Cyber Guru Training

Piano di Comunicazione
Cyber Guru

Sommario

1. Premessa

Il presente documento contiene le indicazioni generali per implementare l'intero piano di comunicazione per il lancio del programma di Cyber Security Awareness con i due programmi formativi Cyber Guru Awareness e Cyber Guru Channel.

La piattaforma Cyber Guru invierà comunicazioni a tutti i partecipanti censiti in piattaforma tramite un **sistema automatizzato di Student Caring**. La **prima comunicazione** avverrà nella data stabilità del **lancio del programma** e conterrà le credenziali di accesso alla piattaforma.

Nei mesi successivi al lancio, i partecipanti riceveranno sempre il medesimo sistema automatico di Student Caring che li avviserà del **nuovo modulo disponibile** (uno al mese) in piattaforma.

Si consiglia, inoltre, di progettare e associare, a questo sistema automatico di Student Caring caratterizzante della piattaforma, un **piano di comunicazioni interna alla Company** che anticipi e sponsorizzi alle figure apicali e a tutti i dipendenti il lancio del programma di Cyber Security Awareness di Cyber Guru.

È importante infine attivare canali di comunicazione interni alla Company come Intranet (con una pagina dedicata al lancio del programma di Cyber Security Awareness) o News.

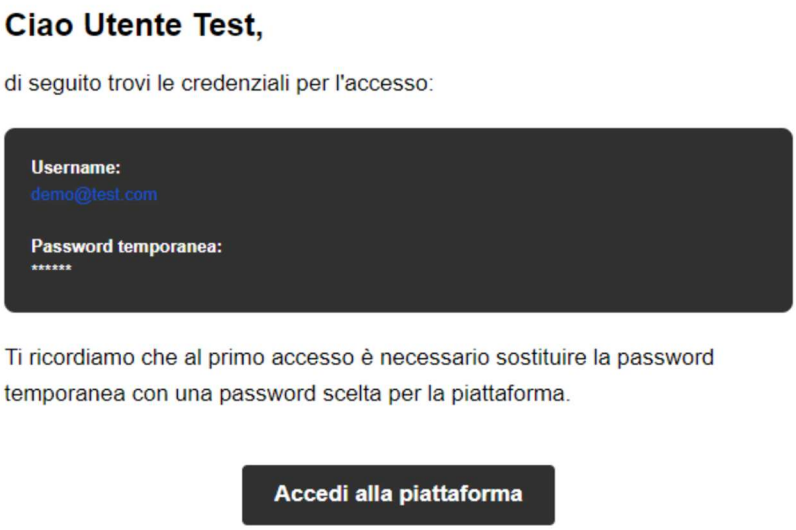
2. Comunicazioni automatiche Cyber Guru School

All'interno della piattaforma Cyber Guru è presente un sistema di Student Caring automatico che consiste nell'invio di:

- **una prima mail di lancio**, ad avvio del programma nella data di GO LIVE concordata tra le parti;
- una mail di Student Caring **nei mesi successivi al lancio**, per informare l'utente del nuovo modulo disponibile in piattaforma.

2.1 Comunicazioni Cyber Guru testo lancio del programma Cyber Security Awareness

Di seguito è indicato il testo della mail che sarà inviato a tutti gli utenti censiti in piattaforma nella data stabilità del go live del programma di Cyber Security Awareness.



2.2 Comunicazioni Cyber Guru Student Caring

Le comunicazioni di Student Caring saranno inviate nei **mesi successivi** al lancio ad attivazione di ogni nuovo modulo.

3. Suggerimenti piano di Comunicazione Interna

Di seguito sarà possibile leggere **alcuni suggerimenti** per la gestione del **piano di comunicazione interna** che consigliamo **preceda il lancio delle comunicazioni automatiche inviate** dalla piattaforma Cyber Guru.

Sono presenti due esempi di tipologie di comunicazioni verso:

- figure apicali;

- tutti i dipendenti.

3.1 Comunicazioni Example verso Figure Apicali

Gentilissime [Direttrici] e Gentilissimi [Direttori],

in collaborazione con la **Direzione/Area/Dipartimento** [indicare Direzione/Area/Dipartimento promotrice dell'iniziativa] è stato organizzato un [**programma formativo**] [percorso formativo] [percorso di addestramento] [un percorso coinvolgente], attraverso la **piattaforma di e-learning Cyber Guru**, dedicato al tema della [**Cyber Security Awareness**] [consapevolezza nell'ambito della Cyber Security] che con un impegno di pochi minuti al mese consentirà a ciascun [utente, collega] di essere custode dei dati che vengono trattati ogni giorno e, quindi, di proteggere se stessi e l'organizzazione dai possibili attacchi informatici.

