

# CYBERSECURITY AWARENESS TRAINING PER AZIENDE

Formazione sulla consapevolezza per la Sicurezza  
Informatica



## Costruiamo insieme il cambiamento con consapevolezza *Cyber security threats*

La crescente digitalizzazione e la conseguente diluizione dei perimetri da mettere sotto controllo hanno creato un ambiente ideale per il proliferare dei **rischi informatici**. In questo contesto diventa fondamentale per le aziende dotarsi di un sistema di **cyber-resilincy**.

Ormai tutte le aziende si stanno adeguando all'*era digitale* con sistemi che aiutino i business ad evitare **incidenti informatici** e **data breach** che ad oggi rappresentano un danno spesso ingente e alla luce delle norme previste dal *Regolamento Generale sulla Protezione dei Dati (GDPR)*, possono essere causa di consistenti multe. Ma, spesso, nonostante un'infrastruttura sicura e un *security plan strutturato*, entra in gioco l'*HUMAN FACTOR*, quell'errore umano che può vanificare i nostri sforzi.

Come affrontare con successo le nuove frontiere e fare in modo che i cambiamenti che affrontiamo ogni giorno diventino una **risorsa** per l'azienda, invece che un ostacolo? È indispensabile favorire la comprensione di nuovi **modelli** e **processi**, fornire alle persone **nuovi strumenti** e **competenze**.

Per questo motivo Security Architect si occupa anche di **awareness**: sensibilizzazione, training e formazione aziendale.



Nata nel 2005 dalla passione e dall'esperienza nel settore informatico, **Security Architect Srl** è diventata importante riferimento di molte grandi aziende. Da 15 anni opera nel settore ICT, offrendo soluzioni IT e per la sicurezza informatica. Grazie al costante aggiornamento, agli alti standard qualitativi, all'innovazione e all'affidabilità delle soluzioni offerte riesce ad essere sempre un passo avanti rispetto ai propri competitors.

### EMAIL

[info@securityarchitect.it](mailto:info@securityarchitect.it)

### PHONE

080 671053

080 8756269

### SEDE CENTRALE

Via Salvatore Matarrese, 36  
70124 Bari (BA), Italia

# In cosa consiste il corso

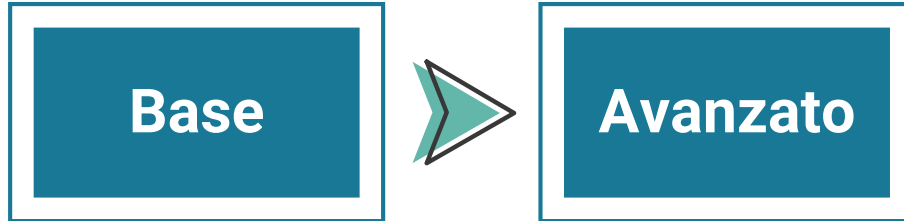
## Cybersecurity Awareness Training

Il corso si rivolge a tutto il personale **non tecnico**, al fine di fornire a tutti i collaboratori gli strumenti e le conoscenze di base per comprendere i reali rischi e le responsabilità delle azioni messe in atto.

Ha lo scopo di aiutare gli utenti a diventare la nostra ultima linea di **difesa** piuttosto che vittime digitali.














La **formazione** fornisce il contesto e suggerimenti pratici sul riconoscimento delle minacce e delle azioni scorrette, avendo effetto immediato sulla sicurezza nell'ambiente di lavoro.

## Moduli Formativi



I livelli proposti sono personalizzabili a seconda delle esigenze aziendali e integrabili con **moduli specifici**.

### Argomenti trattati:

-  Cybersecurity, introduzione al tema
-  Web security e minacce in rete
-  Regolamento Generale per la protezione dei dati
-  Furto e perdita dei dati, come evitarli
-  Gli attacchi informatici e i loro sviluppi
-  I criminali informatici e a cosa mirano
-  Hacking basic dictionary
-  Utilizzo consapevole della posta elettronica e relative minacce (**Phishing, Hoax...**)
-  Password, il giusto utilizzo
-  BYOD, come gestire i propri device
-  Aggiornamenti dei sistemi
-  Sicurezza dei dati finanziari
-  Lavoro agile e cybersecurity

### Vantaggi:

- Rafforzare la sicurezza informatica aziendale
- Non incorrere in danni economici e di immagine
- Comprendere i concetti di base della sicurezza informatica e la terminologia delle minacce come: *phishing, Hoax, spyware e malware*
- Responsabilizzare e rendere consapevoli dei rischi affrontati da organizzazioni e individui
- Comprendere alcuni dei modi in cui queste minacce possono influenzare e avere un impatto sull'azienda
- Fornire suggerimenti e metodi pratici su come identificare le minacce tipiche di posta elettronica e web
- Apprezzamento delle responsabilità legali, normative e gestionali per la protezione del business
- Sapere a chi e come segnalare violazioni e incidenti.