verbraucherzentrale
Hamburg

Smishing: Achtung, gefährliche Paket-SMS können teuer werden!

Ein Geburtstagsgeschenk hier, ein paar neue Schuhe dort und zwischendurch andere Dinge des täglichen Bedarfs – vieles bestellen wir schnell online im Internet. Doch Betrüger nutzen das gezielt aus. Besonders gefährlich: Paket-SMS. Hüten Sie sich vor Smishing!

DAS WICHTIGSTE IN KÜRZE

1. Verbraucherinnen und Verbraucher werden mit gefälschten Paket-SMS aufgefordert, per Link eine Lieferung zu bestätigen.

2. Mit Klick auf den Link wird eine Schadsoftware installiert, die im Sekundentakt SMS verschickt, was teilweise zu Telefonkosten von mehreren hundert Euro führen kann. Bei vorherigen Betrugswellen mit Paket-Nachrichten wurden vor allem persönliche Daten für Kontoabbuchungen und Abofallen abgegriffen.
3. Die Verbraucherzentrale rät, Sendungsverfolgungen von Paketdienstleistern oder anderen Unternehmen stets kritisch zu prüfen und insbesondere dann misstrauisch zu sein, wenn Links angeklickt werden müssen oder zur Zahlung offener Geldbeträge aufgefordert wird.
4. **Kostenloser Vortrag in Hamburg: „Abzocke im Alter - So schützen Sie sich vor Betrug“** Jetzt anmelden

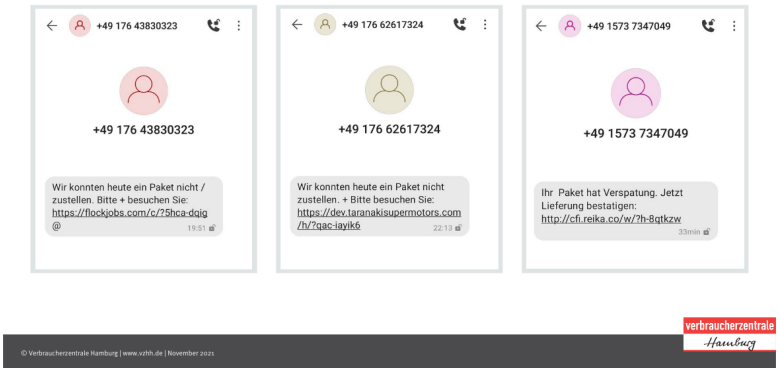
Stand: 27.01.2025

Immer mehr Menschen bestellen Waren online. Betrüger machen sich diesen Umstand zunutze. Uns erreichen immer wieder Anfragen von Ratsuchenden, die angeblich per SMS Informationen zu einer Lieferung erhalten haben. Doch die vermeintliche Paketzustellung ist nur Mittel zum Zweck, um persönliche Daten zu klauen oder das Telefon zu übernehmen. Manche Opfer eines solchen Smishing-Angriffs haben Rechnungen von bis zu 700 Euro für automatisch verschickte SMS erhalten. Doch das muss man nicht hinnehmen!

So funktioniert die SMS-Betrugsmasche

„Wir konnten heute ein Paket nicht zustellen. Bitte besuchen Sie...“ oder *„Ihr Paket hat Verspätung. Jetzt Lieferung bestätigen...“* lauten die Texte der Mitteilungen, denen ein Link folgt. Klickt man darauf, wird eine Schadsoftware auf dem Smartphone installiert, die SMS im Sekundentakt verschickt.

Ohne SMS-Flatrate kann das teuer werden! Zwar sperren die Mobilfunkanbieter zeitnah die SIM-Karten, doch für alle bis zu diesem Zeitpunkt verschickten SMS werden teilweise Entgelte von mehreren hundert Euro berechnet. Manche Telefonunternehmen beharren auf Zahlung von mindestens 100 Euro oder sogar mehr.