Il programma formativo prende avvio [**nel mese di…]** oppure [data di inizio], avrà la durata di [12/24/36 mesi[1]] e comprende [12/24/36] moduli formativi e [12/24/36] episodi, ciascuno dei quali è dedicato ad uno specifico argomento.

I **contenuti formativi** vengono abilitati con la frequenza di uno al mese e il metodo di fruizione è rigidamente sequenziale. È quindi necessario completare la fruizione di un contenuto, prima di passare al successivo.

Ogni modulo relativo alla componente formazione è formato da **3 brevi lezioni**, ognuna delle quali è costituita da un contenuto video di circa 15 minuti e, come alternativa, da un documento che riproduce gli stessi contenuti del video in un formato testo.

Le **3 lezioni** all'interno di un modulo sono organizzate secondo il seguente schema:

- La prima lezione è quella della conoscenza di base; favorisce una presa di conoscenza dell'argomento, fornendo gli elementi cognitivi che consentono la comprensione del rischio;
- La seconda lezione è quella dell'approfondimento; consente di stimolare la "prontezza", creando le condizioni per riconoscere le minacce anche quando queste si presentano in forma insolita e sofisticata;
- La terza lezione è quella delle best practice; consente di acquisire "buone pratiche" di comportamento, stimolando la "reattività", e quindi la capacità di agire in modo consapevole.

Per passare da una lezione all'altra è necessario superare un test di apprendimento, costituito da 4 domande a risposta multipla. La lezione è considerata superata quando si risponde correttamente ad almeno 3

domande su 4.

Ogni episodio relativo alla componente di formazione induttiva è costituito da un contenuto video di circa 5 minuti incentrati sulle principali minacce cyber.

[1] 12 moduli prima annualità, 24 moduli seconda annualità, 36 moduli terza annualità

[Opzionale] Al fine di sostenere il coinvolgimento dei partecipanti, il percorso formativo prevede una **metodologia cosiddetta "gamification",** assimilabile in termini di attribuzione di punteggio ad un campionato virtuale, tale per cui Il percorso formativo permette di valorizzare una **classifica individuale**, che serve a gratificare la persona nel suo percorso e, contestualmente, a **valorizzare la classifica per team,** ossia per Direzione di appartenenza dei singoli partecipanti.

[Opzionale] Tutte le statistiche vengono fornite nel **pieno rispetto della Privacy e della tutela dei dati personali**. Ogni partecipante può vedere solo i propri indicatori, rapportati al team di appartenenza - Direzione di appartenenza - e la valorizzazione della classifica per team.

[Opzionale] Il percorso formativo è [obbligatorio] [facoltativo].

[Entro la settimana corrente] [Entro la prossima settimana], con successiva mail a cura [*del mittente no-reply@cyberguru.eu*] [*della piattaforma di e-learning Cyber Guru Awareness*] **saranno trasmesse a ciascun partecipante credenziali di accesso**.

È garantito **un servizio di supporto con casella di posta dedicata [support@cyberguru.eu].**

[Opzionale] Sarà possibile consultare maggiori informazioni all'interno della pagina Intranet dedicata [indicare link consultabile di riferimento].

Certi della collaborazione, restiamo a disposizione per ogni ulteriore necessità di approfondimento. Cordiali saluti,

Team HR - Team Comunicazione

3.2 Comunicazioni Example verso l'intera popolazione aziendale

Gentilissime e Gentilissimi,

in collaborazione con la **Direzione/Area/Dipartimento** [indicare Direzione/Area/Dipartimento promotrice dell'iniziativa] è stato organizzato un [**programma formativo**] [percorso formativo] [percorso di addestramento] [un percorso coinvolgente], attraverso la **piattaforma di e-learning Cyber Guru**, dedicato al tema della [**Cyber Security Awareness**] [consapevolezza nell'ambito della Cyber Security] che con un impegno di pochi minuti al mese consentirà a ciascun di noi di essere custode dei dati che vengono trattati ogni giorno e, quindi, di proteggere se stessi e l'organizzazione dai possibili attacchi informatici.

Il percorso formativo prende avvio [nel mese di…] oppure [data di inizio], **ha la durata di [12/24/36 mesi], comprende [12/24/36] moduli formativi [e 12/24/36 episodi]** ognuno dei quali è dedicato ad uno specifico argomento.

I contenuti formativi vengono abilitati con la frequenza [**mensile**] e il metodo di fruizione è rigidamente sequenziale. È quindi necessario completare la fruizione di un contenuto, prima di passare al successivo.

