Black Friday 2020: un’occasione d’oro per criminali informatici

Bitdefender invita a tenere sotto controllo gli inviti per lo shopping su appuntamento, le super offerte, i QR code e l’arrivo di Playstation 5 – I consigli per un Black Friday all’insegna della sicurezza informatica

Milano, 11 novembre 2020 - Con l'avvicinarsi della stagione natalizia, gli acquirenti di tutto il mondo si preparano per le annuali occasioni di shopping offerte dal **Black Friday** dalle loro marche di abbigliamento, tecnologia ed elettrodomestici preferiti, per le quali i rivenditori scendono in campo con le migliori offerte online e in-store. Si tratta di uno degli eventi di shopping più attesi dell'anno dai consumatori, importato dagli Stati Uniti, ma che ormai anche in Italia rappresenta un primo **barometro sull'andamento dei consumi per il periodo natalizio**. Un indicatore nel 2020 particolarmente importante, data la situazione economica generale e le restrizioni anti-Covid per il mondo retail.

La data clou sarà il week end del 27 novembre ma **gli esercenti hanno già gradualmente iniziato a comunicare i loro piani di offerte**: la tendenza di quest’anno è estendere l’iperbole delle promozioni iniziando ad anticipare gli sconti di qualche settimana. **Questo offre ai criminali informatici un’ampia finestra temporale di opportunità per attirare e colpire le potenziali vittime**. Infatti, il Black Friday rappresenta per loro un’occasione d’oro per prendere di mira gli acquirenti desiderosi di approfittare degli sconti offerti online.

Lo shopping oggi più che mai è online, il terreno di caccia dei criminali informatici

La pandemia ha incrementato l’e-commerce: con la crisi sanitaria è infatti cambiato il comportamento d’acquisto in tutto il mondo. Il 62% dei consumatori fa acquisti online più adesso che prima della pandemia, e si prevede che i numeri aumenteranno durante le festività natalizie.

Secondo una ricerca internazionale effettuata da Shopify, l’**84% degli italiani prevede di fare acquisti** in occasione del Black Friday 2020, con uno scontrino medio intorno ai 377 euro a testa.

Il **49% degli italiani dichiara che vorrebbe fare shopping sia online sia offline**, mentre ben il 63% degli intervistati ritiene che la nuova ondata pandemica incentiverà gli acquisti online. Secondo un recente sondaggio, i **consumatori negli Stati Uniti dovrebbero spendere un totale di 148,5 miliardi di dollari** durante questo Black Friday. Si tratta di **cifre allettanti per i criminali informatici** che mirano a trarne vantaggio.

Il retail phishing è aumentato del 233 % nel 2019, rivelando che i siti di e-commerce sono obiettivi primari per lo spoofing dei siti web durante le festività natalizie, poiché preparano diligentemente offerte e coupon.

Una marea di pubblicità aggressiva attraverso i social media e la posta elettronica può indurre i consumatori a ignorare i segnali di allarme, rendendoli ancora più suscettibili alle truffe di phishing per la raccolta delle credenziali, ai ladri di account e alle frodi.

Addio alla frenesia da Black Friday

Fare shopping comodamente a casa propria in pigiama sembra fantastico, ma spesso innamorarsi di un'offerta con uno sconto troppo elevato per essere vero potrebbe trasformarsi in un incubo per gli acquirenti.

Bitdefender invita quest'anno a prestare particolare attenzione agli inviti per prenotare lo shopping su appuntamento, in quanto i cybercriminali potrebbero sfruttare i sistemi di programmazione già predisposti da alcuni rivenditori per evitare le lunghe code. Inoltre è raccomandabile ispezionare attentamente le offerte prima di "riservare" il proprio posto per avere la possibilità di fare acquisti in anticipo e ottenere super sconti.

È meglio controllare il sito ufficiale del venditore prima di iscriversi, pagare per un accesso esclusivo in negozio o fornire informazioni personali compilando un modulo online.