© Verbraucherzentrale Hamburg

So wehren Sie sich gegen unrechtmäßige Forderungen

Einzelverbindungsnachweis anfordern: Haben Sie aufgrund eines Smishing-Angriffs eine hohe Rechnung von Ihrem Mobilfunkanbieter erhalten, sollten Sie diese nicht einfach begleichen, sondern sich wehren. Schließlich wurden die SMS nicht von Ihnen, sondern von der Schadsoftware verschickt. Mit einem Einzelverbindungsnachweis, den Sie bei Ihrem Anbieter anfordern können, lässt sich belegen, dass das Versenden der SMS automatisch im Sekundentakt erfolgte.

Wollen Mobilfunkunternehmen die Gebühren der verschickten SMS als Schadensersatz geltend machen, müssen Sie schuldhaft gehandelt haben und der Anbieter muss den entstandenen Schaden nachweisen. Die Berechnung des Schadens kann sich angesichts zahlreicher Flatrate-Modelle am Markt jedoch nicht an dem vereinbarten Entgelt pro SMS (in der Regel zwischen 0,09 und 0,19 Euro) bemessen, meinen wir.

Forderung bestreiten: Mit unserem kostenlosen Musterbrief können Sie Ihren Mobilfunkanbieter informieren, dass die Kosten nicht rechtmäßig sind.

Rechtliche Beratung: Vereinbaren Sie bei Bedarf einen Termin mit unseren Juristinnen und Juristen, um weitere Schritte zu besprechen.

UNSER RAT

Sollten Sie den Link angeklickt haben und Schadsoftware auf Ihr Gerät gelangt sein, handeln Sie schnell:

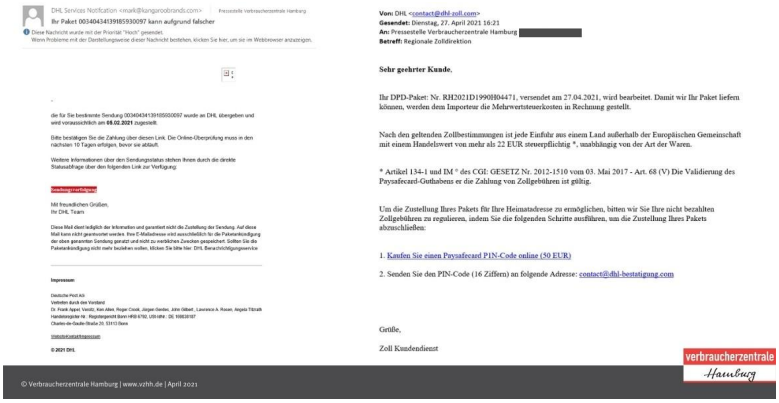
- **Flugmodus aktivieren:** Damit verhindern Sie weitere SMS-Versendungen.
- **Beweise sichern:** Machen Sie Screenshots der SMS und speichern Sie diese.
- **Gerät zurücksetzen:** Setzen Sie Ihr Smartphone auf die Werkeinstellungen zurück, um die Schadsoftware zu entfernen.
- **Polizei informieren:** Erstatten Sie Anzeige bei der Polizei, das ist auch online möglich.
- **Bundesnetzagentur melden:** Unerwünschte SMS können der Bundesnetzagentur gemeldet werden.

Gefälschte Nachrichten von Paketdienstleistern

Neben unspezifischen Paket-SMS werden auch gefälschte Nachrichten im Namen bekannter Paketdienstleister wie DHL oder Hermes verschickt. Diese enthalten oft Texte wie:

„H?llo, wir informieren Sie darüber, da?s Ihr P??????ak?t unser Lager verla??en hat. Leider sind wir ni?ht in d?r Lage, Ihre Li?ferung innerhalb des voraussichtlichen Z?itraums abzus?hließen, da uns ein? fal?ch? Adr?s?e vorliegt. Bitte korrigieren Si? Ihre Adr?ss?.“

Wer auf den Link in einer solchen Meldung klickt, landet auf einer gefälschten Internetseite, die der des echten Paketdienstleisters nachempfunden ist. Dort wird man dann zum Beispiel aufgefordert, einen Geldbetrag zu bezahlen, weil die Adresse auf dem Paket nicht stimmt oder Zollgebühren fällig werden. Die Kosten können sich schnell auf mehrere hundert oder gar tausend Euro aufsummieren.

