

CORSO BASE DI SICUREZZA INFORMATICA PER AZIENDE E PROFESSIONISTI SECONDO ISO/IEC 27001:2022

Formazione pratica per prevenire e gestire gli attacchi informatici di ogni giorno

organizzato da **aicq** in collaborazione con **Trident s.r.l.** su mandato di **AICQ ER**

OBIETTIVI: Impara a riconoscere le truffe, proteggere account e dati, e lavorare online in sicurezza con procedure semplici.

Al termine, AICQ rilascerà l'attestato di frequenza (8 ore); valido anche per l'edizione DAD (online-live) con tracciamento presenze.

PROGRAMMA:

Mattina - Parte Teorico-Pratica Base (09:00 - 13:00)

- 09:00 - 09:30 | Introduzione alla Sicurezza Informatica
 - Cos'è la cybersecurity e perché riguarda tutti
 - Esempi concreti di attacchi aziendali
 - Obiettivi del corso
- 09:30 - 10:15 | Le Minacce Più Comuni
 - Phishing, smishing e vishing (email, SMS e chiamate truffa)
 - Malware, ransomware e trojan
 - Social engineering: trucchi psicologici per ingannare l'utente
- 10:15 - 10:30 | Pausa caffè
- 10:30 - 11:15 | Password e Autenticazione
 - Cosa rende sicura una password
 - Gestori di password: uso sicuro (es. Bitwarden, KeePass)
 - Autenticazione a 2 fattori (2FA): perché è indispensabile
- 11:15 - 12:00 | Navigazione e Posta Elettronica Sicura
 - Riconoscere siti truffa e link sospetti
 - Estensioni utili per la sicurezza del browser (HTTPS HTTPS-Only Mode, uBlock Origin) - Trucchi per evitare allegati malevoli e link fasulli
- 12:00 - 13:00 | Laboratorio Pratico 1
 - Simulazione email phishing con quiz interattivo
 - Analisi di una finta email pericolosa
 - Esercizio su creazione password sicure



Pomeriggio - Parte Pratica e Aziendale (14:00 - 18:00)

- 14:00 - 14:45 | Dispositivi e Account: Uso Sicuro
 - Differenza tra dispositivi aziendali e personali
 - Uso corretto della rete aziendale e del Wi-Fi pubblico
 - Protezione dei dispositivi mobili e portatili
 - 14:45 - 15:30 | Privacy, dati personali e GDPR
 - Cosa dice il GDPR (in modo semplice)
 - Come trattare i dati di clienti e colleghi
 - Errori comuni che violano la privacy
 - 15:30 - 15:45 | Pausa caffè
 - 15:45 - 16:30 | Laboratorio Pratico 2
 - Navigazione in sicurezza con esercizi su browser
 - Simulazione di accesso a siti malevoli (in ambiente sicuro)
 - Esercizio di riconoscimento URL falsi
 - 16:30 - 17:30 | Incidenti e Policy Aziendali
 - Come riconoscere un'infezione o compromissione
 - Cosa fare / non fare in caso di sospetto attacco
 - Politiche aziendali: comportamenti richiesti
 - 17:30 - 18:00 | Conclusioni e Q&A
 - Ripasso dei punti chiave
 - Domande dei partecipanti
 - Suggerimenti per approfondire e link utili
- Materiale da preparare (consigliato)
- Slide sintetiche (massimo 6 punti per slide)
 - PDF riassuntivo delle "10 regole d'oro"

A CHI È RIVOLTO

Impiegati d'ufficio, segreterie, amministrativi, HR, vendite, contabilità, magazzino/logistica, liberi professionisti e titolari di PMI. Adatto a chi usa PC, email e smartphone per lavoro.

DOCENTE

Giuseppe Lorenzo RUMIATO

Giuseppe Lorenzo Rumiato è un ingegnere in telecomunicazioni, analista e programmatore, formatosi a partire dagli anni Settanta, quando l'indirizzo "Informatica" non era ancora presente nelle università italiane. Nel tempo ha focalizzato la propria attività sulla sicurezza informatica, trasformando l'esperienza maturata sul campo in competenze operative e didattiche.

Dopo un passato di analista di tecniche degli hacker che gli ha permesso di sviluppare competenze avanzate, oggi impiegate per prevenire e contrastare attività informatiche illecite, ha intrapreso il percorso da ethical hacker (white hat). Tra il 2002 e il 2004 ha collaborato con gli apparati di sicurezza della Presidenza del Consiglio dei ministri in operazioni a vario titolo e ha ricoperto anche il ruolo di istruttore in cybersecurity e tutor per gli iscritti agli esami (esaminandi).

Oggi collabora con TRIDENT S.R.L., dove porta in aula casi reali, metodologie e buone pratiche per aiutare aziende e professionisti a prevenire, rilevare e rispondere agli attacchi informatici.

Si ricorda che il corso 8 ore
è qualificato da AICQ SICEV.



Costo € 1.400 + IVA

DATI ISCRIZIONE

Il pagamento dovrà avvenire prima dell'inizio del corso. È indispensabile iscriversi al corso inviando il presente modulo a segreteria@aicqer.it con allegata copia del bonifico e con le seguenti informazioni del partecipante:

Cognome
Nome
C.F. Cellulare
Email

☐ corso 8 ore completo

- ☐ Non Iscritto AICQ Emilia Romagna
- ☐ Iscritto AICQ Emilia Romagna
- ☐ Nuovo Iscritto AICQ Emilia Romagna anno 2025

Intestazione fattura:

Ragione Sociale
Indirizzo
Città Cap
P.I. C.F.
Codice Destinatario SdI (campo obbligatorio se diverso da P.IVA)
Telefono Fax
E-mail

Seguirà da parte della segreteria di AICQ Emilia Romagna conferma dell'iscrizione tramite e-mail.



Periodo: Settembre–Ottobre 2025 • 1ª edizione: 22 settembre 2025 • Modalità: DAD (online-live su Zoom)
Massimo 12 iscritti; priorità in ordine di arrivo.