Sicheres Einkaufen im Internet

Ein **TrendLabs** E-Guide für die digitale Welt

von Paul Oliveria, TrendLabs Security Focus Lead

Online-Shopping erfreut sich immer größerer Beliebtheit – es ist einfach, bequem und bietet eine enorme Auswahl. Mit computerbasiertem E-Commerce wurde Anfang 2013 ein Rekordumsatz von 49,8 Milliarden USD erwirtschaftet. Dies ist ein Zuwachs von 16 % gegenüber dem Vorjahr.

Und Sie brauchen zum Einkaufen nicht einmal mehr einen Computer oder ein Notebook. Das Online-Shopping über mobile Geräte wird zunehmend beliebter. Tatsächlich wird bereits einer von zehn US-Dollar für Online-Käufe über mobile Geräte ausgegeben.

Doch ebenso wie bei finanziellen Transaktionen mit einem menschlichen Gegenüber sollten Sie bei Online-Käufen Vorsicht walten lassen. Beim Online-Shopping müssen Sie häufig Daten wie Namen, Adresse, E-Mail-Adresse und Kreditkartendaten angeben, die allesamt das Ziel von Cyber-kriminellen werden können. Wenn Sie die folgenden Tipps beachten, können Sie sowohl Ihre Daten als auch Ihr Geld schützen.

Privatsphäre statt Öffentlichkeit

Öffentliche Hotspots und Netzwerke verführen Sie vielleicht dazu, unterwegs schnell mal Einkäufe zu erledigen. Doch möchten Sie Ihre Kreditkartendaten wirklich in einem Netzwerk preisgeben, auf das jeder, also auch jeder Kriminelle, problemlos zugreifen kann?

Wenn Sie mit dem gleichen Netzwerk verbunden sind, können Cyberkriminelle Ihre Sitzungen ausspionieren, Ihre Daten entwenden und Ihre Konten kapern. Dies ist nicht auf Computer beschränkt. Cyberkriminelle können auch auf Ihrem Smartphone Schaden anrichten. Sie können unbemerkt Malware in Ihren Systemen ablegen.

Wenn Sie über einen öffentlichen Computer auf Ihre Online-Konten zugreifen, erhöhen Sie damit das Risiko, dass Ihre Konten gehackt und Ihre Daten entwendet werden. Öffentliche Computer können auch mit Malware infiziert sein.

Kaufen Sie nur im Internet ein, wenn Sie wissen, dass die Verbindung über ein sicheres Netzwerk hergestellt wird. Solange Sie Ihr Gerät und Ihr privates Netzwerk vor Eindringlingen schützen, können Sie sicher und unterbrechungsfrei einkaufen.

Lesezeichen und seriöse Apps

Falls Sie regelmäßig auf bestimmten Websites einkaufen, erstellen Sie Lesezeichen für den nächsten Besuch. Cyber-kriminelle machen sich Tippfehler bei der Eingabe zunutze, die Sie auf gefälschte Websites führen. Die Ergebnisse von Suchmaschinen können auch so manipuliert werden, dass die bösartigen Websites zu Beginn der Liste angezeigt werden. Dass Sie auf einer falschen Website sind, stellen Sie eventuell erst fest, wenn es bereits zu spät ist.

Da immer mehr Websites Zugriff für mobile Geräte bieten, lohnt es sich auch, nach Möglichkeit offizielle Apps zu verwenden. Ebenso wie Lesezeichen verringern Apps das Risiko, dass Sie versehentlich eine bösartige Website aufrufen, insbesondere weil es schwieriger ist, gefälschte Seiten auf dem kleinen Display eines mobilen Gerätes zu erkennen. Sie müssen nur sicherstellen, dass die App, die Sie herunterladen, von der Website selbst stammt. Auch hier sind Fälschungen leider gang und gäbe.

Vorsicht bei Sonderangeboten

Sonderangebote gibt es im Internet wie Sand am Meer. Beim Online-Shopping werden Ihnen Rabatte, Gutscheincodes und sogar Gratisproben angeboten. Leider sind auch viele gefälschte Angebote und Betrugsversuche dabei.

Man kann sich leicht von Angeboten blenden lassen, die ein Schnäppchen versprechen. Doch auch hier gilt: Übermut tut selten gut. Cyberkriminelle machen gerne unseriöse Versprechungen, um an Ihre Daten zu gelangen.

Vertrauen Sie daher nur Sonderangeboten, die von renommierten Online-Händlern stammen. Im Gegensatz zu unbekannten Websites bieten etablierte Websites mehr Möglichkeiten zum Schutz Ihrer Daten. Recherchieren Sie vor dem Einkauf über eine neue Website, wie die Sicherheit dieser Website bewertet wurde.

Für Werbeaktionen oder zum virtuellen Einkaufen sind auch QR-Codes inzwischen weit verbreitet. Dies können sich Kriminelle zunutze machen, indem sie QR-Codes in Umlauf bringen, mit denen Malware auf Ihre Geräte heruntergeladen wird oder die Sie auf Phishing-Websites führen.

Überprüfen Sie die QR-Codes vor dem Einscannen. Suchen Sie nach genaueren Informationen wie Markennamen oder Beschreibungen. Es ist auch hilfreich zu wissen, wo sich der QR-Code befindet. Wenn der QR-Code in einer Zeitung abgedruckt ist, hat er eine höhere Sicherheitsstufe als ein Code auf einem Aufkleber im öffentlichen Raum.

Achten Sie auf Ihre Brieftasche

Es geht um Geld. Deshalb ist der Bezahlvorgang meistens der Teil des Online-Einkaufs, der die meisten Nerven kostet. Schließlich möchte niemand, dass ein Einkauf mit Problemen endet.

