Cybertraining: il modulo“Awareness” nel dettaglio

Il programma formativo *Cybertraining* si basa sulla piattaforma tecnologica Cyber Guru, azienda italiana leader di mercato accreditata da ACN e inserita nel Catalogo delle Infrastrutture Digitali e dei Servizi Cloud, che garantisce alla PA la conformità dei servizi offerti da operatori privati.

La piattaforma prevede 3 moduli, integrati ma allo stesso tempo indipendenti.

CG Awareness (Conoscenza)

È il modulo didattico di base. Promuove la conoscenza attraverso un processo di formazione che fa da guida al comportamento. Il piano viene erogato in modalità e-learning ed è composto nel suo complesso di 3 cicli annuali.

CG Channel (Percezione del pericolo)

Episodi narrativi a tema cyber in stile serie TV, che tendono ad agire sulla componente più emotiva del cervello stimolando la percezione del pericolo.

CG Phishing (Prontezza di reazione)

Allenare la prontezza è fondamentale per agire velocemente adottando il giusto comportamento di fronte al manifestarsi di un pericolo. È il modulo di training esperienziale anti-phishing

Di seguito il modulo Cyber Guru Awareness (CGA) nel dettaglio.

Caratteristiche generali

Cyber Guru Awareness è il modulo didattico di base, un innovativo sistema di e-learning pensato specificamente per il personale non specialistico di strutture pubbliche e private. Progettato interamente in Italia, si fonda su metodologie formative in linea con le modalità di apprendimento digitale maggiormente efficaci nel nostro Paese.

CGA è stato disegnato per coinvolgere tutta l’organizzazione in uno stimolante percorso educativo, che si caratterizza per un approccio **a rilascio costante e graduale**:

- l’attività di formazione impegna l’allievo per pochi minuti a settimana, con un percorso, ripartito su annualità, che mantiene elevata l’attenzione ogni qualvolta si interagisce con le tecnologie digitali;
- tutte le lezioni sono disponibili in formato multimediale, con la possibilità di fruire dei contenuti sia in video che in modo testo;
- il linguaggio utilizzato risponde a un criterio divulgativo focalizzato su personale non specializzato in cyber security;
- ogni lezione è corredata di test che valutano il livello di apprendimento;

- il corso usa una metodologia di *gamification*, con riconoscimenti atti a stimolare l'apprendimento e premiare l'eccellenza;
- è supportata la formazione di squadre in competizione tra loro;
- ogni modulo formativo è autonomo, nel senso che affronta compiutamente uno specifico argomento e ha valore intrinseco senza dipendere da altri moduli;
- i moduli formativi della prima annualità sono in totale 12, erogati con frequenza concordabile (in genere mensile) e sinteticamente descritti di seguito.

12 moduli formativi

Benché ogni modulo della prima annualità sia autoconsistente, la sequenza con cui sono stati organizzati è studiata per generare richiami "naturali" ad argomentazioni già affrontate in precedenza, rafforzando in questo modo il livello di apprendimento e memorizzazione dei contenuti.

PHISHING. Il phishing è la più comune tecnica di attacco utilizzata dai criminali informatici e sfrutta l'email come principale veicolo di diffusione, anche se si va estendendo velocemente ad altri canali, come le più popolari piattaforme di messaggistica e i social media.

È particolarmente subdola perché basata su un inganno, con cui si cerca di indurre la potenziale vittima a compiere un'azione che consente al criminale di sferrare il suo attacco.

Questo modulo formativo fornisce gli elementi cognitivi per riconoscere un attacco phishing e adottare le necessarie contromisure.

PASSWORD. Uno dei pilastri su cui poggia la cyber security è la password, la chiave personale di accesso a tutte le risorse informatiche che si vogliono mantenere sicure e riservate. La corretta gestione delle proprie password diventa quindi elemento basilare nelle strategie difensive sia della persona che dell'organizzazione.

Questo modulo formativo fornisce gli elementi cognitivi necessari a una gestione sicura delle password, che le pone al riparo da tentativi di violazione con conseguenze potenzialmente disastrose.

SOCIAL MEDIA. I social media rappresentano la nuova modalità di socializzazione basata sulle ampie possibilità che la tecnologia digitale mette oggi a disposizione. Ma allo stesso tempo sono anche fattori di rischio, dove si può arrivare a compromettere sia la privacy delle persone sia la sicurezza dei sistemi delle organizzazioni.

Questo modulo fornisce gli elementi cognitivi per utilizzare in modo consapevole i social, proteggendo la persona e l'organizzazione dai rischi che la condivisione in rete di contenuti individuali e professionali può comportare.

