Ing. Saverio Rubini

Sicurezza informatica: strumenti, tecniche e metodologie per prevenire, reagire e rimediare agli attacchi

Codice corso
RSI015

Durata
5 giorni, in date da stabilire con il committente.

Orario
9-13 (in alternativa 14-18, a seguito di accordi con il committente).

Quota di partecipazione
--,00 € + IVA

Docente
Ing. Saverio Rubini
Docente in master universitari e corsi di formazione professionale, esperto di sicurezza informatica e di tecnologie di comunicazione digitale, consulente aziendale di organizzazione informatica e di Intelligenza Artificiale, sistemista di rete, progettista e creatore di siti Internet, autore di libri e articoli di informatica (Apogeo, Il sole 24 ore, McGraw-Hill).

Obiettivi
Acquisire una solida base di **competenze** in **sicurezza informatica e protezione dei dati**.
Sentirsi più sicuri e autonomi nell'uso delle tecnologie digitali in Rete.
Conoscere i tipi di **malware** e le **tecniche truffaldine** che minacciano chi lavora con il computer: tipi di attacchi, obiettivi, come prevenirli.
Essere in grado di installare, configurare e **utilizzare strumenti software e tecniche** per difendersi.
Saper ripristinare la funzionalità di un **sistema** elaborazione dati **nel caso di attacco conclamato** e segnalare l'evento ai dovuti destinatari.

Sede
Le lezioni sono tenute in presenza nella sede messa a disposizione dall'organizzazione che invia l'ordine con il supporto di elaboratori elettronici con sistema operativo Windows e collegati in Internet, nei quali è installato Microsoft Office.

Destinatari

Utenti che desiderano saper utilizzare consapevolmente il computer e le apparecchiature informatiche per lavorare, comunicare, trasmettere e ricevere documenti informatici via Internet con la massima sicurezza possibile.

Prerequisiti

L'intervento formativo è rivolto ad utenti che utilizzano computer/smartphone collegati in Internet e hanno interesse ad aumentare il livello di sicurezza, evitare di commettere azioni inappropriate e sapere cosa fare e come intervenire nel caso di incidente o di presenza di situazioni anomale (*problem solving*).

Supporto e materiali didattici

Ogni modulo didattico comprende prove pratiche per acquisire competenze materiali svolte con le apparecchiature informatiche fornite in aula dal committente.
Durante le lezioni vengono forniti assistenza e supporto individuale.
Dispense e materiali didattici di ogni lezione sono forniti in formato digitale.

Rilascio attestato di frequenza e profitto

Al termine del corso, a ogni partecipante viene rilasciato un attestato con le caratteristiche del percorso formativo e quanto è stato frequentato (come risulta dai fogli di presenza).

Programma

Giorno 1

- **Sicurezza informatica: perché è importante proteggersi**
  - Competenze digitali nella vita quotidiana e nel mondo del lavoro, perimetro di attacco, comportamenti personali, copie
    - prova pratica: rilevazione dei componenti hardware e software del proprio computer
    - navigazione in siti di informazione sulla sicurezza informatica
- **Sicurezza informatica nei comportamenti in ufficio: cosa fare e cosa no**
  - Utilizzo di risorse aziendali, pericoli con la posta elettronica, attacchi con phishing, rapporto con colleghi e terzi
    - prova pratica: verifica se sono stati violati i dati di accesso personali
    - prova pratica: verifica antivirus online dei file, prima dell'apertura
- **Sicurezza informatica nell'accesso (Identità digitale)**
  - Come avere password affidabili, CIE/CNS/TS/SPID/eIDAS, accessi con tecniche multifattore
    - prova pratica: richiesta di registrazione a SPID
    - prova pratica: attivazione modalità di accesso in Windows diverse da utente/password

Giorno 2

- **Sicurezza informatica con i documenti informatici e i programmi di produttività**
  - Dati e informazioni, dati sensibili/giudiziari (GDPR), documenti e file, crittografia e firma digitale in pratica, protezione dati in Microsoft Office
    - prova pratica: verifica e protezione dei dati nei documenti di Microsoft Office
    - prova pratica: utilizzo password di apertura/modifica nei documenti Word
    - prova pratica: inserimento password in file compressi (ZIP/RAR)
- **Sicurezza informatica con le apparecchiature**
  - Hardware, software, tipi di memorie, il *cloud*, smartphone/tablet, IoT (Alexa, Google Home, smartwatch)
    - prova pratica: elencazione dei dispositivi presenti in ufficio
    - prova pratica: individuazione di tutte le porte presenti in un portatile
    - prova pratica: utilizzo di un motore di ricerca nei dispositivi IoT
- **Sicurezza informatica: software di base e software applicativo**
  - Sistema operativo, driver, programmi applicativi, app, vulnerabilità, aggiornamenti

- prova pratica: verifica dei programmi da aggiornare
- prova pratica: installazione programmi con aggiornamento automatico

