WIDEOFFICE
THE WORLD IS YOUR OFFICE

CORSO SCAW01
SECURITY AWARENESS – CONSAPEVOLEZZA DEL RISCHIO INFORMATICO

Ambito:	Durata:	Vendor:	Modalità:
Sicurezza	2 giorni	Interdisciplinare	Virtual classroom, one-to-one

PRESENTAZIONE

L'obiettivo del corso "*SCAW01 - Security awareness – Consapevolezza del rischio informatico*" è fornire una panoramica sugli attacchi informatici degli ultimi anni e di come vengono messi in atto, trasmettere i concetti base della sicurezza informatica, individuare i comportamenti rischiosi e spiegare come difendersi dalle principali minacce. Il corso è completamente in italiano.

Con suggerimenti puntuali e mirati, presi dall'esperienza quotidiana, verranno trattati non solo gli aspetti tecnici ma soprattutto quelli comportamentali da un punto di vista trasversale, creando consapevolezza e attenzione alle problematiche di security e di privacy.

DESTINATARI

È un corso ad ampio respiro, progettato per tutti gli utilizzatori di sistemi informatici che non si occupano direttamente e in maniera tecnica di sicurezza informatica all'interno delle aziende. Copre molti aspetti essenziali per garantire il contenimento del rischio ed è particolarmente indicato per chi ricopre ruoli di responsabilità e quotidianamente interagisce con risorse legate all'infrastruttura informatica.

MODALITÀ FORMATIVE

Questo corso viene offerto in tre modalità:

- In aula virtuale, live con istruttore da remoto;
- One-to-one come formazione individuale, live con istruttore da remoto;
- In aula con presenza dell'istruttore (ILT) – al momento non attivabile;

Il corso il relativo materiale sono in lingua italiana.

Il numero massimo di partecipanti ad un'edizione del corso è 20, il minimo per attivare il corso è 4. Non sono previsti laboratori, ma verranno esplorati diversi casi d'uso delle tecniche di protezione dei dati e delle identità.

Alla fine del corso è prevista una verifica di apprendimento attraverso un form online.

FINALITÀ DEL CORSO

Alla fine del corso i partecipanti saranno in grado di:

- Comprendere gli aspetti di base della sicurezza informatica
- Analizzare i rischi dell'utilizzo di un dispositivo connesso
- Difendersi dalle minacce cyber più frequenti
- Evitare i comportamenti a rischio
- Proteggersi da furti di identità e violazioni degli account

DURATA E PREZZI

- Durata: 2 giorni (16 ore)
- Quota di partecipazione in aula: € 390+IVA
- Sono disponibili sconti per partecipazioni in gruppo;
- Per un preventivo sulla formazione one-to-one e altre opzioni contattateci

NOTE

- Salvo diversamente concordato, l'orario di svolgimento è: 09-13 / 14-18
- Periodo: schedulazione mensile
- Il corso viene erogato esclusivamente con docenti dotati di esperienza su tematiche di sicurezza in grandi aziende.
- Non è presente un laboratorio ma verranno portati continuamente esempi reali presi dai principali casi d'uso.
- Il materiale didattico è realizzato da Wideoffice e viene fornito su supporto elettronico.

CERTIFICAZIONE

Il corso non prevede una certificazione ma verrà rilasciato un attestato di partecipazione.

PREPARAZIONE RACCOMANDATA

Si raccomanda a chi frequenta di avere una discreta conoscenza generale dei sistemi di posta elettronica, di Internet e delle procedure aziendali.

NOTE INTEGRATIVE

- Non è ammesso registrare le lezioni, né audio né audio/video

SEDI DEI CORSI

- Moncalieri (Torino) – via John Kennedy, 7 – 10024 – al momento non utilizzabile
- Torino – via Val della Torre, 3 – 10149 – al momento non utilizzabile

ARGOMENTI

GIORNO 1

Introduzione alla sicurezza informatica

- Che cos'è la sicurezza informatica
- Che cos'è un attacco informatico
- I nuovi profili degli attaccanti

Tipi di minacce informatiche

- Ransomware
- Attacchi Dos e DDos
- Furti di identità
- Trojan horse
- Le reti Peer-to-peer
- L'ingegneria sociale
- Glossario delle principali minacce su Internet

Casi famosi di compromissione

- Linkedin
- Solarwinds
- Regione Lazio
- SIAE
- Carbanak
- Ashley Madison

Tecniche di protezione dei dati

- La crittografia
- Sistemi di protezione aziendali (Firewall, Antivirus, Intrusion Detection System, Disaster Recovery)
- Verifiche di conformità (ISO/IEC 27001, Vulnerability Assessment)
- Attività di prevenzione

Le normative di legge

- Il Codice in materia di protezione dei dati personali (D. Lgs. 196/2003)
- I reati informatici (D. Lgs. 231/2001)
- Il GDPR (Regolamento UE 2016/679)
- La responsabilità del lavoratore

GIORNO 2

I rischi nelle comunicazioni via email

- Business Email Compromise (BEC)
- Come funziona la Posta Elettronica Certificata
- La crittografia dell'email: PGP (Pretty Good Privacy)

I rischi dei dispositivi connessi (IoT)

- Casi famosi e rischi dei dispositivi smart: Cayla
- I principali fattori di esposizione
- Sicurezza e compliance

Precauzioni da adottare per mitigare i rischi

- Come difendersi dai virus informatici
- Come difendersi dallo spam
- Come utilizzare in sicurezza i Social Network
- Come utilizzare la carta di credito su Internet in modo sicuro

Protezione dell'identità e degli account

- La gestione corretta delle password
- I password manager
- La violazione degli account
- Tracce della navigazione Internet

Il rischio maggiore: il Phishing

- Tipologie di phishing
- Come riconoscere le pagine ingannevoli
- Manipolazione dei link
- Il phishing bancario e finanziario
- Come difendersi dal phishing

WIDEOFFICE.IT - Via John F. Kennedy 7 - 10024 MONCALIERI (TO) - Tel. +39 011 627 28 28 - P.IVA IT09185850014 - education@wideoffice.it - www.wideoffice.it