Ogni modulo è formato da 3 brevi lezioni, ognuna delle quali è costituita da un contenuto video di circa 5 minuti e, come alternativa, da un documento che riproduce gli stessi contenuti del video in un formato testo. La componente induttiva è invece composta da un breve video di circa 5 minuti ciascuno sempre su tematiche legate alla Cyber Security.

Al fine di rendere il percorso formativo più motivante, la piattaforma e-learning prevede l'attribuzione di punteggi per ciascuna risposta esatta fornita al termine dei moduli formativi, **in questo modo si partecipa ad un campionato virtuale** che consente di accumulare i punti acquisiti, all'interno del team di riferimento, rappresentato dalla Direzione di appartenenza.

[Tutte le statistiche vengono fornite nel **pieno rispetto della Privacy e della tutela dei dati personali**. Ogni partecipante può vedere solo i propri indicatori, rapportati al team di appartenenza e **tutti i dati sono anonimi**.]

Il percorso formativo è [obbligatorio] [facoltativo].

Entro la settimana corrente, con successiva mail a cura [del mittente no-reply@cyberguru.eu] [della piattaforma di e-learning Cyber Guru Awareness] **saranno trasmesse a ciascun partecipante le credenziali di accesso**.

Sarà possibile consultare maggiori informazioni all'interno della pagina Intranet dedicata [indicare link consultabile di riferimento].

Fiduciosi della collaborazione, i migliori saluti

Team HR – Team Comunicazione

3.3 Attivazione canali interni alla Company come Intranet e News

È consigliata **l'attivazione di più canali interni** alla Company al fine accrescere la partecipazione ed il coinvolgimento attivo di tutti i dipendenti, favorendo la buona riuscita del programma.

Laddove sia possibile, si può progettare la creazione di una pagina Intranet dedicata al tema dove animare e sponsorizzare anche le dinamiche di gamification incluse nella piattaforma.

3.4 Comunicazioni Post GO LIVE

Può verificarsi che dopo la partenza dei programmi formativi di Cyber Guru qualche utente possa rimanere indietro con il percorso di formazione e sia necessario programmare delle comunicazioni mirate ad hoc [da parte di figure apicale, es. CEO]. Di seguito vi proponiamo un esempio di comunicazione da poter usare in questi specifici casi:

Gentilissimi Colleghi,

Gli attacchi informatici stanno diventando sempre più raffinati e pericolosi. Le tecniche utilizzante dai criminali cyber mettono a rischio non solo la sicurezza della nostra organizzazione ma anche la vostra

sicurezza personale.. Per questo motivo, abbiamo deciso di svolgere all'interno di **[nome company]** il programma di Cyber Security Awareness che con un impegno di pochi minuti al mese ti consentirà di acquisire il giusto grado di consapevolezza nella Cyber Security, proteggendo noi stessi e la nostra organizzazione da possibili attacchi informatici.

Nell'ambito di tale programma stiamo tuttavia riscontrando un livello di partecipazione [basso, molto basso, non completamente soddisfacente]. Allo stato attuale abbiamo:

xxx colleghi in linea con il percorso - utenti che hanno completato tutti i moduli attualmente disponibili;

xxx colleghi in regola con il percorso - utenti che hanno completato tutti i moduli attualmente disponibili eccenzion fatta per quello in corso;

xxx colleghi non regolari con il percorso – utenti che hanno acquisito almeno un punto ma che non sono in linea o regolari;

xxx colleghi inattivi– utenti che non hanno acquisito punti.

Ci sono quindi un xxxx di colleghi inattivi. Richiediamo [la partecipazione di tutta la popolazione aziendale] [di tutti i colleghi] affinché il corso sia seguito nella sua interezza.

In questo periodo la sicurezza informatica è fortemente minaccia e poter riconoscere rischi e pericoli del mondo cyber ci permette di non esporci a blocchi operativi. Sviluppare un sapere comune e affinare la capacità di riconoscere i pericoli è fondamentale.

Confidiamo nella partecipazione di tutti i colleghi perché il tema della Sicurezza Informatica è un bene comune.

Cordiali saluti,

I testi ed i riferimenti sopra indicati rappresentano suggerimenti che potranno essere modificati liberamente in base allo stile ed al registro comunicativo adottato e in uso dalla Company.

