



# Fake Shops im Internet

Dunkelfeldstudie zu Betrugsdelikten in  
Zusammenhang mit Einkaufen im Internet

Wien, Jänner 2021

# Fake Shops im Internet

## Dunkelfeldstudie zu Betrugsdelikten in Zusammenhang mit Einkaufen im Internet

### **Autor**

Stefan Georgiev MA

### **Fachliche Verantwortung**

Dr. Georg Plattner

### **Auftraggeber**

Dr. Armin Kaltenegger

### **Gender-Hinweis**

Zugunsten besserer Lesbarkeit findet entweder die männliche oder weibliche Form personenbezogener Begriffe Verwendung. Dies impliziert keinesfalls eine Benachteiligung des jeweils anderen Geschlechts. Gemeint und angesprochen sind alle Geschlechter.

# Inhaltsverzeichnis

<b>1. Einleitung</b>	<b>4</b>
1.1. Problemlage	4
1.2. Betrug im Internet	4
1.3. Fake Shops	5
1.4. Rechtliches	6
<b>2. Studiendesign</b>	<b>7</b>
2.1. Dunkelfeldforschung	7
2.2. KFV-Studie „Betrug im Internet“	7
<b>3. Ergebnisse</b>	<b>9</b>
3.1. Basisangaben	9
3.2. Betroffenheit	9
3.3. Finanzieller Schaden	10
3.4. Sicherheitsvorkehrungen	11
3.5. Konsequenzen	12
3.6. Risikogruppen	13
<b>4. Conclusio</b>	<b>16</b>
4.1. Zusammenfassung der Ergebnisse	16
4.2. Empfehlungen des KFV	17

# 1. Einleitung

## 1.1. Problemlage

Online-Shopping bietet, neben der Bequemlichkeit, direkt von zu Hause aus einzukaufen, viele weitere Vorteile. Die vielfältigen und günstigen Angebote locken an, und das stundenlange Stöbern nach Schnäppchen wird für viele zum Unterhaltungsprogramm. Besonders ausgeprägt sind diese Merkmale in Zeiten der Covid-Pandemie, da aufgrund der Ausgangsbeschränkungen, der teilweisen Schließung des Handels sowie der Nichtverfügbarkeit bestimmter Produkte im Einzelhandel eine große Nachfrage (z.B. an Schutz- und Haushaltsartikeln) entstanden ist. Eine Studie aus dem Jahr 2019, durchgeführt von RegioData Research, zeigt, dass über 13 % des österreichischen Einzelhandelsumsatzes bereits in den Onlinehandel fließen, mit steigender Tendenz. Davon wiederum fließen 64 % ins Ausland. (Regiodata Research GmbH Österreich, 2019)

Neben dem regulären, legalen Online-Handel existieren jedoch auch in immer größerer Zahl gefälschte Internet-Verkaufsplattformen, die ihre Opfer durch unseriöse Angebote ködern. Diese Fake Shops sehen oft täuschend echt aus und sind daher auf den ersten Blick nur sehr schwer zu erkennen. Immer mehr Konsumenten werden Opfer dieser Form von Internet-Betrug, und die Durchsetzung von Konsumentenrechten ist schwierig bis unmöglich. Der beste Schutz davor ist erhöhte Achtsamkeit.

Das tatsächliche Ausmaß von Betrug durch Fake Shops ist allerdings unbekannt, da die Dunkelziffer in diesem Kriminalitätsbereich sehr hoch ist. Betrugsfälle im Internet scheinen meist nicht in der Kriminalstatistik auf, weil sie schlicht und einfach nicht gemeldet werden. Die Gründe dafür können unterschiedlich sein: Scham wegen der eigenen fahrlässigen Handlung, fehlendes Bewusstsein oder zu geringer Schaden, der weitere rechtliche Schritte aus Sicht der Betroffenen nicht rechtfertigt.

Um Licht in dieses Dunkelfeld zu werfen, hat das KfV gemeinsam mit dem Bundeskriminalamt und dem IFES Forschungsinstitut eine Studie entwickelt und durchgeführt, um die bislang unbekanntes Zahlen zu Betrugsdelikten in Zusammenhang mit Einkaufen im Internet zu erheben.

## 1.2. Betrug im Internet

Allgemein existiert eine Vielzahl verschiedener Formen des Betrugs im Internet, von Phishing-Mails, die versuchen, vertrauliche Daten zu erbeuten, über gefälschte Gewinnversprechen und irreführende Gratis-Angebote bis hin zu Identitätsdiebstahl und Social Engineering. Neben diesen illegalen Handlungen ist der Online-Betrug eine der am weitesten verbreiteten Formen der Internetkriminalität.

