SAA SCUOLA ASSICURATIVA
ASSINFORM

# CYBER RISK

## LA COLLANA E-LEARNING DI FORMAZIONE CONTINUA ED OPERATIVA

**24 MODULI**

**25 ORE COMPLESSIVE**

**4 UNITÀ DIDATTICHE PER MODULO**

**104 CASI CONCRETI**

### NON PIÙ FORMAZIONE UNA TANTUM...

Moduli da un'ora ciascuno, a loro volta composti da 4 unità didattiche in cui vengono analizzati e approfonditi casi reali.

### 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.

### CASI PRATICI ORGANIZZATI PER TARGET E FREQUENZA DI RISCHIO

I **nuovi moduli 2021** sono organizzati in base al target (famiglia, PMI, scuola, ..) e ai contesti di utilizzo dei dispositivi (a casa, in mobilità)

## OBIETTIVI

**La fruizione di corsi inerenti la sicurezza informativa è esplicitamente richiesta dall'IVASS** nella Lettera al mercato del 29.12.2017, da parte degli intermediari assicurativi.

## DESTINATARI

- **Intermediari (sez. A, B, E)**
- **Impiegati**

**La lettera al mercato IVASS del 29 dicembre 2017 - Estratto**

**"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 didattici

**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)
- Attaccchi 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

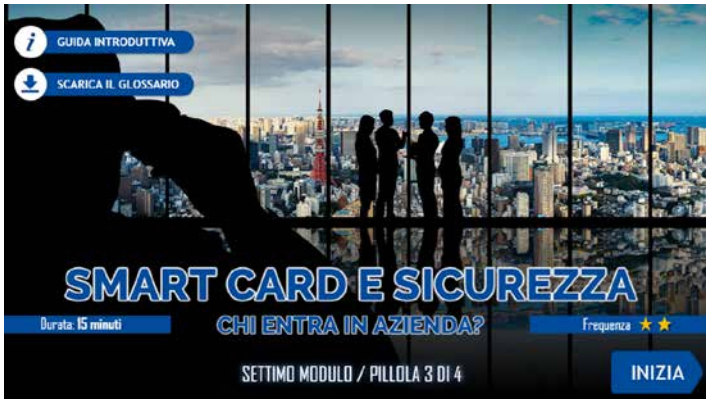
### 14° modulo (1h)
- Internet Of Things - la 'S' sta per sicurezza
- Clearview - la fine della privacy per come la conosciamo
- L'Intelligenza Artificiale a servizio contro il phishing
- Il protocollo WPA3 - è davvero sicuro?

### 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




## L'importanza di un corso sui rischi informatici

Chi fruisce del web è al contempo un professionista che ne utilizza le potenzialità per gestire, comunicare e cercare i propri clienti, e un privato che naviga liberamente, si informa, si iscrive a portali, acquista servizi e prodotti.

Uno strumento che contiene rischi: le informazioni, siano essi personali o dei propri clienti, vengono immesse nella rete ed **è proprio il nostro comportamento o la scarsa conoscenza della grammatica del web a metterne a repentaglio la sicurezza.**

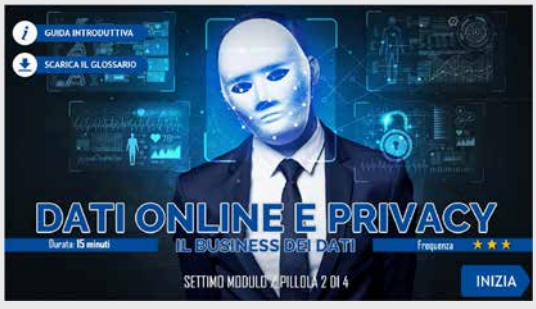
## Cosa si impara?

**Gli obiettivi degli hacker**
*Cosa li spinge a cercare di rubare documenti, informazioni o credenziali d'accesso?*

**E-mail, smartphone, gestionali, portali web, e-commerce, domotica**
*Quali sono le modalità d'attacco degli hacker e cosa stiamo rischiando?*

**Suggerimenti e best-practices**
*Come evitare brutte sorprese, costi inaspettati o insostenibili, perdita di dati.*

**La gestione dei profili personali online**
*L'importanza di gestire con consapevolezza la propria presenza sul web in quanto professionista.*



# Il Cyber Risk nei contesti di utilizzo

### 19° modulo: Smart working e didattica a distanza (1h)

*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

### 20° modulo: Cyber risk in ufficio e nelle amministrazioni (1h)

*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

### 21° modulo: Cyber risk nei reparti produttivi (1h)

*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

### 22° modulo: Cyber risk in mobilità - agenti e rappresentanti (1h)

*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

### 23° modulo: e-commerce e transizioni online (1h)

*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

### 24° modulo: Cyber risk nel tempo libero (1h)

*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 **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.**

**Per informazioni** tel: 0434 26136
Federico Manassero - manassero@assinews.it

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