ASSINEWS

SAA SCUOLA ASSICURATIVA ASSINFORM

Corso online sul Cyber Risk

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

18 moduli

20 ore complessive

4 unità didattiche per modulo

72 casi concreti

ASSINFORM

Società certificata UNI EN ISO 9001:2015 -
settori Formazione EA 37 - Editoria EA 08 - Consulenza EA 35

La Collana e-learning sul Cyber Risk

18 CORSI DA UN'ORA CIASCUNO CIRCA
4 UNITÀ DIDATTICHE PER ORA
72 CASI CONCRETI

Non più formazione una tantum...

...ma corsi 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.

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.

Il metodo didattico Assinform

- partecipazione attiva ed esperienziale
- studio a partire da casi concreti

Attestazione crediti IVASS

Al termine di ogni corso sarà somministrato il test finale che darà diritto al credito IVASS.

Caratteristiche tecniche

Formato SCORM 1.2 / xAPI - HTML5

ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI
IVASS

La lettera al mercato IVASS del 29 dicembre 2017 per gli intermediari assicurativi

Estratto dalla lettera dell'IVASS

"Esiti dell'indagine conoscitiva sui presidi degli intermediari tradizionali per la gestione delle informazioni e la prevenzione dei rischi informatici. Indicazioni per gli intermediari".
"Fondamentale, sempre sul piano della prevenzione, sarà l'accrescimento delle conoscenze informatiche degli intermediari stessi e 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."

I moduli e le tematiche

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

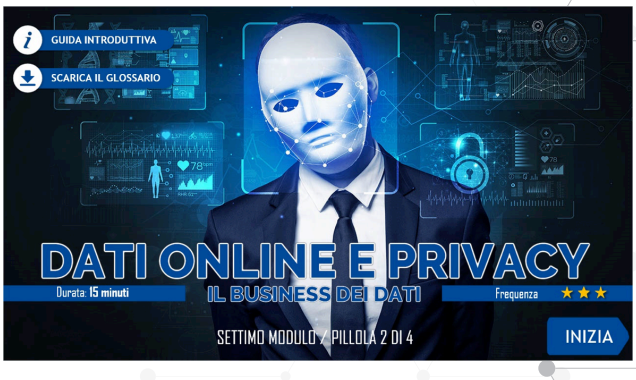
8° modulo (1h)
- Sicurezza in viaggio
- Pharming
- Attacchi mirati
- Spyware worm e botnet

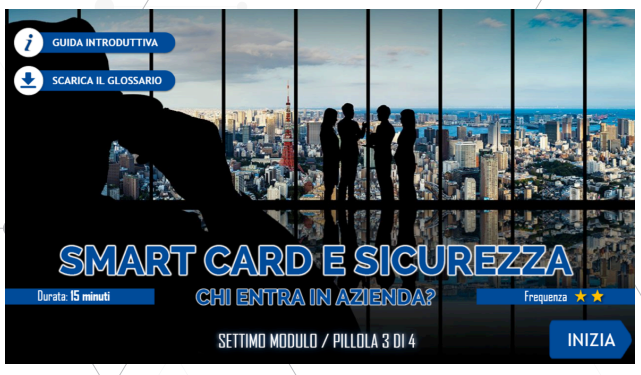
9° modulo (1h)
- IoT
- Cloud e sicurezza
- Data breach
- Come funziona un ransomware

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)

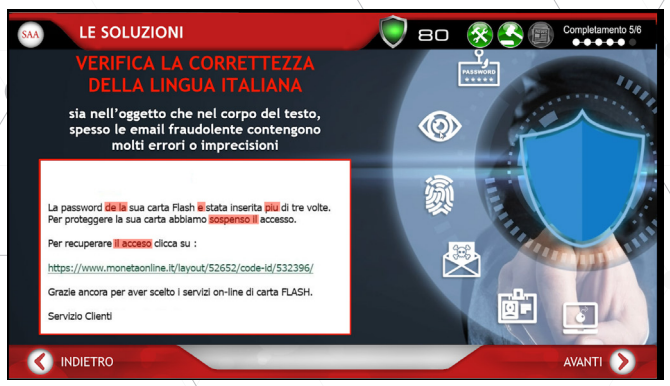
- Malware sLoad: PEC sotto attacco
- Cyber Security e Polizia Postale
- Attacco NoiPA, il phishing che ruba le buste paga
- Furto di identità: le frodi creditizie

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



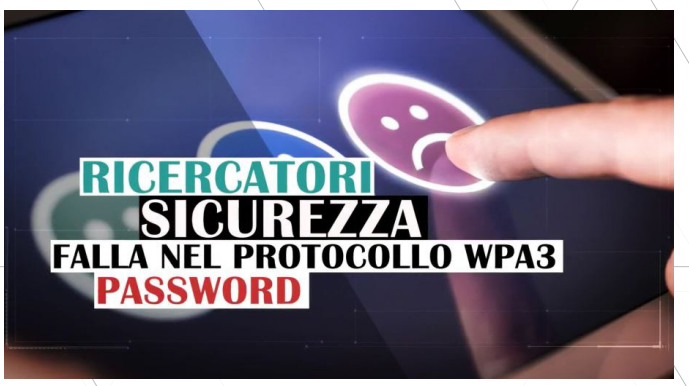
Sapresti rispondere a...

Perchè sono tanto importanti gli Aggiornamenti Windows?

A gennaio 2020 Microsoft ha dismesso il supporto tecnico per Windows7.
Analizzando un caso concreto si scoprirà perchè è tanto importante mantenere un qualsiasi sistema operativo aggiornato, e quali sono i rischi in caso di attacchi a sistemi non aggiornati. Durante l'unità didattica verranno trattati i temi della crittografia dei dati e alcune tipologie di attacco informatico come l'exploit e l'attacco man in the middle.

I Deep Fake sono pericolosi?

Una nuova tecnologia basata sul machine learning permette a chiunque di poter sostituire i volti delle persone nei filmati con quelli di attori e politici.
Quali sono i possibili impieghi di questa tecnologia e perchè è bene essere preparati a riconoscere i video falsificati da quelli autentici?
Introducendo la tematica del machine learning si esploreranno le implicazioni sociali dell'impiego su vasta scala di questa tipologia di contenuti.



Per informazioni
mail: vialmin@assinews.it
tel: 043426136