Laut Martin Schallbruch, stellvertretendem Direktor des Digital Society Instituts der ESMT Berlin und ehemaligem Abteilungsleiter für Informationstechnik im deutschen Bundesministerium des Innern, liegt der Kern der Problematik des Internet-Betrugs „an der Mühsal einer verlässlichen Identifizierung im Netz und an den genau damit zusammenhängenden Vollzugsdefiziten des

Staates.“ (Schallbruch, 2018). Yaman Akdeniz, Professor für Recht an der Bilgi-Universität Istanbul, beschreibt Anonymität im Internet als einen der größten Vorteile einerseits, der allerdings für Nutzer und Staat auch einige der größten Hürden darstellt (Akdeniz, 2002). Diese Anonymität erleichtert den Betrug im Internet massiv, da die Nachverfolgung des Übeltäters erschwert wird und oft mit ungerechtfertigtem Aufwand verbunden wäre.

Laut der polizeilichen Kriminalstatistik des österreichischen Bundeskriminalamts ist der gesamte Internet-Betrug im Jahr 2019 mit 16.831 Anzeigen um ca. 26 % angestiegen (im Vergleich zu 2018 mit 13.328 Anzeigen), wobei die Aufklärungsquote recht niedrig bei 37,9 % liegt. Im Jahr 2010 wurden nur 3.229 Anzeigen erstattet. Das ergibt einen Anstieg von über 420 % in den letzten 10 Jahren. (BMI/BK, 2020)

	2018	2019	Veränderung absolut	Veränderung relativ
Bestell-/Warenbetrug	9.379	10.473	1.094	+ 11,7 %
Sonstiger Betrug	103	707	604	+ 590,2 %
Trickbetrug	442	917	475	+ 107,5 %
Betrug mit unbaren Zahlungsmitteln	747	1.140	393	+ 52,6 %
Vorauszahlungsbetrug	1.245	1.522	277	+ 22,2 %
Kontoeröffnungs-/ Überweisungsbetrug	697	927	230	+ 33,0 %
Dienstleistungs-/Zechbetrug	0	224	224	
Darlehens-/Kreditbetrug	171	292	121	+ 70,8 %
Anlagebetrug	169	285	116	+ 68,6 %
Urkunden-/Beweismittelbetrug	11	27	16	+ 145,5 %
Versicherungsbetrug	2	3	1	+ 50,0 %

*Tabelle 1: Internet-Betrug - 2019 - Österreich - Anzahl der Straftaten; Quelle BMI, eigene Darstellung*

### 1.3. Fake Shops

Fake Shops sind gefälschte Verkaufsplattformen, die ihre Opfer durch günstige Angebote locken, eine Vorauszahlung bei der Bestellung verlangen und keine oder gefälschte Ware liefern. Das Angebot solcher Fake Shops ist sehr vielfältig und umfasst u.a. Möbel, Werkzeug, Spielzeug, Softwareprodukte, Veranstaltungstickets und vieles mehr. (Watchlist Internet, 2020)

Eine Studie des Amtes der Europäischen Union für geistiges Eigentum (EUIPO) zum Ausmaß der Fake Shops in der EU zeigt, dass zwischen Dezember 2016 und Jänner 2017, in einem Zeitraum von nur zwei Monaten, 27.000 Online-Shops, die mutmaßlich markenrechtsverletzende Ware vertreiben, in mehreren europäischen Ländern aktiv waren. (Hildebrandt & Kolf, 2017) In

Deutschland schätzen Polizeibehörden die jährliche Zahl der Opfer auf mehr als 700.000. Für Österreich existieren hierzu bislang keine Studien oder Statistiken.

Im Jahr 2020 sorgte der Ausbruch der globalen Corona-Pandemie für enorme Umwälzungen im täglichen Leben. Durch Ausgangsbeschränkungen und Sperre des Handels hat auch der Online-Handel einen deutlichen Zuwachs erlebt, der über sein normales Wachstum weit hinausgeht. Kriminelle haben schnell gelernt, die Unsicherheit der Menschen sowie die Knappheit bzw. Nicht-Verfügbarkeit von bestimmten Hygiene- und Haushaltsartikeln auszunutzen und schnell Profit aus der Not und Unsicherheit der Menschen zu machen. Besonders Betreiber von Fake Shops sind auf dieses Thema aufgesprungen. (Internet Ombudsmann, 2020)

## 1.4. Rechtliches

Betrugsformen im Internet sind im Strafgesetzbuch (StGB) durch die Delikte der §§ 146 ff (Betrug, insbesondere Betrügerischer Datenverarbeitungsmissbrauch) sowie bspw. § 118a (Widerrechtlicher Zugriff auf ein Computersystem), § 119a (Missbräuchliches Abfangen von Daten) oder § 126a bis 126c (Datenbeschädigung, Störung der Funktionsfähigkeit eines Computersystems, Missbrauch von Computerprogrammen oder Zugangsdaten) geregelt und strafbar.

