Checklist sulla sicurezza informatica nel settore dell'e-commerce internazionale.

La sicurezza informatica è un fattore essenziale da considerare nel settore dell'e-commerce internazionale. Questo perché le transazioni internazionali di e-commerce spesso comportano il trasferimento di dati sensibili, come quelli finanziari e personali, attraverso confini nazionali.

Per garantire la sicurezza di questi dati, le organizzazioni devono adottare diverse misure di sicurezza, come la crittografia, i sistemi di pagamento sicuri e l'autenticazione a due fattori.

Inoltre, le organizzazioni devono assicurarsi che i loro siti web siano conformi alle leggi internazionali sulla privacy e sulla sicurezza dei dati.

Le organizzazioni devono monitorare le proprie reti alla ricerca di attività sospette e adottare misure appropriate per proteggersi dalle minacce informatiche.

Questo strumento è stato progettato per consentire agli utenti di sapere se la loro attività di e-commerce internazionale dispone di misure di base per la protezione dagli attacchi informatici. Le grandi aziende hanno spesso reparti dedicati a queste funzioni, ma le piccole imprese hanno spesso bisogno di maggiori risorse per farlo.

Questo strumento vi fornirà una panoramica completa del livello di protezione della vostra azienda contro la criminalità informatica e forse identificherà le lacune o le vulnerabilità che possono essere affrontate.

In ogni caso, l'utente verrà a conoscenza di aspetti della cybersecurity che potrebbero non essere stati considerati e che è in tempo di affrontare, personalmente o tramite professionisti specializzati.

Co-funded by the European Union

Lo strumento è una checklist con domande relative alla cybersecurity e al commercio elettronico internazionale. Per ogni domanda ci sono tre possibili risposte, a seconda dell'esperienza dell'utente:

SI: 

NO: 

NON SO: 

Supponiamo che la maggior parte delle risposte sia NO o NON SO. In questo caso, invitiamo l'utente a mettersi al lavoro per migliorare la sicurezza della propria attività di e-commerce internazionale, per evitare di essere vittima di attacchi che potrebbero portare a ingenti perdite o addirittura al fallimento dell'azienda.

Al termine della checklist, gli utenti troveranno una serie di consigli pratici sulla cybersecurity che li guideranno sui passi successivi da compiere per migliorare la sicurezza online della loro azienda internazionale.

Co-funded by the European Union

E4F

WOMEN IN GLOBAL EXPORT

e4f-network.eu

CHECKLIST:

Domande			
Il vostro sito di e-commerce è adeguatamente crittografato per proteggere le informazioni dei clienti durante le transazioni?	☐	☐	☐
Avete adottato criteri di password forti per gli account dei clienti e per quelli amministrativi?	☐	☐	☐
Aggiornate regolarmente il software del vostro sito web e le patch di sicurezza per proteggervi dalle vulnerabilità note?	☐	☐	☐
Avete un piano per rispondere a una potenziale violazione della sicurezza, ad esempio un programma di risposta alle minacce?	☐	☐	☐
Tutti i rischi sono presi in considerazione nella pianificazione aziendale? Se no, quali?	☐	☐	☐
Avete formato i vostri dipendenti sulle migliori pratiche di cybersecurity, ad esempio su come individuare e prevenire gli attacchi di phishing?	☐	☐	☐
Utilizzate sistemi di pagamento sicuri e seguite i protocolli di sicurezza standard del settore per la gestione e la trasmissione delle informazioni sensibili dei clienti?	☐	☐	☐
Disponete di misure per individuare e prevenire accessi non autorizzati al vostro sito web e ai dati dei clienti?	☐	☐	☐
Avete condotto regolari valutazioni della sicurezza e test di penetrazione per identificare e risolvere le potenziali vulnerabilità del vostro sistema di e-commerce?	☐	☐	☐
Disponete di politiche e procedure per smaltire in modo sicuro le informazioni sensibili dei clienti quando non sono più necessarie?	☐	☐	☐
Avete un processo per monitorare e rivedere regolarmente le vostre misure di sicurezza per assicurarvi che rimangano efficaci?	☐	☐	☐

Co-funded by the European Union

Suggerimenti sulla sicurezza informatica nel settore dell'e-commerce internazionale

1. Utilizzare reti sicure: assicuratevi di utilizzare reti sicure, come le reti private virtuali (VPN), per proteggere i vostri dati durante le transazioni di e-commerce.

2. Utilizzate password forti e uniche: utilizzate password forti e uniche per tutti i vostri account online ed evitate di usare la stessa password per più account.

3. Attivate l'autenticazione a due fattori: l'autenticazione a due fattori aggiunge un ulteriore livello di sicurezza ai vostri account online, richiedendo l'inserimento di un codice unico oltre alla password.

4. Mantenere aggiornati software e sistemi: aggiornate regolarmente il vostro software e i vostri sistemi per assicurarvi di avere le ultime patch e funzioni di sicurezza.

5. Utilizzare metodi di pagamento sicuri: quando si effettuano transazioni di e-commerce, utilizzare metodi di pagamento sicuri, come pagamenti con carta di credito criptata o sistemi di pagamento digitale come PayPal.

6. Attenzione agli attacchi di phishing: fate attenzione agli attacchi di phishing, che sono tentativi di indurre l'utente a fornire informazioni sensibili, come la password o i dati della carta di credito.

7. Utilizzate un software di sicurezza affidabile: utilizzate un software di sicurezza affidabile per proteggere i vostri dispositivi e i vostri dati da malware e altre minacce.

8. Fate attenzione quando condividete informazioni personali: fate attenzione quando condividete online informazioni personali come nome, indirizzo e dati della carta di credito. Condividete queste informazioni solo con siti web e commercianti fidati.

9. Utilizzare canali di comunicazione sicuri: utilizzate canali di comunicazione sicuri, come e-mail criptate o app di messaggistica, per proteggere le vostre informazioni sensibili quando comunicate con altri online.

10. Monitorare le potenziali minacce e violazioni della sicurezza e, se necessario, intervenire immediatamente.

Co-funded by the European Union

In generale, la chiave per un'efficace sicurezza informatica nel settore dell’e-commerce internazionale è l'adozione di una strategia di sicurezza completa che includa una serie di strumenti e tecnologie per la protezione dalle potenziali minacce.

Grazie!

Co-funded by the European Union