- **Sicurezza informatica con il sistema operativo**
  - Windows, Linux, MacOS, Android, iOS, file e cartelle, *file system*, formati e nomi dei file, configurazione Windows per protezione dati
    - prova pratica: navigazione nelle impostazioni di Microsoft Windows
    - prova pratica: navigazione nelle impostazioni di Android

Giorno 3

- **Sicurezza informatica con le reti**
  - Reti locali (LAN-WLAN) e reti geografiche (WAN), Internet e intranet, indirizzi IP, *switch*, *router*, collegamenti con cavi e senza fili (Wi-Fi), reti telefoniche 3G/4G/5G, VPN
    - prova pratica: verifica e impostazione parametri della scheda di rete (IP, DNS)
    - prova pratica: configurazione di un router in una piccola rete
- **Sicurezza informatica in Internet: come proteggersi e difendersi**
  - I browser, difesa dagli attacchi, estensioni di protezione, cronologia, cookie, Javascript
    - prova pratica: configurazione del browser
    - prova pratica: pulizia dati memorizzati dal browser
    - prova pratica: installazione estensioni di protezione
    - prova pratica: navigazione con il browser Tor nel *dark* web
- **Sicurezza informatica nelle ricerche in Internet**
  - Motori di ricerca, ricerche efficaci, ricerche con l'Intelligenza Artificiale, protezione dei dati e della *privacy*, *deep* e *dark* Web
    - prova pratica: ricerche mirate utilizzando appositi operatori
    - prova pratica: utilizzo dell'applicazione di Intelligenza Artificiale generativa ChatGPT
    - prova pratica: generazione di testi
    - prova pratica: generazione di immagini e di grafica di presentazione

Giorno 4

- **Sicurezza informatica con la posta elettronica e i programmi di comunicazione in rete**
  - Posta elettronica, Outlook e Webmail, pericoli nei collegamenti e negli allegati, PEC, videochiamate (Microsoft Teams, Google Meet, Webex), lavoro agile, WhatsApp
    - prova pratica: collegamento a distanza con attivazione delle condivisioni
    - prova pratica: dividere un file di grandi dimensioni in parti

- **Sicurezza informatica con i siti Internet (privati, *e-government*, servizi finanziari)**
  - Dati obbligatori nei siti, servizi bancari, siti di commercio elettronico, pubblica amministrazione, fatturazione elettronica
    - prova pratica: verifica presenza dei dati obbligatori in siti Internet
    - prova pratica: navigazione in Agenzia Entrate, INPS, Fascicolo Sanitario Elettronico
- **Sicurezza informatica con immagini e filmati**
  - Siti con filmati video, visualizzazione con VPN di video protetti
    - prova pratica: accesso a filmati con VPN
- **Sicurezza informatica con le reti sociali**
  - Facebook/WhatsApp: configurazione, a cosa fare attenzione
- **Sicurezza informatica con il *cloud***
  - Condivisione dei file, elaborazione contemporanea dei documenti, come utilizzarlo per proteggere i propri file
    - prova pratica: trasferimento e condivisione file in Microsoft OneDrive e Google Drive
    - prova pratica: elaborazione contemporanea di documenti

Giorno 5

- **Sicurezza informatica, malware e attacchi**
  - Tipi di attacchi, finalità, virus, *worm*, troiani, *criptojacker*, *ransomware*, *backdoor*, *rootkit*, *spyware*, *hacker*, APT, SCADA
    - prova pratica: programmi per la protezione da *rootkit*
- **Sicurezza informatica: software di protezione, tecniche di prevenzione e di intervento**
  - Logiche e tipi di difese, antivirus, firewall, cancellazione memorie per dismissione
    - prova pratica: utilizzo programmi di protezione
    - prova pratica: configurazione di un programma antivirus
    - prova pratica: verifica dei dati delle schede di rete
- **Sicurezza informatica: proteggersi con le copie degli archivi (*backup* e *restore*)**
  - NAS, sincronizzazione, tecniche e programmi di *backup*, modalità di ripristino delle funzionalità del sistema informatico
    - prova pratica: programma di sincronizzazione dei file tra due unità di memoria
    - prova pratica: trasferimento dati da e verso il cloud
- **Sicurezza informatica nell'ambiente, ergonomia e prodotti di consumo**

- Illuminazione, umidità, temperatura, segnali elettromagnetici, alimentazione elettrica, postazione, postura, come evitare possibili patologie articolari e della vista, smaltimento prodotti di consumo
  - prova pratica: impostazione della postura corretta con computer, mouse e schermo

- **Sicurezza informatica: conoscenza delle principali regolazioni (leggi, direttive)**
  - Diritto d'autore, protezione dati (GDPR), NIS 2, Legge *cyber* italiana 90/2024 per le pubbliche amministrazioni (in vigore dal 17/07/2024), D.Lgs. 138/2024 per tutte le organizzazioni pubbliche e private (in vigore dal 16/10/2024)
    - prova pratica: verifica di quali disposizioni riguardano la propria attività