Black Friday: Vorsorgen, für eine sichere Schnäppchenjagd

Am 26. November ist es wieder so weit, zahlreiche Schnäppchenjäger freuen sich bereits auf die Angebote am Black Friday. Aber Achtung, auch Hacker und Onlinebetrüger stehen bereits in den Startlöchern. Hier erfahren Sie, wie Sie Warnsignale erkennen und sich vor Angriffen schützen können, für ein sicheres Shoppingerlebnis.

Der Black Friday und die Black Week verhelfen dem November dazu, sich als einer der umsatzstärksten Monate des Jahres zu etablieren. Zahlreiche Menschen warten das ganze Jahr auf die Sonderangebote und Schnäppchen in der Vorweihnachtszeit – darunter auch Hacker und Onlinebetrüger, welche sich dadurch, so wie die Händler, große Gewinne erwarten.

Vertrauliche Daten als Beute

Die Hauptbedrohung dieses Shoppingereignisses stellt nach wie vor Phishing dar. Phishing bezeichnet die nicht autorisierte Beschaffung von persönlichen Daten wie z.B. Kreditkarten- oder Kontonummern, Passwörtern oder Adressen. Dabei wird versucht, die enthusiastischen und deshalb oft leichtsinnigen Schäppchenjäger durch gefälschte E-Mails, Direktnachrichten oder Webseiten dazu zu bewegen, diese vertraulichen Daten preiszugeben. Die Folgen dieser Angriffe können gravierend sein: es kann beispielsweise zu Identitätsdiebstahl, Kontenplünderung oder Malware kommen.

Wann ist Vorsicht geboten?

Viele Hackerangriffe wirken auf den ersten Blick sehr professionell und sind für das Opfer häufig nur schwer zu erkennen. Es gibt aber trotzdem einige grundlegende Warnsignale, welche Sie kennen sollten, um gar nicht erst auf die Masche der Onlinebetrüger hineinzufallen.

Werden Sie in einer E-Mail etwa um die Angabe von vertraulichen Daten wie Passwörtern, Kreditkartendaten etc. gebeten ist Vorsicht geboten. Auch bei Ihnen nicht vertrauten, „komischen" Absenderadressen und weiteren Empfängern in der Kopie (CC) sollten Sie die Seriosität hinterfragen und keine Informationen preisgeben. Lassen Sie sich dabei nicht von knappen Fristen und „Drohungen" verwirren, da auch diese typisch für Hackerangriffe sind.

Kommt Ihnen eine E-Mail unseriös oder verdächtig vor, so vermeiden Sie es unbedingt, die Anhänge zu öffnen. Dubiose Anhänge können Sie gegebenenfalls an den Formaten erkennen: besondere Vorsicht ist beispielsweise bei Dateiformaten wie .exe, .com, .msi oder .scr geboten.

Suchen Sie auf Websites, die Ihnen nicht ausreichend vertraut sind, immer nach dem Impressum. Onlinebetrüger erstellen häufig kein Impressum, während ein seriöser Händler immer ein solches vorliegen haben wird. Auch die Menüpunkte auf den Webseiten von Onlinebetrügern funktionieren häufig nicht.

Gut vorbereitet in die Einkaufszeit

Oft reicht das reine Erkennen der oben genannten Signale allerdings nicht aus. Um gut vorbereitet auf das Onlineshopping zu sein, sollten Sie also noch weitere Punkte beachten:

- Nutzen Sie eine fortschrittliche Sicherheitslösung, die präventiv vor Gefahren schützt.
- Statten Sie Ihr Gerät mit einer Lösung aus, die durch Social Engineering initiierte Attacken abwehrt.
- Implementieren Sie eine Lösung, die vor infizierten Webseiten warnt und das Herunterladen von Schadcodes verhindert.
- Aktivieren Sie einen Werbeblocker.

KONVERTO AG | S.p.A. via Bruno-Buozzi-Str. 8, 39100 Bozen | Bolzano
Info Center 800 031 031 T 0471 064 500 info@konverto.eu info@pec.konverto.eu konverto.eu

- Tätigen Sie keine Transaktionen, während Sie ein öffentliches WLAN nutzen, dies erleichtert es den Hackern sich Ihre Daten zu sichern.
- Achten Sie darauf, dass Sie ein sicheres und komplexes Passwort erstellen und ändern Sie dieses in regelmäßigen Zeitabständen.
- Hinterlegen Sie Passwörter und Zahlungsmodalitäten nie, sondern erfassen Sie diese vertraulichen Daten bei jedem Einkauf neu.
- Installieren Sie auf Ihrem Gerät die aktuelle Version des Betriebssystems, aller Browser und Plug-Ins und des Antivirenprogrammes.

