

Black Friday e Cyber Monday alle porte. Occhio alle truffe online e al phishing

venerdì 18 novembre 2022

Black Friday e Cyber Monday sono alle porte. Attenzione agli acquisti perché in questo periodo dell'anno aumentano i tentativi di truffa, il phishing che "ruba" il brand di aziende note, i falsi domini e gli attacchi di malware

Black Friday e

Cyber Monday sono alle porte, anche se molti sconti sono già partiti o partiranno molto prima delle date ufficiali su diverse piattaforme di e-commerce. Attenzione però agli acquisti perché in questo periodo dell'anno aumentano i tentativi di truffa, il phishing che "ruba" il brand di aziende note per arrivare ai dati dei consumatori, i falsi domini e gli attacchi di malware. A sollevare il tema è Check Point® Software Technologies Ltd., fornitore di soluzioni di sicurezza informatica a livello globale, che vuole sensibilizzare i consumatori e invitarli alla cautela durante gli acquisti per il Black Friday e il Cyber Monday mentre cercano offerte incredibili. Che spesso sono troppo belle per essere vere.

Black Friday e Cyber Monday, lo shopping online e i rischi

Il Black Friday

inizialmente era dedicato alle vendite nei negozi e il Cyber Monday era dedicato all'e-commerce. Ora le date sono praticamente uguali, non solo in termini di acquisti e cifre, ma anche a livello di cyber pericoli e attacchi informatici. Le previsioni di vendite quest'anno sono alte anche perché gli store online hanno iniziato a pubblicizzare le offerte con giorni di anticipo. Il budget medio dei consumatori in Italia sarà di circa 250 euro con due consumatori su tre pronti a fare acquisti online (fonte Idealo 2022).

«Black Friday

e Cyber Monday sono ottime opportunità per tutti coloro che vogliono acquistare prodotti scontati. Ma, allo stesso tempo, offrono ampi spazi di azione ai criminali informatici. È bene che tutti gli utenti adottino azioni preventive per riuscire a riconoscere le truffe informatiche, il phishing e quelle offerte 'troppo belle' per essere vere – afferma Pierluigi Torriani, Security Engineering Manager di Check Point Software – In questo tipo di giornate, abbiamo riscontrato la tendenza degli hacker a impersonare le aziende coinvolte in queste offerte speciali, come le compagnie di delivery, i brand o gli store per colpire l'utente finale. È sempre necessario fare attenzione prima di cadere in questi raggiri e prevenire le possibili truffe online».

L'anno scorso,

nei giorni precedenti al Black Friday, è stato registrato un aumento del 178% dei web store malevoli, a livello globale. Il phishing usa anche i brand di compagnie di trasporto per i suoi attacchi, facendo riferimento a nomi noti o attraverso il furto di account.

Shopping online, consigli di sicurezza

Affinché le

persone prendano le precauzioni necessarie quando acquistano i loro prodotti preferiti, gli esperti di Check Point Software condividono una serie di consigli per rimanere al sicuro mentre si fa shopping online. Ecco di

seguito.

Acquistare

sempre da una fonte autentica e affidabile: l'ideale è digitare il link dello store da cui volete acquistare il prodotto, direttamente nel motore di ricerca. Cliccare su un link inviato via e-mail senza conoscerne l'origine potrebbe essere pericoloso.

Attenzione ai

domini fasulli: è molto importante prestare attenzione ai link e ai domini delle pagine web in cui entriamo. Gli errori di ortografia o i nomi sbagliati sono un indizio per i quali le pagine visualizzate sono state create per attaccare gli utenti che ci entrano.

Le offerte

irresistibili sono sempre troppo belle per essere vere: controllate diversi siti per vedere se l'offerta è reale o meno. Uno sconto insolito su un prodotto molto richiesto potrebbe essere un chiaro indicatore di una truffa.

Cercate sempre

il lucchetto nei siti web: i siti che presentano la dicitura HTTPS invece di HTTP sono i siti sicuri e autentici. Inoltre, avranno un lucchetto posto davanti a essi per distinguerli dagli altri. Entrare solo in questi siti perché sono quelli che rispettano gli standard di sicurezza internazionali.

Disporre di

soluzioni di sicurezza per gli endpoint: dovrete disporre di tali soluzioni di sicurezza anche per la vostra posta elettronica. Con questa misura è possibile prevenire molti attacchi informatici e leak.

Attenzione

alle e-mail di reimpostazione della password: soprattutto quando il volume di traffico online è al massimo, se ricevete un'e-mail per reimpostare la password non richiesta, visitate sempre direttamente il sito web. Quindi non cliccate sui link e cambiate la vostra password per sicurezza.

Fonte HelpConsumatori