Generell sollten beim Einkauf in Online-Shops folgende Kriterien beachtet werden:

- Sind allfällige Gütesiegel vorhanden?
- Sind AGB, Produktbeschreibungen, Lieferzeiten leicht abrufbar?
- Achtung bei Zahlungsmöglichkeiten: Sichere Zahlungsvarianten wählen – Zahlungen im Voraus mittels Banküberweisung sollten vermieden werden.
- Ist der Verkäufer durch Firmennamen, Anschrift, Telefonnummer, E-Mail-Adresse, Nennung einer Kontaktperson und Firmenbuchnummer zu identifizieren? Findet sich auf der Webseite ein (für Online-Shops verpflichtendes) Impressum?
- Werden Bestellungen per E-Mail bestätigt?

## 2. Studiendesign

### 2.1. Dunkelfeldforschung

*„Der Schwerpunkt der kriminalpolizeilichen Arbeit liegt neben den klassischen Ermittlungsmethoden auf nationaler und internationaler Ebene auch in der Präventionsarbeit mit der Privatwirtschaft, Nichtregierungsorganisationen und Vereinen.“ (BMI/BK, 2020)*

Bereits in den Anfängen der kriminologischen Forschung wurde erkannt, dass es neben den von der Polizei erfassten Fällen eine andere „Kriminalitätswirklichkeit“ gibt. (Köllisch, 2004) Ein wesentlicher Punkt für die Verbesserung der Präventionsarbeit im Bereich Betrug im Internet ist die Erforschung bzw. Informationsgewinnung von bislang den Behörden verborgen gebliebenen Delikten, da sie von den betroffenen Personen nicht angezeigt wurden (das sogenannte „Dunkelfeld“). Eine Verknüpfung der Erhebungsdaten zu Viktimisierungen (sog. „relatives Dunkelfeld“) mit den angezeigten Straftaten aus der amtlichen Kriminalstatistik (sog. „Hellfeld“) ermöglicht die Erstellung eines umfassenden Kriminalitätslagebildes. „Das Ziel von Dunkelfelduntersuchungen ist es, Erkenntnisse über das Gesamtaufkommen bestimmter Straftaten einschließlich des sogenannten (relativen) Dunkelfeldes, also der bei der Polizei nicht bekannten Straftaten, zu gewinnen. Denn während sich die amtliche Kriminalstatistik auf das "Hellfeld" amtlich registrierter Vorgänge – und somit nur auf einen kleinen Ausschnitt von Kriminalität – bezieht, versuchen Dunkelfelduntersuchungen ein umfassenderes Bild von Umfang und Struktur von Kriminalität zu liefern.“ (Bundeskriminalamt Deutschland, 2020)

### 2.2. KFV-Studie „Betrug beim Online-Shopping“

Das KFV hat im Oktober 2020 das Markt- und Meinungsforschungsinstitut IFES mit der Durchführung einer Dunkelfeldstudie zum Thema „Betrug beim Online-Shopping“ beauftragt. Die Befragung, die als Teil der Studie durchgeführt wurde, erforscht die nicht-angewiesenen Fälle und analysiert die Gewohnheiten der Konsumenten im Online-Handel und deren typische Verhaltensfehler.

Um Licht in das Dunkelfeld zu bringen, wurde eine repräsentative Befragung der österreichischen Privatbevölkerung ab 18 Jahren durchgeführt. Im Kern der Studie ging es darum, zu erheben, wie viele Personen (wie häufig) Opfer von Betrug beim Kauf von Gütern und Dienstleistungen im Internet wurden und diese Delikte gemeldet bzw. zur Anzeige gebracht haben.

Wie bei Dunkelfeldstudien üblich, wurden neben der eigenen Opferwerdung (Viktimisierung) auch Beobachtungen im sozialen Umfeld einbezogen, um die zielgruppenspezifische Betroffenheit noch besser einschätzen zu können.

Die Stichprobe wurde disproportional zusammengesetzt, um insbesondere jüngere Personen zu berücksichtigen. Die Disproportionalität ermöglicht es, die Betroffenheit in der primären Zielgruppe statistisch zuverlässiger zu schätzen und detaillierter zu analysieren (z.B. nach Subgruppen in der primär betroffenen Altersgruppe). Homogenere Gruppen können dagegen

auch anhand kleinerer Fallzahlen gut beschrieben werden. Anschließend wurde diese Disproportionalität mittels Gewichtungsverfahren wieder aufgehoben und Repräsentativität hergestellt.

