Collana CYBERSECURITY

Collana
CYBERSECURITY

Concetti di base per la sicurezza online

Come minimo, la maggior parte delle persone chiude le porte quando esce. Altri installano luci sensibili al movimento o telecamere di sicurezza. Alcuni investono in sistemi di allarme per proteggersi dalle minacce.

Ma le misure di salvaguardia non riguardano solo gli spazi fisici: ormai tutti archiviano I dati sensibili online. Le conseguenze, in caso di perdita di questi dati sono spesso più devastanti della perdita di oggetti di valore a causa di un ladro.

In questo breve corso imparerai le strategie per proteggerti online e otterrai suggerimenti per bloccare le minacce in arrivo. Infine, esaminerai come agire rapidamente per ridurre al minimo i danni in caso di violazione della sicurezza.

Contenuti del corso

1. Cos'è la sicurezza informatica?
2. Buone pratiche per una navigazione Internet sicura
3. Suggerimenti per la sicurezza del Wi-Fi pubblico
4. Uso sicuro dei social media
5. Affrontare un incidente di sicurezza
6. Test Finale

DURATA CORSO
30m

Collana
CYBERSECURITY

Come difendersi dagli attacchi Phishing

Il corso è rivolto a tutte le persone che quotidianamente interagiscono con **risorse digitali**, sia in ambito domestico, che in ambito lavorativo, con l'obiettivo di fornire una maggiore consapevolezza alle persone riguardo le **più comuni minacce** in cui la componente umana viene sfruttata come vettore principale.

E' incentrato su quelle minacce che possono essere sfruttate da un attaccante **per raccogliere informazioni sensibili o rappresentare una persona fidata**, con lo scopo di **innalzare il livello di sicurezza** nell'utilizzo dei **dispositivi sia aziendali che personali**, riconoscendo queste minacce e riuscendo a difendersi da esse.

Contenuti del corso

1. Introduzione
2. Link Malevoli
3. Business E-mail Compromise
4. Spear Phishing & Malware
5. Look alike & Sub-Domain Attack
6. Test Finale

DURATA CORSO
40m

Collana
CYBERSECURITY

Come proteggere i dati

I **furti odierni** non sono solo le rapine e i furti con scasso, come avveniva nel passato.
Si sono **evoluti anche nella sfera digitale**, richiedendo di apprendere **nuove pratiche di sicurezza**, da associare a quelle esistenti.

In questo corso, scopriremo **cosa sono i dati riservati**, perché è importante **mantenerli al sicuro** e le migliori e indispensabili pratiche di sicurezza che includono sia il cyberspazio sia le strutture fisiche.

Verranno inoltre approfonditi strumenti come le **password complesse**, l'**autenticazione a più fattori** e le **misure di sicurezza fisica** per la protezione delle risorse.

Contenuti del corso

1. Introduzione
2. Cosa sono i dati riservati
3. Come proteggere le informazioni riservate
4. Creazione e gestione di password complesse
5. L'autenticazione a più fattori
6. Dispositivi portatili e supporti rimovibili
7. Utilizzo della sicurezza fisica per mantenere al sicuro le risorse

DURATA CORSO
25m

Collana
CYBERSECURITY

Difendersi dal social engineering

Il **social engineering è l'arte della manipolazione per rubare informazioni.** A differenza dei crimini informatici che implicano il cracking di algoritmi complessi, **si basa sul comportamento umano** prevedibile **per convincere** le vittime a rivelare informazioni.

Il corso fornisce una panoramica di come i social engineers sfruttano la psicologia umana per accedere a informazioni sensibili, oltre a suggerimenti per individuare gli attacchi. Essendo **consapevoli di questi pericoli**, avremo meno probabilità di cadere vittima di varie forme di manipolazione.

Contenuti del corso

1. Cos'è il social engineering?
2. Come funziona
3. Tipologie d'attacco
4. Come identificare un attacco
5. Test Finale

DURATA CORSO
15m

Collana
CYBERSECURITY

Furto d'identità, privacy e GDPR

Ti sei mai chiesto cosa succederebbe se qualcuno diventasse te con un semplice clic?

Il **furto d'identità,** noto anche come frode d'identità, è un crimine in cui l'impostore ottiene e utilizza nostre informazioni personali d'identità con cui possiamo essere identificati come ad esempio il numero di un nostro **documento**, il **codice fiscale** o altro, per impersonare qualcun altro.

Le **informazioni possono essere utilizzate per ottenere credito, merci e servizi** a nome della vittima o per fornire al cyber criminale **false credenziali** e le conseguenze possono essere gravi e durature, incidendo sulla sicurezza personale, economica e sulla reputazione della vittima.

