CORSO BASE SULLA SICUREZZA E SUI RISCHI INFORMATICI NELL'ATTIVITÀ LAVORATIVA DEI DIPENDENTI DELLA PA: RISCHI, REGOLE E BUONE PRATICHE

TORNA AL CATALOGO CORSI

Data inizio corso:
04/07/2025

Orario:
9.00-13.00

Sede:
Online in diretta

DOCENTE

Dott. ALFONSO PISANI
Responsabile servizio di innovazione tecnologica, sistemi informativi e gestione documentale informatizzata Ente Locale.

ISCRIVITI ONLINE
STAMPA IL PROGRAMMA
ABBONAMENTI
RICHIEDI PREVENTIVO

In conformità alla **Direttiva Zangrillo 2025** il presente corso si qualifica come intervento formativo specialistico, per contenuti, modalità erogative e livello di apprendimento.

DESTINATARI

Tutto il personale di uffici privati e della Pubblica Amministrazione.

PRESENTAZIONE

Il presente seminario ha lo scopo di descrivere le problematiche di sicurezza connesse alla digitalizzazione dei processi e le corrispondenti misure mitigatrici che possono essere messe in campo nel lavoro quotidiano. Il fattore umano è il vettore di attacco principale da parte dei criminali informatici, oltre ad essere una delle cause anche accidentali di perdita o compromissione di dati e problematiche connesse alla continuità operativa.
Il corso verrà tenuto in un linguaggio semplice, ricco di esempi e riferimenti all'attività lavorativa quotidiana proprio allo scopo di diffondere a diffondere la cd cyber security awareness (termine che possiamo tradurre con consapevolezza dei rischi informatici) tanto importante sia per AGID che per l'Agenzia per la Cybersicurezza Nazionale tenendo conto, in particolare, degli utenti con meno esperienza in materia informatica.

PROGRAMMA

I sessione (9:00-11:00)

1. RISCHI E MINACCE NEGLI AMBIENTI DIGITALI
   - La sicurezza informatica: proteggersi da chi e da cosa.
   - I principali rischi per i dati:
     - la perdita di confidenzialità,
     - la distruzione,
     - l'alterazione,
     - l'indisponibilità.
   - I principali rischi per gli utenti ed i sistemi:
     - l'accesso abusivo,
     - il furto delle credenziali,
     - l'impersonificazione ed altro.
   - I principali tipi di attacco informatico:
     - Gli attacchi ai servizi:
       - il denial of service (DoS),
       - il distributed denial of service (DDoS).
   - Le principali tipologie di software maliziosi informatici:
     - malware in generale,
     - virus,
     - rootkit,
     - cavalli di troia.
   - I malware spia: Spyware e keylogger.
   - I malware che ingannano: gli scareware/roguaware.
   - I malware che ricattano: i ransomware.

II sessione (11:15-13:15)

1. MISURE BASE DI SICUREZZA
   - L'impossibilità di ridurre a zero i rischi e l'importanza del contributo degli utenti.
   - La custodia delle credenziali.
   - L'uso consapevole della mail.
   - La mail di phishing e spamming..buone prassi per il riconoscimento
   - I filtri antiphishing ed antispam come funzionano, alcuni approcci basati sull'intelligenza artificiale
   - La navigazione in rete.
   - L'importanza di avere le postazioni di lavoro in dominio.
   - L'aggiornamento del sistema operativo.
   - Le buone prassi da adottare.
   - La gestione corretta delle password.
   - Gli attacchi a forza bruta.
   - Gli attacchi a dizionario.
   - La lunghezza della password.
   - Il cambio periodico della password e come scegliere la nuova password: policy e buyone pratiche per la scelta
   - I rischi di perdita accidentale dei dati: l'uso del backup e delle cartelle condivise sui server.
   - Il lavoro agile e l'uso dei dispositivi personali: una nuova fonte di rischio.
   - Internet, la intranet, le connessioni VPN e virtual desktop environment pro e contro
   - La sicurezza informatica ed il lavoro agile: le raccomandazioni a cura di AgID e dell'Agenzia per la Cybersicurezza Nazionale e la loro applicabilità in contesti differenziati.
   - La cybersecurity awareness nel Piano Triennale per l'Informatica nella PA
   - Alcuni strumenti online per il riconoscimento di malware, URL dannosi e minacce informatiche
2. Le misure minime di sicurezza ICT:
   - Le linee guida AGID del 2017.
   - I livelli minimo, standard ed avanzato.

MODALITÀ DI PARTECIPAZIONE

Lezione frontale interattiva a distanza, analisi di buone pratiche e casi studio. Il corso, della durata di 120 minuti per ogni sessione, consiste in una video lezione in streaming con presentazione di slides. Al termine del corso verranno consegnate le credenziali di accesso alla nostra area riservata, all'interno della quale è possibile trovare l'attestato di partecipazione, la videoregistrazione e i materiali del corso. L'accesso all'area riservata è disponibile per 15 giorni dalla data di attivazione.

L'accesso alla piattaforma avverrà tramite un link che sarà inviato all'indirizzo mail del partecipante ad iscrizione avvenuta. Sarà sufficiente disporre una connessione stabile ad internet e un sistema audio con casse o cuffie.

Per maggiori informazioni e assistenza è possibile rivolgersi alla segreteria di PAcademy al numero 049-777029 o all'email info@pacademy.eu

QUOTE DI PARTECIPAZIONE E SCONTI*

	Quota a partecipante Iscrizioni Entro 20/06/25	Quota a partecipante Iscrizioni Dopo 20/06/25
Enti pubblici o Privati	**315,00 EUR** (Sconto 10%) Codice MEPA: PACAD2	**350,00 EUR** Codice MEPA: PACAD1
Quota Clienti Psychometrics**	**300,00 EUR** (Sconto 15%) Codice MEPA: PACAD3	**315,00 EUR** Codice MEPA: PACAD2