SAA SCUOLA ASSICURATIVA ASSINFORM

Collana formativa online sul Cyber Risk

La collana e-learning di formazione continua ed operativa per gli intermediari di assicurazione

Nella Lettera al mercato del 29.12.2017 l'IVASS ritiene fondamentale l'accrescimento delle conoscenze informatiche degli intermediari, dei collaboratori e dipendenti.

"A tal fine l'istituto si attende che una quota del 20% del monte ore di formazione biennale obbligatoria per l'aggiornamento professionale, ex articolo 7 del Regolamento IVASS n. 6/2014, sia dedicata, a partire dal 2018, ai temi della sicurezza informatica."

Scuola Assicurativa Assinform ha progettato e realizzato una collana formativa e-learning da 20 ore complessive che illustrano in modo semplice ma esaustivo le principali tematiche del cyber risk, con numerosi casi pratici risolti.

- Analisi dei casi in base alla frequenza di rischio
  Il programma complessivo è strutturato per analizzare tutte le principali tematiche del cyber risk, dando priorità agli eventi che accadono con maggior frequenza.
- 18 moduli da un'ora ciascuno, a loro volta composti da 4 unità didattiche in cui vengono analizzati e approfonditi vari casi reali.
  A norma IVASS Reg. 40/2018.
- Coinvolgimento continuo
  L'approccio pratico consente al discente di riflettere sulle sue abitudini e grazie alle nuove tecniche di storytelling si sente costantemente coinvolto e stimolato a migliorarle.

24 moduli

26 ore complessive

4 unità didattiche

104 casi concreti

Percorso formativo personalizzabile selezionando solo i moduli d'interesse

Caratteristiche tecniche
Formato SCORM1.2/xAPI
HTML5

Maggiori informazioni e demo su
www.assinformsolutions.it/servizio/corso-cyber-risk/

I 18 moduli subito disponibili

1° modulo (1h 30')
- Il cybercrime
- Phishing
- La navigazione Web
- Uso di dispositivi Mobili
- Le connessioni Wi-Fi (reti pubbliche)

2° modulo (1h 30')
- Password
- La posta elettronica
- App Malevole e Permessi
- La Crittografia

3° modulo (1h 30')
- Sicurezza Wi-Fi
- I Cookie
- Ransomware
- Vettori di Attacco - Dispositivi USB

4° modulo (1h)
- Malware e Antivirus
- Allegati e Link Malevoli
- Backup e Ripristino
- Ingegneria Sociale

5° modulo (1h)
- La firma digitale
- Cosa sono i trojan
- Le connessioni VPN
- Cifratura nei dispositivi mobili

6° modulo (1h)
- Sicurezza bluetooth
- Cifratura della posta
- Attacchi reali
- Gestione dei dati sensibili

7° modulo (1h)
- Keylogger
- Dati online e privacy
- Smart card e sicurezza
- Smishing e vishing

8° modulo (1h)
- Sicurezza in viaggio
- Pharming
- Attacchi mirati
- Spyware worm e botnet

9° modulo (1h)
- IoT
- Cloud e sicurezza
- Data breach
- Come funziona un ransomware

10° modulo (1h)
- Trojan bancari
- Casi reali stuxnet
- Rischi dei social network
- Hacking Team

11° modulo (1h)
- Attacchi attraverso Shodan
- Sicurezza dei browser
- Casi reali - un attacco ransomware
- Casi reali - il mondo della cybersecurity

12° modulo (1h)
- APT e Hacking Governativo
- Casi reali - Crittovalute, TOR, Dark Web
- La riforma del copyright e il GDPR
- Il futuro e il presente dell'hacking / attacchi ai veicoli

13° modulo (1h)
- Aggiornamenti Windows perchè sono tanto importanti?
- La Supremazia Quantistica possibilità infinite, rischi concreti
- Deep Fake - sono pericolosi?
- L'attacco ForkBomb un caso di Denial of Service

14° modulo (1h)
- Internet Of Things - la 'S' sta per sicurezza
- Clearview - la fine della privacy per come la conosciamo
- L'Intelligenza Artificiale a servizio contro il phishing
- Il protocollo WPA3 - è davvero sicuro?