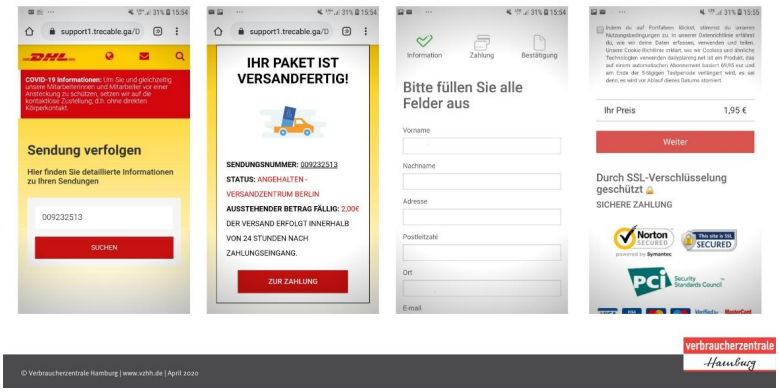


Auch die Verbraucherzentrale erhält Nachrichten, wonach sie angeblich wegen einer falschen Adresse oder Zollgebühren Geld überweisen soll.

© Verbraucherzentrale Hamburg

In der Vergangenheit waren die SMS auch mit Identitätsdiebstahl und Datenklau verbunden. Wer seine persönlichen Daten in die vorgegebenen Formularfelder der Website einträgt und an die Betrüger übermittelt, muss damit rechnen, dass Fremde sie nutzen. Im schlimmsten Fall wird Geld vom Konto abgebucht, oder es landen Wochen später Rechnungen und Inkassoforderungen in Ihrem Briefkasten.

Sind Sie versehentlich in eine solche (Abo)Falle getappt, bewahren Sie Ruhe. Haben Sie Ihre Kreditkartendaten angegeben, setzen Sie sich mit Ihrem Kreditkarteninstitut in Verbindung und stoppen Sie die Abbuchungen. Erhalten Sie Mahnbriefe, lassen Sie sich nicht einschüchtern. Erklären Sie schriftlich per Einwurf-Einschreiben, dass Sie keinen Vertrag geschlossen haben und widersprechen Sie der Forderung.



Screenshots einer gefälschten DHL-Website mit Formularen fürs Abgreifen persönlicher Daten und Häkchenfeld für eine Abofalle

UNSERE TIPPS

- Überlegen Sie, ob Sie wirklich ein Paket bestellt haben und eine Sendung erwarten. Haben Sie dafür tatsächlich eine Benachrichtigung per SMS eingestellt?
- Prüfen Sie den Absender der SMS. Seriöse Paketdienstleister nennen den eigenen Namen immer in der Adresse. DHL beispielsweise operiert über „dhl.de", Hermes nutzt „myhermes.de", UPS finden Sie unter „ups.com", GLS ist mit „gls-pakete.de" im Netz

vertreten und Sendungen vom DPD können Sie unter „dpd.com" nachverfolgen.

- Öffnen Sie keine Links von verdächtigen Absendern. URL-Adressen mit Schreibfehlern oder unbekannten Domains sind ein klares Warnsignal.
- Werden Sie vorab zur Zahlung aufgefordert, löschen Sie die Nachricht. Paketdienstleister fordern grundsätzlich nicht dazu auf, Waren im Vorfeld zu bezahlen.
- Melden Sie die verdächtigen SMS oder Mails dem Kundenservice des Paket-Dienstleister und der Bundesnetzagentur.

Gefördert durch:

Bundesministerium
für Umwelt, Naturschutz, nukleare Sicherheit
und Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

https://www.vzhh.de/themen/telefon-internet/phishing-mails-spam/smishing-achtung-gefaehrliche-paket-sms-koennen-teuer-werden