il fattore umano
Casi reali di incidenti cyber

02



Phishing e Social Engineering

Come riconoscere il phishing
Link e allegati sospetti
Falsi siti di autenticazione
Spear phishing
Business Email Compromise
Truffe tramite SMS, telefono e QR Code
Impersonificazione e social engineering

03



Password e Protezione degli Account

Password sicure
Riutilizzo delle password
Password manager
Autenticazione a più fattori
Furto delle credenziali
Account compromessi

04



Email e Navigazione Sicura

Uso sicuro della posta elettronica
Verifica di mittenti, link e allegati
Siti web contraffatti
HTTPS
Download sicuri
Browser e aggiornamenti
Utilizzo consapevole dei servizi cloud



Il programma

Moduli 05-07

05



05 – Malware e Ransomware

- Virus, Trojan, spyware e infostealer
- Come avvengono le infezioni
- Ransomware
- Supporti USB
- Aggiornamenti e protezione degli endpoint
- Backup
- Come reagire a una possibile infezione

06



06 – Protezione dei Dati Aziendali

- Il valore delle informazioni
- Dati interni, riservati e sensibili
- Condivisione sicura dei documenti
- Email e servizi cloud
- Principio del minimo privilegio
- Protezione dei dati personali
- Condivisione involontaria delle informazioni

07



07 – Smartphone, Smart Working e Lavoro da Remoto

- Protezione di smartphone e tablet
- Wi-Fi pubblici
- Hotspot e VPN
- Smart working
- Dispositivi personali
- Furto o smarrimento dei dispositivi
- Sicurezza durante viaggi e trasferte



Il programma

Moduli 08–10

08



08 – Social Network, Intelligenza Artificiale e Nuove Minacce

- Oversharing
- Raccolta di informazioni
- Profili falsi
- Deepfake
- Truffe potenziate dall'AI
- Utilizzo sicuro dell'AI generativa
- Protezione delle informazioni aziendali

09



09 – Cosa Fare in Caso di Incidente

- Come riconoscere un incidente
- Link sospetti
- Credenziali compromesse
- Malware e ransomware
- Furto di dispositivi
- Segnalazione tempestiva
- Errori da evitare

10



10 – Casi Pratici e Scenari Aziendali

- Email sospette
- Tentativi di phishing
- Social engineering
- Falsi colleghi e dirigenti
- Link e allegati sospetti
- Compromissione delle credenziali
- Rischi durante lo smart working
- Comportamenti corretti nelle situazioni quotidiane

Più consapevolezza. Più sicurezza.



Riconoscere le
principali minacce
informatiche



Individuare
phishing e social
engineering



Proteggere
password
e account



Utilizzare
email e web
in sicurezza



Proteggere
i dati aziendali



Utilizzare
correttamente
smartphone e
servizi online



Usare
l'intelligenza
artificiale con
maggiore
consapevolezza



Riconoscere e
segnalare
rapidamente un
possibile incidente



20 ore di formazione per rendere
la sicurezza informatica parte del
lavoro quotidiano.

