

CORSO DI CYBER SECURITY (120 Ore)

Obiettivi: I partecipanti acquisiranno le competenze necessarie per gestire la sicurezza informatica e la tutela della privacy, acquisendo nozioni di come navigare, ricercare, proteggersi dalle possibili frodi informatiche. Come utilizzare gli strumenti di posta elettronica evitando di incorrere in phishing. Tutelare la propria identità digitale e usufruendo di Vpn per mantenere sicura la propria navigazione. Panoramica generale di base sulla GDPR (tutela della privacy). Tutelare i propri dati personali e file con l'uso di protezione crittografate e l'uso della doppia convalida nell'uso delle password. Verranno svolti esercitazioni pratiche (reali) di casi di frodi come evitarli e come anticiparli anche inerente ad annunci di lavoro (rubare l'identità digitale).

Figura professionale in uscita: Addetto Cyber Security.

Modulo 1 (8h teoria - 8h pratica)

Definizione di Cyber Security. Web Quali sono i pericoli che nasconde, come riconoscerli ed evitarli. Navigare in internet con strumenti (identità nascosta). Definizione di Vpn e come usarlo nei casi reali e pratici.

Modulo 2 (4h teoria - 4h pratica)

E-mail: perché è diventata il primo veicolo di attacco. Cos'è il phishing e come riconoscerlo. Usare i servizi di provider più sicuri e l'uso dell'e-mail più consapevole.

Modulo 3 (4h teoria - 4h pratica)

Esempi di Phishing e corrette modalità di risposta. E-mail SCAM e SPAM. Uso inappropriato delle e-mail.

Modulo 4 (4h teoria - 4h pratica)

Social Network: informazioni a disposizione di tutti, come evitare di esporre l'azienda e se stessi a rischi. Il Social Engineering e le sue forme, cosa c'è da sapere e quali accortezze usare. Privacy e sicurezza. Le tracce della navigazione

Modulo 5 (4h teoria - 4h pratica)

Come evitare di esporsi a furti di dati e informazioni. App lecite ed illecite: come riconoscerle e quali rischi comportano.

Modulo 6 (4h teoria - 4h pratica)

Privacy: a chi servono i nostri dati e come tutelarli. Cookies, come siamo tracciati, controllati e profilati.

Modulo 7 (4h teoria - 4h pratica)

La normativa europea sulla privacy UE 2016/679 (GDPR): cenni.

Modulo 8 (4h teoria - 4h pratica)

Nozioni tecnologiche di base per utenti. La gestione del PC e delle identità. Strumenti mobili, laptop e Smart device: come usarli in modo sicuro all'esterno dell'organizzazione.

Modulo 9 (4h teoria - 4h pratica)

Gestione Utenti e Password. Guida all'uso delle Password e mantenimento.

Modulo 10 (4h teoria - 4h pratica)

Software Patch Updates & Gestione Anti- Virus.



Modulo 11 (4h teoria - 4h pratica)

Consigli utili in ambito aziendale per la tutela e la condivisione sicura dei dati. Best Safety Practices. Come implementare in autonomia le misure minime di sicurezza (convalida doppia password).

Modulo 12 (6h teoria - 6h pratica)

Configurazioni di sicurezza del browser.

Modulo 13 (2h teoria - 2h pratica)

Pulizia della cache e salvataggio delle password (App e programmi per usare la Key unificata) e generatore random di password per rendere sicuro la propria identità digitale e i dati.

Modulo 14 (Moduli Obbligatori)

D.lgs 81/08: Salute e Sicurezza sui Luoghi di Lavoro (4h teoria)

Diritti e Doveri dei Lavoratori Temporanei (4h teoria)