Der große Black Friday 2020 naht – fünf praktische Tipps zum sicheren Online-Einkauf

Traditionell ist der Black Friday das Hochfest der Schnäppchenjäger weltweit. Und in diesem Jahr verspricht er ein gigantisches Geschäft zu werden. Klar droht dabei auch Unbill durch Cyber-Betrüger. Wie man seine Daten und Systeme sicher durch den Angebotsk(r)ampf führt, verrät Sophos.

Der Black Friday in den Vereinigten Staaten ist der Freitag *nach* dem Fest Thanksgiving und in *diesem* Jahr der 27. November. Nicht nur in den USA, sondern weltweit überbieten sich Händler und Online-Händler rund um diesen Termin mit unglaublichen Angeboten.

Zur Bezeichnung Black Friday kam es durch eine Kombination aus dem Brückentag, den sich viele Amerikaner nach Thanksgiving frei nehmen und einer Anspielung auf die Tintenfarbe Schwarz, mit der Buchhalter früher positive Positionen (im Gegensatz zu den roten Negativen) verbuchten. Dieser Tag wurde als Schwarzer Freitag bekannt, weil es ein Tag war, an dem so viel gekauft wurde, dass viele Einzelhändler ausreichend Geld verdienen konnten, um ihre jährlichen Handelskonten in die schwarzen Zahlen zu bringen. Heute ist der Black Friday auf der ganzen Welt gleichbedeutend mit massiven Verkäufen, enormen Rabatten und einigen erstaunlich guten Angeboten, besonders bei technischen Geräten. Das ursprüngliche Konzept wurde dabei inzwischen großzügig abgewandelt und etwa zur „Black Friday Week“ oder sogar zum „Black Friday Month“ erweitert.

In diesem besonderen Jahr 2020 wird für den Online-Handel am Black Friday Großes erwartet. Das gilt besonders auch für Länder, in denen das Einkaufen in den Geschäften aufgrund eines Lockdowns ausscheidet und nur online stattfinden darf.

Angesichts all der verlockenden Rabatte verlieren zahlreiche Nutzer allerdings die Sicherheit aus dem Blick. Schnell kann so nicht nur Geld für die vermeintlichen Schnäppchen verloren gehen, sondern auch Kreditkartennummern, Passwörter oder andere persönliche Informationen.

Wichtig ist also – und das gilt natürlich nicht nur für die Black-Friday-Zeit – immer ein solides Sicherheitssystem aufrecht zu erhalten.

Sophos zeigt anhand 5 praktischer Tipps wie der Online-Einkauf sicher bleiben kann:

1. Kontaktdaten der Finanzdienstleister notieren
Wenn man Mobilgeräte oder Kreditkarten verliert bewährt sich der gute alte Notizzettel. Darauf sollten Notfallkontaktnummern und Ansprechpartner stehen, von Banken, Versicherungen etc. So kommt man nicht in Verlegenheit, sich auf Kontaktdaten verlassen zu müssen, die aus einer gefälschten E-Mail kommen.

2. Wie sperre ich mein Konto?
Um im Fall der Fälle gewappnet zu sein, sollte man sich bei Bank oder Kartenaussteller zur Funktion der Kontosperrung informieren. Mittlerweile verfügen viele Anbieter über eine "Schnellverriegelungsoption", mit der sich der Zugriff auf Konto oder Zahlungskarte innerhalb von Sekunden einfrieren und wieder freigeben lässt. Hat man den Verdacht, seine Kartennummer auf einer gefälschten Website eingegeben zu haben, lässt sich der Zugang sofort sperren, noch bevor man die Bank um Rat fragen kann (siehe 1.).

3. Autofill-Speicher des Browsers bereinigen
Praktisch, wenn der Browser sich via Autofill Passwörter, Adressen und Kreditkartennummern merkt und bei Bedarf automatisch anbietet. Man sollte diese „fast online“ in einem Speicher abgelegten Daten aber dennoch für seine eigenen Browser überprüfen und korrigieren, um seine Daten so auch bei Diebstahl des Gerätes zu schützen. Das geht so:
Bei Firefox wählt man die Einstellungen: Präferenzen > Datenschutz und Sicherheit > Formulare und Automatisches Ausfüllen.
Bei Chrome und Safari wählt man die Einstellungen: Automatisches Ausfüllen.
Bei Edge wählt man die Einstellungen: Profile > Zahlungsinfo.

4. Verwendung von Pre-paid Karten
Will man bei einem Händler einkaufen, über den man nicht viel weiß, macht es Sinn, diesen Einkauf mit einer Pre-paid Karte von geringem Wert zu begleichen. Diese sind mittlerweile in fast jedem Supermarkt erhältlich. Vorteil 1: Eine vorausbezahlte Karte im Wert von zum Beispiel 50 Euro verringert das Risiko für genau diesen Betrag (wenn das Geld weg ist, hört die Karte einfach auf zu funktionieren). Vorteil 2: Die Karte ist nicht mit einem anderen Konto verknüpft.

5. Zwei-Faktor-Authentifizierung wo immer möglich
Der Vorteil einer Zwei-Faktor-Authentifizierung besteht darin, dass ein Krimineller, der an das Passwort für einen Dienst herangekommen ist, auch im Besitz eines Gerätes sein muss, um sich einzuloggen. Das macht den Missbrauch von Konten und Daten um ein Vielfaches schwerer. Besonderes Augenmerk sollte dabei auch auf einem sicheren E-Mail-Konto liegen.

Und nun: Fröhliches und sicheres Shoppen.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de