Allegato A – Example Pagina Intranet

Progetto	**Programma di Cyber Security Awareness** **Proteggi la tua persona e la tua organizzazione** **I comportamenti fanno la differenza**
Programma	Dal [mese] [anno], tutto il personale [nome Company] potrà partecipare in modalità e-learning al programma formativo di Cyber Security Awareness, per aumentare la propria consapevolezza sui rischi derivanti da un cattivo utilizzo delle tecnologie digitali e imparare a proteggersi dagli attacchi cyber.
FAQ	L'obiettivo del corso è coinvolgere tutti in prima linea perché chiunque potrebbe diventare una inconsapevole vittima del cyber crime.
Report	Entra nel programma di Cyber Security Awareness, con un impegno di pochi minuti al mese potrai acquisire il giusto grado di consapevolezza e imparare a difenderti.
Note operative	Accedi alla piattaforma
Documentazione a supporto	Partecipare all'iniziativa sarà un'occasione per ampliare le proprie conoscenze divertendosi e rinforzando la collaborazione con i colleghi

Il Progetto

La [Nome Direzione sponsor iniziativa], nell'ambito delle sue competenze per la sicurezza informatica, propone un percorso semplice ed efficace che consenta ad ogni singolo individuo di riconoscere le potenziali minacce provenienti dal mondo Cyber.

Oggi si stima che un'alta percentuale di incidenti di sicurezza informatica abbia origine da una qualche forma di errore umano e tra le forme più comunemente rilevate di errori e abitudini rischiose si registra una inadeguata gestione delle proprie password, l'incapacità di riconoscere siti fraudolenti, allegati mail pericolosi e URL ingannevoli.

La proposta di questo programma nasce dunque dalla consapevolezza che la sicurezza informatica non possa essere affidata solamente ad interventi specialistici e tecnici ma si debba garantire anche investendo sul fattore umano.

In questa prospettiva, il programma di Cyber Security Awareness offre a tutto il personale un percorso semplice e in grado di sviluppare un elevato grado di consapevolezza nell'uso delle tecnologie digitali e nella navigazione Web.

Il percorso si svolge attraverso una piattaforma di e-learning e si articola in 3 livelli che saranno proposti nell'arco di [un anno, due anni, tre anni…].

Ogni livello comprende moduli dedicati ad argomenti specifici, test di apprendimento, e la partecipazione ad una fase di "gioco" *(gaming*) proposta per incentivare e vivacizzare il percorso di addestramento.

Partecipare al programma è semplice, basta accedere alla piattaforma utilizzando le credenziali individuali consegnate attraverso una mail, e seguire la video lezione proposta nel modulo.
Per eventuali necessità di chiarimento sull'accesso e sul funzionamento della piattaforma sono disponibili [FAQ o mail di supporto…].

Il programma

Il programma completo del corso di addestramento si struttura su tre livelli, che saranno proposti nell'arco di tre anni.

I contenuti

Ogni livello si struttura su 12 moduli ed 1 episodio dedicati ad argomenti specifici.
Ai moduli si accede attraverso la piattaforma di e- learning Cyber Guru Awareness.
Ogni mese viene abilitato un nuovo contenuto e il personale viene invitato a proseguire il percorso.
Il metodo di fruizione è sequenziale, è necessario, cioè, completare un contenuto prima dipassare al successivo.

Lezioni per modulo

Ogni modulo è formato da 3 lezioni brevi, ognuna delle quali è costituita da un contenuto video di pochi minuti e, come alternativa, da un documento in formato .pdf che riporta gli stessi contenuti.
Le 3 lezioni all'interno del modulo sono organizzate come segue:

- la prima lezione propone una conoscenza di base dell'argomento;
- la seconda lezione propone l'approfondimento e stimola la "prontezza" dell'utente creando le condizioni per riconoscere le minacce;
- la terza lezione propone delle best practice e stimola le risposte comportamentali corrette.

Test di apprendimento

Per passare da una lezione all'altra è necessario superare un test di apprendimento, costituito da 4 domande a risposta multipla. La lezione si considera superata quando si risponde correttamente ad almeno 3 domande su 4. Il test può essere ripetuto più di una volta, ai fini del percorso formativo viene considerato sempre il risultato migliore.

Episodi

Ogni episodio è caratterizzato da una tematica cyber specifica. La fruizione non prevede un test al completamento dell'episodio.
Anche in questo caso esiste un concetto di propedeuticità, per cui è necessario completare un episodio per passare al successivo.

La fase di gaming

Il progetto prevede:

- un sistema di **gaming individuale**, con la possibilità per chi partecipa di acquisire un punteggio personale fatto anche di medaglie e coppe;
- un sistema di **gaming a squadre**, che vede il personale di ogni [Direzione…] costituirsi come una squadra. Ogni squadra avrà un team leader e accumulerà il proprio punteggio sommando quello dei singoli componenti.

Per conoscere meglio il sistema di attribuzione del punteggio e del gioco in generale consulta il Regolamento

FAQ