15° modulo (1h)
- La Rete 5G: novità e minacce
- Sito INPS al collasso: un caso concreto di DoS
- COVID-19 e cyber crime: alcune strategie di attacco
- Furto di Account: la tua vita in mano ad altri

16° modulo (1h)
- Malware sLoad: PEC sotto attacco
- Cyber Security e Polizia Postale
- Attacco NoiPA, il phishing che ruba le buste paga
- Furto di identità: le frodi creditizie

17° modulo (1h)
- SCA: quando la norma non è al passo con la tecnologia
- La BOTnet: i computer zombie
- Il Cyber Criminale: conosci il tuo nemico
- Attacco APT: il caso di Red Apollo

18° modulo (1h)
- Password più sicure: le nuove regole del NIST
- Mobile Forensics: lo scontro Apple-FBI
- L'attacco Pharming: attenzione ai siti-trappola
- Cyber Security: le sfide del 2020

Nuova collana formativa 2021

Modulo 1: Smart working e didattica a distanza

Target: impiegati, dirigenti, consulenti, insegnanti di ogni ordine e grado, famiglie con figli in età scolastica

1.1: La panoramica d'insieme
1.2: I rischi dello smart working
1.3: Videoconferenze e didattica a distanza
1.4: Il futuro dello smart working

Modulo 2: Cyber risk in ufficio e nelle amministrazioni

Target: Pubblica Amministrazione, banche, imprese private etc

2.1: Struttura della rete aziendale
2.2: Hardware e software
2.3: Gli anelli deboli
2.4: Buone norme

Modulo 3: Cyber risk nei reparti produttivi

Target: PMI e industrie

3.1: La panoramica d'insieme
3.2: Tipologie di attacco
3.3: Firmware, software e sensori
3.4: Gli infiltration test

Modulo 4: Cyber risk in mobilità - agenti e rappresentanti

Target: consulenti, agenti, rappresentanti

4.1: La panoramica d'insieme
4.2: Smartphone e tablet
4.3: wi-fi pubbliche
4.4: Roaming dati e rete 5G

Modulo 5: e-commerce e transizioni online

Target: commercianti di beni e servizi venduti tramite e-commerce, famiglia, persone fisiche

5.1: Le transizioni online
5.2: Truffe e frodi
5.3: e-commerce infetti
5.4: Il futuro dell'ecommerce

Modulo 6: Cyber risk nel tempo libero

Target: Famiglia, persone fisiche

6.1: La disinformazione, il fenomeno delle fake news
6.2: Siti pirata e streaming video
6.3: Smart home e domotica
6.4: Le truffe telefoniche

Approccio didattico

La **nuova collana formativa 2021** è focalizzata sugli **aspetti pratici** di come, nelle varie **realtà professionali e private,** tali minacce possano compromettere la sicurezza delle persone e comportare danni economici.

Ogni modulo si focalizza su una realtà specifica su cui poter fare focus sui rischi e avere a disposizione leve commerciali a cui poter agganciare una risposta assicurativa.

Le pillole del nuovo ciclo Cyber Risk sono infatti progettate sui diversi:

- **Settori merceologici**
- **Ambiti di vita privata**
- **Modalità di utilizzo delle tecnologie per i diversi ruoli / abitudini professionali,** delineandone:
  - i **rischi**
  - i **casi di cronaca**
  - le **soluzioni tecniche** da adottare

Obiettivi formativi

- **conoscere i rischi trasversali e specifici** dei diversi target / ambiti di utilizzo delle tecnologie
- saper **approcciare il cliente (imprenditore, famiglia, persona fisica) con motivazioni di vendita che si basano su esempi concreti** relativi alle diverse minacce cyber

I moduli sono personalizzabili con le coperture assicurative di riferimento della Compagnia.

- **6 moduli da 1 ora l'uno**
- **A rilascio mensile da Aprile a ottobre 2021**

Per informazioni tel: 0434 26136
Mauro Venier - venier@assinews.it
Chiara Vialmin - vialmin@assinews.it

ASSINFORM
Società certificata UNI EN ISO 9001:2015
Settori EA 37 - EA 08 - EA 35