5 typische Risiken beim Online-Shopping

26. Juli 2021

[News](https://www.usd.de/category/news/) | [Cyber Defence](https://www.usd.de/category/cyber-defence/) | [Cybersecurity Tips](https://www.usd.de/category/cybersecurity-tips/)

Schnell, einfach, rund um die Uhr und von überall auf der Welt - Online Shopping erfreut sich bereits seit vielen Jahren immer größer werdender Beliebtheit und ist heute kaum mehr aus unserem Kaufverhalten wegzudenken. Doch mit steigender Popularität wachsen auch die Risiken. So rücken [Online Shops immer mehr in das Visier krimineller Hacker](https://www.usd.de/news-online-shops-im-visier-krimineller-hacker/) und gefährden Ihr sicheres Einkaufen.

Hier sind 5 typische Risiken beim Online-Shopping, die Sie im Hinterkopf haben sollten, um sich gegen potentielle Angriffe von Hackern und Cyberkriminellen zu schützen:

Identitätsdiebstahl

Auch wenn es vielen Menschen nicht bewusst ist, gehört der Diebstahl Ihrer Identität zu den größten Sicherheitsrisiken[[1]](#footnote-1) beim Online-Shopping. Cyberkriminelle versuchen, durch verschiedene Vorgehen möglichst viele persönliche Daten[[2]](#footnote-2) von Ihnen zu stehlen.  Sobald sie das geschafft haben und Ihre Daten erfasst wurden, können diese entweder weiterverkauft[[3]](#footnote-3) oder für Einkäufe, Vertragsabschlüsse und andere kriminellen Aktivitäten missbraucht werden.

Fake-Shops

Das Internet ist voller falscher Online Shops und die Anonymität im Internet macht es für Cyberkriminelle noch einfacher, Menschen in ihre Falle zu locken. Mit unschlagbaren Angeboten und Internetseite, die den originalen Shops zum Verwechseln ähnlich[[4]](#footnote-4) sehen, werden Käufer dazu verleitet, Geld in nichtexistierende Ware zu investieren oder sensible Daten preiszugeben. So kann die Person, die hinter dem Betrug steckt, alle Daten, die Sie eingeben, protokollieren und Ihre persönlichen Informationen stehlen. Um das Risiko zu minimieren und zu prüfen[[5]](#footnote-5), ob der Shop vertrauenswürdig ist, hilft oft schon ein Blick in das Impressum. Dort sollte mindestens der Unternehmensname plus Anschrift aufgeführt sein.

Phishing

Mit Phishing ist das „Angeln“ nach Informationen gemeint. So werden potenziellen Opfern oft E-Mails mit manipulierten Anhängen oder Links geschickt, die die Käufer zur Eingabe persönlicher Daten bringen sollen. Die meisten Links führen[[6]](#footnote-6) entweder auf eine mit Malware infizierte Seite oder auf gefälschte Webseiten von bekannten Online-Shops, Banken oder Behörden. Durch die Eingabe von Zugangs- oder Bankdaten, können diese gestohlen werden und Ihnen erheblicher finanzieller aber auch persönlicher Schaden entstehen.

Adware und Malware

Wer kennt es nicht? Während[[7]](#footnote-7) man in Online Shops surft, überschütten[[8]](#footnote-8) Anzeigen[[9]](#footnote-9) und Angebote die Bildschirme. Doch nicht immer sind diese Angebote echt oder seriös. So kann es sein, dass sobald auf die Anzeige geklickt wurde, man dazu aufgefordert wird, sensible Daten zu teilen oder das Gerät augenblickblich mit einer Malware infiziert wird. Drücken Sie also möglichst nicht auf Pop-up-Werbung und bedenken Sie, dass auch ein Klick auf das „X“ Ihr Gerät infizieren kann.

Unverschlüsselte Daten und unsichere Zahlungsmethoden

Es gibt viele Möglichkeiten, online für seinen Einkauf zu bezahlen, doch es ist Vorsicht geboten. So ist das Zahlen per Lastschrift, bei dem der Käufer dem Verkäufer seine Kontodaten[[10]](#footnote-10) übermittelt und ihn zur Abbuchung des Betrags ermächtigt, zwar bequem, ermöglicht aber gleichzeitig das Ausspähen von Kontodaten, wenn die Übertragung nicht verschlüsselt ist. Hier sollte vor dem Kauf immer darauf geachtet werden, dass die Webseite SSL-Verschlüsselungen[[11]](#footnote-11) verwendet. Erkennen lässt sich das an der URL, die mit „https“ statt „http“ beginnt. Auch bei der Zahlung mit Kreditkarte lassen sich Daten missbrauchen und es sollte auf eine verschlüsselte Übertragung geachtet werden.

Frage 1: Wat proberen criminelen te doen als ze je persoonlijke gegevens gestolen hebben?

Frage 2: Hoe kan men controleren of een website betrouwbaar is.

Frage 3: Waar leiden Phishing mails je naar toe?

Frage 4: Wat wordt volgens de tekst afgeraden om te doen bij pop ups op het scherm? Noem twee punten!

Frage 5: Wat moet je volgens de tekst controleren om te zien of de website SSL versleuteld is?

1. veiligheidsrisico [↑](#footnote-ref-1)
2. gegevens [↑](#footnote-ref-2)
3. doorverkopen [↑](#footnote-ref-3)
4. lijkend [↑](#footnote-ref-4)
5. testen [↑](#footnote-ref-5)
6. leiden [↑](#footnote-ref-6)
7. terwijl [↑](#footnote-ref-7)
8. bedelven [↑](#footnote-ref-8)
9. advertenties [↑](#footnote-ref-9)
10. bankgegevens [↑](#footnote-ref-10)
11. Versleuteling [↑](#footnote-ref-11)