PRIVACY & DATI PERSONALI. L'introduzione del nuovo regolamento europeo sulla protezione dei dati aumenta la responsabilità delle organizzazioni rispetto alla privacy e alla protezione dei dati sensibili.

Al di là dei ruoli specifici, è importante che tutti i membri dell'organizzazione acquisiscano una maggiore sensibilità verso la protezione dei dati.

Questo modulo fornisce gli elementi cognitivi per assumere un atteggiamento proattivo riguardo alla protezione dei dati e per contribuire alla conformità dell'organizzazione alle nuove norme europee.

DISPOSITIVI MOBILI. I dispositivi mobili, soprattutto smartphone e tablet, sono strumenti che diventano ogni giorno più indispensabili e che rappresentano la massima espressione della rischiosa sovrapposizione delle dimensioni personale e professionale.

Questo modulo fornisce gli elementi cognitivi per utilizzare i dispositivi mobili, siano essi personali o professionali, in modo consapevole, abilitando buone pratiche in grado di aumentare il livello di sicurezza e di protezione dei dati.

FAKE NEWS. Le fake news sono "bufale" inventate o notizie semplicemente distorte, che hanno lo scopo di manipolare l'informazione. Una piaga pericolosa, che può avere ripercussioni negative sia per l'individuo sia per le organizzazioni. Le fake news hanno spesso come riferimento gli ambiti sociale e politico, ma non mancano le relazioni dirette con la cyber security.

Questo modulo formativo fornisce gli elementi cognitivi necessari a riconoscere una fake news, attivando alcuni processi di indagine che aiutano a sviluppare un atteggiamento corretto verso qualsiasi informazione acquisita in rete.

MEMORIE USB. Le chiavette USB, come tutte le memorie esterne, possono diventare un elemento critico rispetto alla necessità di proteggere le informazioni riservate, ed è per questa ragione che sono spesso oggetto di specifiche policy.

Questo modulo formativo fornisce gli elementi cognitivi per riconoscere tutti i rischi associati alle memorie esterne, abilitando buone pratiche per evitare di incorrere in fenomeni di furto di dati.

MALWARE & RANSOMWARE. I software malevoli in generale e il ransomware in particolare hanno conquistato velocemente gli onori della cronaca, mettendo in evidenza tutta la loro pericolosità. È bene comprendere e accettare che gli antivirus non garantiscono la protezione totale da questi software.

Questo modulo formativo fornisce gli elementi cognitivi per ridurre il rischio di cadere vittime di questa particolare tipologia di software e per limitare le conseguenze negative in caso di violazioni.

EMAIL SECURITY. L'email è uno strumento di cui nessuno oggi può fare a meno nella vita professionale. Il suo ruolo è centrale e particolarmente critico. Attraverso l'email vengono scambiate molto spesso informazioni sensibili e quindi l'aspetto della sicurezza non può essere sottovalutato.

Questo modulo formativo fornisce gli elementi cognitivi per una corretta gestione dell'email e delle informazioni scambiate.

BROWSING. La navigazione nel web presenta molti rischi e quella che è ormai un'attività di routine nasconde parecchi aspetti critici. Una buona conoscenza di alcune caratteristiche peculiari dei siti web e dei browser può aiutare a ridurre notevolmente il livello di rischio.

Questo modulo formativo fornisce gli elementi cognitivi su come navigare nel web in sicurezza.

SCENARI CRITICI. L'interazione con il cyber spazio prevede alcuni scenari critici come per esempio l'uso delle infrastrutture cloud o delle piattaforme di e-commerce, sia in ambito B2B che B2C.

Sono scenari che risultano particolarmente esposti alla possibilità di subire attacchi da parte dei cyber criminali, con rischi sia sul piano individuale sia sul piano professionale.

Questo modulo vuole fornire elementi essenziali di consapevolezza che aiutano a comprendere le minacce, spesso sottovalutate, collegate a questi particolari scenari di utilizzo delle tecnologie digitali.

SOCIAL ENGINEERING. La cosiddetta ingegneria sociale è la madre di tutte le strategie di attacco cyber. È una strategia che punta sull'inganno e sulla manipolazione psicologica per perseguire finalità truffaldine, di norma basate sull'acquisizione di informazioni riguardanti la vittima designata.

Questo modulo fornisce elementi di consapevolezza in merito alle tecniche utilizzate dai cyber criminali, diventando di fatto la sintesi ideale di elementi già trattati nei moduli precedenti.

Contatto: Marcello Fontana
commerciale@gotech.it
+39 351 4272010