Das größte Shopping-Event des Jahres steht bevor
Ein Fest nicht nur für viele Verbraucher, sondern auch für Cyberkriminelle

Online-Shopping mit Erfolg und gutem Gefühl hängt nicht nur von echten Schnäppchen und wirklichem Bedarf ab – wer in der Hektik Betrügern auf den Leim geht, zahlt am Ende sogar drauf. Wer die acht Sicherheitstipps von Sophos beachtet, hat beste Chancen für ein glückliches Shopping-Erlebnis.

Auf den 29. November und 2. Dezember fiebern Schnäppchenjäger schon lange hin. Manch einer wird sich da endlich einen langersehnten Wunsch erfüllen oder Notwendiges günstiger kaufen wollen. An Black Friday und Cyber Monday locken kleine und große Händler mit verlockenden Angeboten zum größtem Shopping-Event des Jahres und läuten gleichzeitig die umsatzstarke Weihnachtszeit ein.

Mittlerweile kann man sich gut auf den Shopping-Wahn vorbereiten: Wunschlisten festlegen, wirkliche Rabatte von Blendwerk unterscheiden, und am wichtigsten: die Sicherheitseinstellungen fürs Online-Shoppen aktualisieren. Los gehts:

1. **Einen Ad-Blocker verwenden:** Werbung verfolgt nicht nur jede Bewegung und sammelt so viele Informationen wie möglich über Nutzergewohnheiten, sondern sie ist auch eine Hauptquelle für bösartige Links und irreführende Inhalte im Internet. Das Surfen ist ohne Werbung nicht nur sicherer, sondern auch schneller.

2. **Privat Surfen oder im Inkognito-Modus**: Um zu verhindern, dass die eigenen Einkaufsgewohnheiten und -interessen von Website zu Website verfolgt werden, sollte man privates Surfen (z.B. Firefox) oder den Inkognito-Modus (z.B. Chrome) aktivieren, um die Tracking-Cookies blockieren.

3. **Wirksamer Cyberschutz:** Für die Cybersicherheit sollte auf allen Desktops und Laptops ein guter Cyberschutz installiert sein, der zuverlässig die Machenschaften von Hackern erkennt und eliminiert. Sicherheits-Tools für mobile Geräte sorgen für deren Cyberschutz und erhöhen mit Funktionen wie Authenticator, Password Safe, Secure QR Code Scanner oder einem Privacy Advisor die Sicherheit noch weiter.

4. **Kein Konto bei mehreren Diensten**: Beim Anmelden auf einer E-Commerce-Website ist es oft verlockend, die Schaltfläche „Mit Facebook anmelden“ oder „Mit Google anmelden“ zu verwenden. Es dauert zwar ein paar Minuten länger, ein neues Login zu erstellen, aber es bietet mehr Privatsphäre, da man nicht alle Websites, auf denen man einkauft, mit diesen Tech-Giganten teilt.

5. **Lieber Gast-Login verwenden**: Viele Websites bieten nicht nur die Möglichkeit, ein Konto von anderen Websites zu verwenden, sondern auch ein Gast-Login zu nutzen, anstatt ein neues Konto zu erstellen. Wer auf dieser Webseite nur einmalig bestellen will, sollte das Angebot nutzen.

6. **Keine Kartendaten speichern**: Viele E-Commerce-Websites speichern standardmäßig die Kreditkarteninformationen für die "Bequemlichkeit" der Nutzer (oder in der Hoffnung, dass Sie dort wieder einkaufen). Aber: Die Websites können nicht verlieren, was sie nicht haben. Lieber nur dann diesen Service wählen, wenn es absolut notwendig ist.

7. **Vorsicht bei Direktnachrichten über soziale Medien/Chat-Apps:** Mit moderner, generativer KI-Technologie ist es fast trivial, einen kompletten gefälschten Online-Shop zu erstellen und Menschen mit Direktnachrichten inklusive Link dazu zu bringen, ihre persönlichen Informationen und Zahlungsdaten dort zu teilen. Am sichersten ist es, auf etablierten Websites einzukaufen und bei Nachrichten von Unbekannten auf Social-Media-Plattformen trotz Shoppingfieber wachsam zu bleiben.

8. **Achtung vor dubiosen Lockangeboten:** Finger weg von Angeboten in E-Mails, die zu gut aussehen, um wahr zu sein oder von Unternehmen stammen, bei denen man gar kein Konto hat - es könnte sich hierbei um Phishing-E-Mails handeln, die den Kaufwilligen dazu verleiten sollen, auf Links zu gefälschten, bösartigen Websites zu klicken.

Neben diesen acht Tipps sollten alle Schnäppchenjäger generell darauf achten, dass ihre Mobiltelefone, Tablets, Laptops oder Computer auf dem neuesten Stand sind und alle Sicherheits-Updates durchgeführt werden. Denn nicht nur in diesen Zeiten sind bekannte Sicherheitslücken in Betriebssystemen und Applikationen eines der Haupteinfallstore für Cyberkriminelle.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

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