Verwenden Sie niemals eine Zahlungsmethode, die keinen Käuferschutz bietet. Von Überweisungen und Zahlungsanweisungen wird abgeraten, da Sie nach dem Versand keine Möglichkeit haben, das Geld zurückzuerhalten. Dies ist einer der Gründe, warum Betrüger diese Zahlungsmethoden bevorzugen.

Wählen Sie immer Kreditkartenzahlung oder renommierte Zahlungsseiten wie PayPal. In diesem Fall sind Sie besser geschützt, falls es ein Problem mit Ihrer Transaktion geben sollte. Achten Sie darauf, dass Sie sich bei der richtigen Website anmelden. Websites mit Zahlungsfunktionen stehen bei Cyberkriminellen besonders hoch im Kurs.

Bei mobilen Geräten gibt es andere Zahlungsmöglichkeiten, zum Beispiel Google Wallet, NFC oder sogar SMS. Doch wie die anderen Zahlungsarten sind auch diese mit Risiken behaftet. Grundlegende Sicherheitsmaßnahmen wie die Installation einer Sicherheitssoftware und die Verwendung der Sperrfunktion Ihres Gerätes schützen Ihre Transaktionen.

Achten Sie auf eine sichere Umgebung

Auch beim entspannten Einkaufen im Internet sind Sie nicht allein. Externe Faktoren können immense Auswirkungen auf die Sicherheit Ihres Einkaufs haben. Auch wenn Sie nur auf rechtmäßigen Websites einkaufen, kann ein infizierter Computer erheblichen Schaden anrichten.

Daher müssen Sie jeden Teil Ihrer digitalen Welt absichern:

- **Schützen Sie Ihre Geräte**. Installieren Sie eine Sicherheitslösung, die Ihre Geräte vor den verschiedensten Bedrohungen schützt. Sperren Sie Ihre Geräte, damit Unbefugte keinen Zugriff auf Ihre Konten erhalten. Sie können auch eine „Gerätefinder"-Software mit Sperrfunktion und Datenlöschung per Fernzugriff installieren, für den Fall, dass Ihr Gerät verloren geht oder gestohlen wird.
- **Verwenden Sie komplexe Kennwörter**. Beim Einrichten von Kennwörtern sollten Komplexität und Länge wichtige Kriterien sein. Sie können auch ein Tool zur Kennwortverwaltung verwenden. Bedenken Sie, dass mehrere Online-Konten sehr verwaltungsintensiv sind.
- **Lesen Sie das Kleingedruckte**. Wenn Sie sich über alle Bedingungen informieren, sind Sie besser vor Betrugsversuchen und unseriösen Händlern geschützt.

TREND MICRO HAFTUNGSAUSSCHLUSS

Die in diesem Dokument bereitgestellten Informationen sind lediglich allgemeiner Natur und für Aufklärungszwecke gedacht. Sie stellen keine Rechtsberatung dar und sind nicht als solche auszulegen. Die in diesem Dokument bereitgestellten Informationen finden womöglich nicht auf alle Sachverhalte Anwendung und spiegeln womöglich nicht die jüngsten Sachverhalte wider. Die Inhalte in diesem Dokument sind ohne eine Rechtsberatung auf der Grundlage der vorgestellten besonderen Fakten und Umstände nicht als verlässlich oder als Handlungsanweisungen zu verstehen und nicht in anderer Weise auszulegen. Trend Micro behält sich das Recht vor, die Inhalte dieses Dokuments zu jeder Zeit und ohne Vorankündigung zu ändern.

Übersetzungen in andere Sprachen sind ausschließlich als Unterstützung gedacht. Die Genauigkeit der Übersetzung wird weder garantiert noch stillschweigend zugesichert. Bei Fragen zur Genauigkeit einer Übersetzung lesen Sie bitte in der offiziellen Fassung des Dokuments in der Ursprungssprache nach. Diskrepanzen oder Abweichungen in der übersetzten Fassung sind nicht bindend und haben im Hinblick auf Compliance oder Durchsetzung keine Rechtswirkung.

Trend Micro bemüht sich in diesem Dokument im angemessenen Umfang um die Bereitstellung genauer und aktueller Informationen, übernimmt jedoch hinsichtlich Genauigkeit, Aktualität und Vollständigkeit keine Haftung und macht diesbezüglich keine Zusicherungen. Sie erklären Ihr Einverständnis, dass Sie dieses Dokument und seine Inhalte auf eigene Gefahr nutzen und sich darauf berufen. Trend Micro übernimmt keine Gewährleistung, weder ausdrücklich noch stillschweigend. Weder Trend Micro noch Dritte, die an der Konzeption, Erstellung oder Bereitstellung dieses Dokuments beteiligt waren, haften für Folgeschäden oder Verluste, insbesondere direkte, indirekte, besondere oder Nebenschäden, entgangenen Gewinn oder besondere Schäden, die sich aus dem Zugriff auf, der Verwendung oder Unmöglichkeit der Verwendung oder in Zusammenhang mit der Verwendung dieses Dokuments oder aus Fehlern und Auslassungen im Inhalt ergeben. Die Verwendung dieser Informationen stellt die Zustimmung zur Nutzung in der vorliegenden Form dar.

Als weltweit führender Anbieter im Bereich Sicherheit hat Trend Micro Incorporated das Ziel, eine sichere Welt für den Datenaustausch zu schaffen. Weitere Informationen erhalten Sie unter www.trendmicro.com.

TREND MICRO™

Enjoy your digital life safely

Created by:
TrendLabs, The Global Technical Support & R&D Center of TREND MICRO