I criminali informatici stanno anche approfittando dell'attesissima uscita della nuova console PlayStation 5, destinata ad arrivare nei negozi il 19 novembre. Il Laboratorio Antispam di Bitdefender ha registrato un picco nella corrispondenza relativa alla PS5 tra il 29 e il 30 ottobre 2020, quando più del 72% di tutte le email ricevute da PlayStation sono state contrassegnate come spam.

Attenzione ai QR code

La pandemia ha portato anche ad un incremento dell’utilizzo dei QR code. Si stima che circa 11 milioni di famiglie negli Stati Uniti scansioneranno un QR code nel solo 2020.

I QR code possono essere utilizzati negli annunci pubblicitari e nelle promozioni per reindirizzare i clienti verso le pagine web dei prodotti, dove possono aggiungere rapidamente la merce al loro carrello della spesa online. Sebbene questo metodo sia efficiente in termini di tempo per il

cliente, i criminali informatici potrebbero creare codici QR dannosi e codificare payload personalizzati per reindirizzare gli utenti verso siti web fasulli e rubare dati personali o installare malware sui dispositivi dell'utente.

Consigli per un Black Friday all'insegna della cybersecurity

1. **Fidarsi di ciò che si conosce** ed evitare di cliccare sui link nelle email o sulle piattaforme dei social media che pubblicizzano sconti speciali e offerte di rivenditori sconosciuti. Controllare la sintassi e l'ortografia di ogni email che si riceve e passare il mouse sul link per assicurarsi che conduca realmente a un sito ufficiale. Le email di phishing sono lo strumento più utilizzato dai truffatori, e sono un modo comune per rubare informazioni personali e finanziarie.
2. **Utilizza una rete sicura** durante la navigazione per fare acquisti. Circa l'82% degli acquirenti controlla i propri telefoni in negozio prima dell'acquisto, quindi evitare di collegarsi a qualsiasi rete Wi-Fi pubblica o di controllare i siti bancari, in quanto i criminali informatici potrebbero aver compromesso la rete.
3. **Attivare l'autenticazione a due (2FA) o più fattori (MFA)** per tutti i conti online e le transazioni finanziarie, ove possibile. Questo ulteriore livello di sicurezza potrebbe proteggere dalle frodi, anche se l'aggressore è in possesso delle credenziali di accesso dell'utente.
4. **Modificare le password di tutti gli account online**, in particolare di quelli affiliati ai rivenditori online. Anche se questa fase di sicurezza potrebbe richiedere molto tempo, non è mai troppo tardi per rivedere le impostazioni degli account e preferire password solide e difficili da indovinare. È sempre possibile utilizzare un gestore di password dedicato per tenere sotto controllo i dati di accesso.
5. **Impostare avvisi per le carte di credito** che possono aiutare a proteggere l'utente dalle frodi, notificando rapidamente gli addebiti sospetti o insoliti. Se i dati della carta di credito vengono utilizzati, si riceveranno delle notifiche in tempo reale che permetteranno di evitare che i truffatori causino danni finanziari.
6. **Utilizzare una soluzione di sicurezza su tutti i dispositivi**: **è** il primo passo per proteggere in locale i dati personali. Saranno così scongiurate minacce dannose e i dati sensibili saranno al riparo dai criminali informatici.

***

A proposito di Bitdefender

Bitdefender è un leader globale della sicurezza informatica che protegge oltre 500 milioni di sistemi in più di 150 paesi. Dal 2001, l'innovazione di Bitdefender ha costantemente fornito prodotti di sicurezza pluripremiati e informazioni sulle minacce per la casa connessa in modo intelligente, gli utenti mobili, le aziende moderne e le loro reti, dispositivi, data center e infrastrutture cloud. Oggi, Bitdefender e i suoi Labs sono anche il fornitore di fiducia, integrato in oltre il 38% delle soluzioni di sicurezza del mondo.

Riconosciuta dall'industria, rispettata dai fornitori ed evangelizzata dai clienti, Bitdefender è la società di sicurezza informatica di cui puoi fidarti e su cui puoi fare affidamento.

***

Per ulteriori informazioni

Prima Pagina Comunicazione

02/91339820

Tania Acerbi, Monica Fecchio, Elisa Pagano

tania@primapagina.it

monica@primapagina.it

elisa@primapagina.it