KPMG Digital Learning Cybersecurity

Perché la formazione sulla cyber security?

Gli attacchi cyber rappresentano una delle sfide più complesse con cui le organizzazioni si stanno attualmente confrontando. Per questo, le iniziative di **cybersecurity** sono diventate una **priorità** che non può essere trascurata da nessuna azienda.

Per prevenire i **cyber attacchi**, le organizzazioni sono chiamate a **definire e implementare strategie** che coniughino il **potenziamento dei sistemi informatici** con la **promozione di comportamenti**, in linea con le **policy aziendali di sicurezza informatica**.

A tal fine, le aziende non possono prescindere dal **sensibilizzare** tutti i dipendenti sull'**importanza della sicurezza informatica**, anche attraverso **iniziative formative** dedicate.

La proposta KPMG

Il team Digital Learning KPMG propone un'**offerta formativa sulla Cyber Security** che mira a:

— Rafforzare le skill e le **conoscenza in materia di IT Security**

— **Sensibilizzare** tutti i dipendenti sui potenziali fattori di rischio, che potrebbero generare un cyber attacco

— Supportare **l'evoluzione del singolo individuo** da potenziale fattore di rischio ad attore protagonista per la difesa di asset e informazioni aziendali

Per rispondere adeguatamente alle esigenze delle organizzazioni che intendono approcciare questo tema con efficacia e logiche strutturate, il team Digital Learning KPMG, in collaborazione con i professionisti dell'Information Risk Management, ha sviluppato due diverse soluzioni.

Pillole formative

Dieci pillole formative della durata massima di **5 minuti** ciascuna

Moduli **auto-consistenti**, ispirati alla logica del **microlearning**, che favoriscono una fruizione allineata all'esigenze dell'utente

Un **piano editoriale personalizzabile** sula base delle esigenze specifiche

Un percorso formativo **articolato nel tempo** che consente di mantenere alta l'attenzione

Corso e-Learning

Un corso completo per affrontare tutti i rischi connessi alla cybersecurity della durata di **1,5 ore**

Approfondimento dei contenuti supportato da un **framework narrativo** di riferimento grazie alle tecniche dello **storytelling**

Utilizzo di logiche di **gamification** per ingaggiare gli utenti e assicurare coinvolgimento ed apprendimento attivo

Un **approccio pragmatico** per favorire l'adozione di nuovi comportamenti, personalizzabile in base ai rischi del settore

Entrambe le soluzioni sono fruibili in logica multi-device (PC, tablet e smatphone) e sono accessibili anytime e anywhere

LMS

Piattaforma personalizzata con logiche innovative di comunicazione, interazione e ingaggio

È possibile integrare servizi aggiuntivi

Penetration Test

Verifica delle conoscenze apprese attraverso simulazioni di attacchi informatici

Contenuti

Pillole formative

1. Launch: *we've been hacked!)*
2. Credenziali di autenticazione
3. Disciplina della protezione dei dati nell'era del GDPR
4. Phishing
5. Social Network
6. Social Engineering
7. Utilizzo corretto dei device aziendali
8. Phisical Security
9. File sharing
10. Impatto di un Cyberg incidente

Inquadra il QR Code per una breve demo oppure clicca qui

Corso trasversale

Un *escape room* in cui l'utente si confronta con una successione di prove che consentono di consolidare le competenze per difendersi di rischi connessi a:

- Social Network
- Reti Wi-Fi
- Internet of Things (IOT)
- Dispositivi usb
- Archiviazione cloud
- Stampanti e documentazione cartacea
- Dispositivi aziendali

Inquadra il QR Code per una breve demo oppure clicca qui

Percorsi formativi blended

In linea con **approcci didattici 70/20/10**, i nostri professionisti possono supportare anche lo sviluppo di percorsi blended articolati in sessioni formative **in aula**, con **webinar, workshop** ed esperienze strutturate di **training on the job,** progettate con i nostri esperti di Cyber Security.

- **CONTENUTI CUSTOM**, progettati sulle specifiche esigenze dell'organizzazione e dei discenti
- Utilizzo di tecniche innovative di **SIMULAZIONE** in una prospettiva metodologica **LEARNING BY DOING**
- **Impiego SERIOUS GAMES** per un ingaggio costante e coinvolgente della popolazione target

KPMG Advisory

Expertise di settore

Rete di professionisti con competenze multidisciplinari e un consistente portafoglio di esperienze nell'ambito della cyber security

Customer satisfaction

Percorsi formativi personalizzati rispetto alle esigenze del cliente e al target, al fine di assicurare un contenuto formativo digitale stimolante e soluzioni d'apprendimento efficace

Our people

Non solo competenze tecniche, ma anche predisposizione a lavorare con una logica collaborativa con il cliente instaurando un rapporto di fiducia fra le persone

Contatti

Andrea Tabladini
Partner
KPMG Advisory S.p.A.
People & Change
Via Vittor Pisani 27 – 20124 Milano
T: +39 348 2708853
E: atabladini@kpmg.it

Luca Boselli
Partner
KPMG Advisory S.p.A.
Information Risk Management
Via Vittor Pisani 31 – 20124 Milano
T: +39 348 3056864
E: mboselli@kpmg.it

Marta Lodigiani
Manager
KPMG Advisory S.p.A.
People & Change
Via Vittor Pisani 31 – 20124 Milano
T: +39 348 3080747
E: mlodigiani@kpmg.it