Contenuti del corso

DURATA CORSO

30m

Collana
CYBERSECURITY

Minacce data leakage alla cyber sicurezza

Il data leakage rappresenta una delle minacce più insidiose per la cyber sicurezza, capace di mettere a rischio informazioni sensibili e la reputazione aziendale.

In questo corso scoprirai **cos'è il data leakage, quali rischi comporta** per le organizzazioni e come **riconoscere comportamenti a rischio**.

Imparerai inoltre le strategie e le **best practice** fondamentali **per prevenire la perdita di dati**, applicandole concretamente nell'attività quotidiana.

Contenuti del corso

1. Cos'è il data leakage e perché è una minaccia
2. Prevenzione del data leakage
3. Test finale

DURATA CORSO
15m

Minacce introdotte dalla AI

In un mondo sempre più digitalizzato, la comprensione delle minacce legate all'AI è diventata fondamentale per ogni professionista.
Non si tratta solo di **conoscere i rischi**, ma di essere in grado di **anticiparli e affrontarli** con competenza.
In questo corso, **imparerai a riconoscere le principali minacce legate all'AI**, identificare attacchi, rischi reali e allucinazioni, apprendendo come adottare comportamenti sicuri nell'uso degli strumenti digitali. Attraverso un approccio pratico e interattivo, esplorerai vari scenari in cui l'IA può essere **sfruttata in modo improprio**, e come questi possono impattare le aziende. Grazie a esempi pratici e linee guida chiare, acquisirai le competenze necessarie per **proteggere i dati aziendali** e contribuire attivamente alla sicurezza informatica dell'organizzazione. Imparerai a riconoscere i segnali di allerta, a implementare misure preventive e a rispondere in modo efficace a potenziali minacce.

Contenuti del corso

1. I rischi legati all'uso dell'intelligenza artificiale
2. Esempi pratici di attacchi e rischi aziendali utilizzando l'AI
3. Comportamenti sicuri e buone pratiche per la protezione dei dati aziendali
4. Il pericolo delle allucinazioni AI
3. Test finale

DURATA CORSO
15m

Collana
CYBERSECURITY

Minaccia phishing usando SPID e PEC

Il corso è rivolto a tutte le persone che quotidianamente interagiscono con risorse digitali, con l'obiettivo di fornire una maggiore **consapevolezza riguardo ai pericoli del phishing**, in particolare quando si utilizzano **SPID** e **PEC**.

È fondamentale riconoscere come gli attaccanti possano sfruttare queste **identità digitali** per raccogliere informazioni sensibili o impersonare una persona fidata.

Il corso si concentra sulle minacce specifiche legate al phishing, evidenziando come **proteggere** le proprie credenziali e garantire la **sicurezza** nell'utilizzo di **dispositivi aziendali e personali.**

Contenuti del corso

1. Evoluzione delle minacce digitali
2. Il phishing oggi
3. SPID: il bersaglio perfetto
4. PEC: sicurezza e minacce
5. Test finale

DURATA CORSO
15m

Collana
CYBERSECURITY

Phishing: sottovalutazione del rischio e contro-misure

Il corso è rivolto a tutte le persone che quotidianamente interagiscono con risorse digitali, con l'obiettivo di aumentare la consapevolezza riguardo alla sottovalutazione del fenomeno phishing.
Spesso, infatti, le persone non percepiscono il rischio reale, **sottostimando le tecniche** sofisticate **utilizzate dagli attaccanti** per ingannare le loro vittime.

Il corso si concentra sugli aspetti della **psicologia del rischio**, aiutando a **riconoscere i segnali** di potenziali minacce e **fornendo strategie pratiche** per evitare di cadere nelle trappole del phishing, sia nell'ambito personale che professionale.

Contenuti del corso

1. Psicologia del rischio: tener conto dei sospetti
2. La sottovalutazione del pericolo phishing
3. Come allenarci per riconoscere il pericolo
4. Test finale

DURATA CORSO
15m

Collana
CYBERSECURITY

Phishing, Vishing & Smishing

Le segnalazioni di **truffe online** e **attacchi informatici** sono in aumento, ma la maggior parte delle persone non le ascolta finché non è troppo tardi.

Quali passi si possono fare subito per evitare di diventare una vittima?

Una misura di sicurezza fondamentale è **proteggersi dal phishing**, e dalle sue varianti **vishing e smishing**, **quando** un utente **malintenzionato finge** di essere un contatto o un'organizzazione conosciuta **per ottenere l'accesso alle informazioni personali.**

Contenuti del corso

DURATA CORSO
15m