Durch die Anwendung dieser Lösungen und Sicherheitsregeln, können Sie beruhigt shoppen und vielen Cyberattacken zuvorkommen.

Neben einer zuverlässigen Antivirus-Software für PC, Tablet und Smartphone in privaten Haushalten bietet KONVERTO hochspezialisierte und individuell konzipierte Security-Lösungen für Unternehmen. Wir sind auf intelligente Sicherheitslösungen spezialisiert und setzen auf innovative Lösungen zum Rundum-Schutz von Unternehmensnetzen.

Black Friday: suggerimenti per una caccia all'affare sicura

Manca poco al 26 novembre e molti cacciatori di occasioni sono già in attesa delle offerte del Black Friday. Ma attenzione, anche gli hacker e i truffatori online sono già in agguato. Scopri come si riconoscono i segnali di avvertimento per proteggersi dagli attacchi e vivere un'esperienza di shopping sicura.

Il Black Friday e la Black Week aiutano novembre ad affermarsi come uno dei mesi più redditizi dell'anno. In molti aspettano proprio queste offerte speciali e occasioni del periodo che precede il Natale - compresi gli hacker e i truffatori online che si aspettano di fare grandi profitti, proprio come i rivenditori.

Caccia ai dati

La principale minaccia per questo appuntamento di shopping continua ad essere il phishing. Il phishing si riferisce all'acquisizione non autorizzata di dati personali come numeri di carte di credito, di conti orrenti, password o indirizzi. Si tenta di persuadere i utenti entusiasti e quindi spesso incauti a divulgare questi dati confidenziali per mezzo di false e-mail, messaggi o siti web fasulli. Le conseguenze di questi attacchi possono essere gravi, come il furto di identità, il saccheggio dell'account o un'infezione da malware.

Quando prestare attenzione

Molti attacchi sembrano professionali a prima vista e sono spesso difficili da riconoscere per la vittima. Tuttavia, ci sono alcuni segnali di cui si dovrebbe essere consapevoli al fine di non cadere in trappola.

Se in una e-mail viene chiesto di fornire dati confidenziali come password o dettagli di carte di credito, è opportuno fare attenzione. Bisogna inoltre mettere in dubbio la serietà di qualsiasi indirizzo mittente sconosciuto o "strano", soprattutto nel caso ci fossero altri destinatari in copia (CC). È fondamentale non farsi confondere dalle scadenze e dalle "minacce", anche queste sono tipiche degli attacchi degli hacker.

Se una e-mail sembra dubbia o sospetta, bisogna evitare di aprire gli allegati a tutti i costi. Potrebbe essere possibile riconoscere gli allegati insoliti dai loro formati: si consiglia una particolare cautela, per esempio, con formati di file come .exe, .com, .msi o .scr.

Consigliamo inoltre di cercare sempre le proprietà dei siti web, un commerciante rispettabile ne avrà sempre una. Inoltre, le voci di menu sui siti web dei truffatori online spesso non funzionano.

Prepararsi alla stagione dello shopping

Spesso, però, il semplice riconoscimento dei segnali di cui sopra non è sufficiente. Quindi, per essere preparati per lo shopping online, si dovrebbe prestare attenzione a ulteriori punti:

- Utilizzare una soluzione di sicurezza avanzata che fornisce una protezione preventiva contro i pericoli.
- Equipaggiare il vostro dispositivo con una soluzione che respinge gli attacchi innescati dal social engineering.
- Implementare una soluzione che avvisi in caso di siti web infetti e impedisca il download dannosi.
- Attivare un blocco degli annunci.

- Non eseguire transazioni mentre si utilizza una rete Wi-Fi pubblica, questo rende più facile per gli hacker rubare i tuoi dati.
- Assicurarsi di creare password sicure e complesse e cambiale a intervalli regolari.
- Non memorizzare mai le password e i metodi di pagamento, ma inserire nuovamente questi dati riservati ad ogni acquisto.
- Installare l'ultima versione del sistema operativo, di tutti i browser, i plug-in e il programma antivirus sul vostro dispositivo.

Applicando queste soluzioni e regole di sicurezza, è possibile fare acquisti in tutta tranquillità ed evitare molti cyberattacchi.

Oltre all'affidabile software antivirus per PC, tablet e smartphone per privati, KONVERTO offre soluzioni di sicurezza altamente specializzate e progettate individualmente per le aziende. Siamo specializzati in soluzioni di sicurezza intelligenti e ci concentriamo su soluzioni innovative per la protezione completa delle reti aziendali.