Auch die Cybergauner lieben die Vorweihnachtszeit: So gehen Sie im Endspurt des Geschenkekaufs auf Nummer sicher

10 Tipps von Sophos, um auch in der heißen Phase des Online-Geschenkekaufs sicher zu sein

Von Chester Wisniewski, Global Field CTO bei Sophos

Es ist wieder soweit: der Weihnachtseinkauf geht in die intensivste Phase, die Online-Shopping-Drähte laufen heiß. Dies wissen und nutzen auch Cyberkriminelle, die genau zu dieser Zeit die größte Datenbeute machen können. Damit Sie nicht zu den Opfern gehören, beherzigen Sie bitte die folgenden 10 simplen Tipps:

1. **Verwenden Sie einen Add-Blocker:** Werbung verfolgt nicht nur jede Ihrer Bewegungen und sammelt genug Informationen über Ihre Gewohnheiten, 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 und verbraucht weniger Bandbreite. Zwei unserer Favoriten sind uBlock Origin und Ghostery.
2. **Nutzen Sie das private Surfen oder den Inkognito-Modus**: Um zu verhindern, dass Ihre Einkaufsgewohnheiten und -interessen von Website zu Website verfolgt werden (und möglicherweise anderen Nutzern Ihres Geräts verraten, welche Geschenke Sie kaufen), sollten Sie privates Surfen (Firefox) oder den Inkognito-Modus (Chrome) aktivieren, die Tracking-Cookies blockieren.
3. **Machen Sie Ihren Browser "datenschutzsmart"**: Die Electronic Frontier Foundation (EFF) bietet eine Browsererweiterung namens Privacy Badger an, die automatisch die richtigen Entscheidungen beim Surfen trifft und dabei unsere Privatsphäre schützt und unsichtbare Tracker blockiert.
4. **Vermeiden Sie die Verwendung eines Kontos bei mehreren Diensten**: Beim Anmelden auf einer E-Commerce-Website anmelden, 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 Sie nicht alle Websites, auf denen Sie einkaufen, mit diesen Tech-Giganten teilen.
5. **Verwenden Sie einen Gast-Login**: 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. Dies ist eine gute Option, wenn Sie nicht erwarten, dass Sie technische Unterstützung benötigen oder regelmäßig Geschäfte machen: Weniger Passwörter, weniger persönliche Daten, weniger Probleme, wenn Sie gehackt werden.
6. **Speichern Sie keine Kartendaten**: Viele E-Commerce-Websites speichern standardmäßig Ihre Kreditkarteninformationen in Ihrem Profil für Ihre "Bequemlichkeit" (oder in der Hoffnung, dass Sie dort wieder einkaufen). Aber: Die Websites können nicht verlieren, was sie nicht haben. Wählen Sie die Option Ihre Kartendaten zu speichern daher grundsätzlich nicht, bzw. wirklich nur dann, wenn es absolut notwendig ist.
7. **Nutzen Sie temporäre Kartennummern**: Viele Finanzdienstleister bieten jetzt temporäre oder einmalig verwendbare Kreditkartennummern an. Sie können die App auf Ihrem Telefon oder in Ihrem Browser öffnen und eine Einweg-Kreditkartennummer erhalten, um Kartenbetrug und Nachverfolgung zu verhindern, wenn Händler Karten-Verarbeiter gemeinsam nutzen. Manchmal können Sie sogar ein Kartenlimit für die temporäre Nummer festlegen, um Ihr Konto weiter zu schützen.

8. **Verwenden Sie Kredit statt Debit:** Wir alle müssen aufpassen, dass wir während der Feiertage nicht zu viel ausgeben, aber es ist am besten, die Debitkarte zu Hause zu lassen. Kreditkarten bieten deutlich mehr Schutz vor Online-Betrug, und Sie sind in einem Streitfall in der besseren Position: Sie können Ihre Rechnung einfach nicht bezahlen und die Abbuchung anfechten, anstatt dass Kriminelle Ihr hart verdientes Geld direkt von Ihrem Bankkonto abheben.
9. **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 dazu zu bringen, ihre persönlichen Informationen und Zahlungsdaten zu teilen. Am sichersten ist es, auf etablierten Websites oder solchen, die Ihnen persönlich von Freunden und Familie empfohlen wurden, einzukaufen. Viele unaufgeforderte Nachrichten führen zu Datensammlungen oder Diebstahl.
10. **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 Sie kein Konto haben - es könnte sich hierbei um Phishing-E-Mails handeln, die Sie dazu verleiten sollen, auf Links zu gefälschten, bösartigen Websites zu klicken.

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