PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5145 di Venerdì 15 aprile 2022

Come impostare un programma di educazione informatica dei dipendenti

Un esperimento condotto presso un'azienda inglese ha dimostrato come un programma di educazione informatica deve essere impostato in maniera corretta, per evitare reazioni assai negative.

Verso la fine dell'anno scorso, una azienda di trasporti inglese aveva deciso di effettuare un test di sensibilizzazione dei dipendenti sui problemi di sicurezza informatica. Il responsabile informatico ha quindi sviluppato un attacco con la tecnica phising, coinvolgendo tutti i dipendenti.

Il messaggio inviato prometteva a tutti i dipendenti, che avessero collaborato all'iniziativa, di offrire un significativo bonus, se avessero favorito in tutti i modi il regolare funzionamento dei mezzi di trasporto, in regime di COVID 19. Molti dipendenti dettero la loro collaborazione, ma evidentemente non vi era alcun bonus!

Le organizzazioni sindacali hanno reagito in maniera fortemente negativa, dichiarando che si trattava di un test cinico e scioccante per i soggetti coinvolti.

Ecco la ragione per la quale è opportuno che l'avvio di un programma di educazione informatica dei dipendenti, che può anche coinvolgere delle esercitazioni specifiche, deve essere impostato in modo corretto, per evitare reazioni negative.

Chi scrive, di concerto con il responsabile della sicurezza informatica di un grande ente, aveva fatto circolare una guida al comportamento nell'utilizzo di chiavette USB portatili. Nella guida si ricordava di non usare mai chiavette, di cui non si fosse certi dell'origine, per evitare che su di esse fossero presenti programmi criminosi. Dopo aver fatto circolare questa guida, è stata deliberatamente abbandonata una decina di chiavette, nell'ambito degli spazi uffici dell'azienda. Quando la chiavetta veniva inserita nel computer, si attivava in modo automatico un programma, che indicava su quale computer la chiavetta era stata installata. In molti casi, il programma mise in evidenza come la chiavetta era stata prelevata da qualche dipendente e utilizzata sul computer domestico!

Oggi sono molte le aziende specializzate, che offrono dei programmi di sensibilizzazione e cultura informatica, ma è indispensabile che questi programmi vengano gestiti in un quadro di riferimento appropriato.

Ad esempio, occorre rifuggire dall'uso di espressioni tecniche troppo specialistiche, che risultano difficilmente comprensibili ad un normale operatore.

Inoltre, occorre adottare un approccio coinvolgente, in modo che un atteggiamento frequente, del tipo "il problema della sicurezza informatica è dell'azienda e non è mio", venga rigettato al più presto.

Una tecnica assai fruttuosa è quella di convincere il dipendente che un atteggiamento corretto, in materia di sicurezza informatica, è utile non solo nel contesto aziendale, ma anche nel contesto della propria famiglia e della propria abitazione, dove certamente sono presenti dei computer, che potrebbero essere esposti a rischi informatici.

A tutti coloro che hanno partecipato ai corsi di sensibilizzazione sulla sicurezza informatica è bene rilasciare sempre un attestato, che può essere assai utile quando il dipendente deve costruire ed aggiornare il suo curriculum vitae.

Quando si effettuano delle simulazioni pratiche, è sempre bene avvertire tutti soggetti coinvolti che tra breve verrà effettuata una simulazione, per evitare proprio le reazioni negative che sono state illustrate in precedenza.

Ci troviamo in una situazione simile a quella nella quale si trova il responsabile della sicurezza aziendale, che debba effettuare una simulazione di evacuazione di emergenza dell'edificio. Tutti gli esperti, tra cui chi scrive, raccomandano di non effettuare mai queste simulazioni senza preavviso, non indicando l'ora ed il minuto in cui la simulazione verrà effettuata, ma ponendo all'ingresso dell'azienda un cartello del tipo:

"Nei prossimi giorni verrà effettuata una simulazione di evacuazione di emergenza. Vi preghiamo di rileggere le istruzioni di comportamento, che avete già ricevuto in precedenza".

Anche una attività, che con espressione anglosassone oggi viene chiamata "gamification", può essere assai interessante. Ad esempio, si possono presentare dei questionari agli allievi, che prevedono diversi esiti, in funzione delle diverse risposte date.

Ovviamente, a nulla serve avviare un programma di sensibilizzazione informatica, se l'azienda non dispone di un manuale aggiornato e posto a conoscenza di tutti i dipendenti.

Si raccomanda inoltre di evitare di dare premi o penalità a chi segue più o meno bene il corso di formazione, perché l'obiettivo è che alla fine tutti siano promossi! Questo è motivo per cui la correzione di eventuali questionari di valutazione del livello di apprendimento è bene avvenga collettivamente.

È importante anche adattare il percorso formativo ai ruoli dei partecipanti. È del tutto normale che i vari dipendenti abbiano maggiore o minore coinvolgimento nella gestione dei dati informatici aziendali e, per conseguenza, la loro formazione deve essere specificamente adattata.

Infine, a completamento di questa breve nota, offriamo ai lettori un esempio degli argomenti che dovrebbero essere trattati in un corso di sensibilizzazione su temi di sicurezza informatica:

- scelta e gestione delle parole chiave,
- la sicurezza dei dispositivi mobili, come smartphone, chiavette USB e simili,
- modalità sicure di navigazione su Internet,
- cautele da adottare sui social network,
- la sicurezza fisica degli apparati informatici,
- la cancellazione corretta dei dati,
- la gestione corretta dei dati aziendali,
- i modelli di comportamento afferenti alla riservatezza dei dati,
- le politiche BYOD-Bring your own device.

A questo punto, buon lavoro a tutti i lettori!

Adalberto Biasiotti

---

www.puntosicuro.it