

# SOS-Karte

## Schutz beim Online-Shopping



**Online einzukaufen ist bequem und beliebt. Produkte lassen sich schnell bestellen und direkt nach Hause liefern. Doch beim Einkauf im Internet ist auch Vorsicht geboten, denn Betrüger nutzen immer wieder die Möglichkeiten des digitalen Handels aus.**

### **Online bestellt, aber die Ware nicht erhalten.**

- ☐ Versuchen Sie herauszufinden, wo die Ware ist – beispielsweise mit Hilfe einer Sendungsnummer.
- ☐ Prüfen Sie Ihre Kreditkarten- und Kontoumsätze auf Abbuchungen.
- ☐ Sie haben den Verdacht, es handle sich um einen Fakeshop? Kontaktieren Sie umgehend Ihre Bank und lassen Sie prüfen, ob sich die Zahlung noch stoppen lässt.
- ☐ Besteht der Verdacht des Betruges? Erstellen Sie Strafanzeige bei der Polizei. Sichern Sie E-Mails mit vermeintlichen Bestellbestätigungen und Screenshots vom Fakeshop als Beweismittel.

### **Fremde Person bestellt über Ihren Onlineshop-Account Waren.**

- ☐ Informieren Sie den Anbieter des Onlineshops über den Vorfall.
- ☐ Kontaktieren Sie umgehend Ihre Bank und lassen Sie ggf. Ihre Kreditkarten sperren. Prüfen Sie, ob Sie bereits bezahlte Beträge zurückbuchen lassen können.
- ☐ Ändern Sie umgehend Ihr Passwort für den Shop-Account sowie Ihr E-Mail-Konto. Ändern Sie ggf. Passwörter anderer Online-Accounts. Nutzen Sie dasselbe Passwort nie für mehrere Accounts!
- ☐ Erstellen Sie Strafanzeige bei der Polizei. Sichern Sie Kontoumsätze und E-Mails als mögliche Beweismittel.

**da, wenn's zählt.**

**Sparda-Bank**

# Schutzmaßnahmen für zukünftiges Online-Shopping:

## Achten Sie auf die Anzeichen eines Fakeshops:

- ☐ Der Name der Internetadresse passt nicht zu den angebotenen Produkten – beispielsweise werden Schuhe auf blumenkaufen.de.com angeboten.
- ☐ In der Adressleiste findet sich kein Schlosssymbol und Zahlungen sind nur per Vorkasse möglich.
- ☐ Die Preise sind ungewöhnlich günstig.
- ☐ Beim Bestellprozess werden mehrere Zahlungsarten angeboten, der Kaufabschluss ist dann allerdings nur noch gegen Vorkasse möglich.
- ☐ Gütesiegel lassen sich nicht anklicken und führen nicht zum Zertifikat des Siegel- Ausstellers.
- ☐ Es gibt nur positive Kundenbewertungen – und die lesen sich zum Teil wie schlechte Übersetzungen.
- ☐ Auf der Seite finden sich weder Allgemeinen Geschäftsbedingungen noch Impressum.

## Schützen Sie Ihren Onlineshop-Account vor unbefugten Zugriffen:

- ☐ Je sensibler ein Zugang ist, desto mehr Sorgfalt erfordert ein starkes Passwort.
- ☐ Nutzen Sie ein individuelles Passwort pro Account.
- ☐ Falls es keine Zeichenbegrenzung für das Passwort gibt, gilt: Je länger, desto besser!
- ☐ Als sicher gilt ein Passwort aus zwei Zeichenarten mit 20 bis 25 Zeichen.
- ☐ Ein kürzeres Passwort muss komplexer sein: Kombinieren Sie Klein- und Großbuchstaben, Zahlen und Sonderzeichen. Vermeiden Sie Muster (z.B. qwertz) oder Reihen (z.B. 12345).
- ☐ Aktivieren Sie, wenn möglich, die Zwei-Faktor-Authentisierung.

## Berücksichtigen Sie außerdem diese Tipps:

- ☐ Unbekannte Shops mit dem Fakeshop-Finder der Verbraucherzentrale prüfen.
- ☐ Achten Sie darauf, sich wirklich auf der offiziellen Webseite des Shops anzumelden, da gefälschte Seiten häufig täuschend echt aussehen und nur dazu dienen, Passwörter oder Zahlungsdaten abzugreifen.
- ☐ Wählen Sie möglichst die Zahlungsoptionen „Auf Rechnung“ oder „Lastschrift“, da sich Überweisungen meist nicht zurückrufen lassen.
- ☐ Seien Sie sparsam mit Ihren Daten. Speichern Sie möglichst keine Zahlungsdaten in Ihrem Account.
- ☐ Tätigen Sie keine Käufe über ein öffentliches, unverschlüsseltes WLAN.
- ☐ Kundenbewertungen auch über andere Seiten recherchieren, insbesondere wenn auf der Shopseite nur positive Bewertungen sind.

**Sparda-Bank West eG**

Ludwig-Erhard-Allee 15, 40227 Düsseldorf, Telefon: 0211 23 93 23 88

**sparda-west.de**

**da, wenn's zählt.**

**Sparda-Bank**