Eckdaten der Studie	
Auftraggeber:	KFV – Kuratorium für Verkehrssicherheit
Durchgeführt durch:	IFES Institut für empirische Sozialforschung GmbH
Thema der Studie:	Betrug beim Online-Shopping
Stichprobe:	1.000 Internetnutzer/-innen ab 18 Jahren
Grundgesamtheit:	Österreicher/innen ab 18 Jahren, die zumindest gelegentlich das Internet nutzen
Methode:	Telefonische Befragung (CATI) & Online-Befragung (CAWI)
Design:	Zufallsauswahl, österreichrepräsentative Stichprobe



## 3. Ergebnisse

### 3.1. Basisangaben

Als Basis für die Studie wurden die „European Social Survey Runde 9“<sup>1</sup> und die „Media Analyse 2019“<sup>2</sup> gewählt. Laut den Erkenntnissen dieser Studien beträgt der Anteil der Online-Nutzer zwischen 18 und 80 Jahre 87 % der Bevölkerung (6 Millionen Personen), wobei die durchschnittliche tägliche Nutzung 2 Stunden beträgt.

Laut der KfV-Studie „CyBar 2020“ sowie der Media Analyse 2019 kaufen zwischen 62 und 67 % der Online-Nutzer in Österreich online ein. Dies entspricht zwischen 4 und 4,4 Millionen Personen. Die durchschnittlichen Ausgaben im Monat betragen 70 Euro. Rund 66 % der Bevölkerung schließen ihre Online-Einkäufe am PC ab, rund 35 % tun das am Smartphone und 41 % am Tablet.

### 3.2. Betroffenheit

**Ein Viertel (25 %) der befragten Online-Nutzer geben an, in ihrem Leben bereits von Internet-Betrug betroffen gewesen zu sein. Das entspräche auf ganz Österreich umgerechnet 1,5 Millionen Menschen.**

Weitere 21 % (dies entspräche 1.260.000 Personen) geben an, in den letzten 5 Jahren betroffen gewesen zu sein, 9 % waren in den letzten 12 Monaten persönlich von Online-Betrug betroffen.

Internet-Betrug	
Gesamt	41 %
Nur Betrug beim Online-Shopping	19 %
Nur andere Formen von Internet-Betrug	16 %
Beides	6 %

*Tabelle 2: Betroffenheit von Internet-Betrug inkl. Betrug beim Online-Shopping und anderen Formen von Internet-Betrug, n=1.002*

Internet-Betrug umfasst unterschiedliche Deliktsformen. Folgende Delikte wurden von jenen Befragten, die in ihrem Leben bereits von Internet-Betrug betroffen waren, am häufigsten angegeben:

<sup>1</sup> [https://www.europeansocialsurvey.org/docs/round9/fieldwork/austria/ESS9\\_fieldwork\\_and\\_interviewer\\_instructions\\_AT.pdf](https://www.europeansocialsurvey.org/docs/round9/fieldwork/austria/ESS9_fieldwork_and_interviewer_instructions_AT.pdf)

<sup>2</sup> <https://media-analyse.at/table/3349>

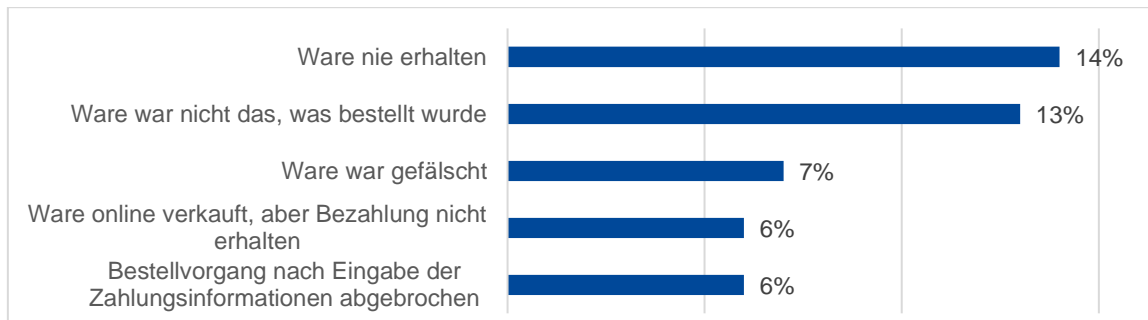


Abbildung 1: Häufigste Betrugsformen in %

Weitere (auch milde) Betrugsformen, die die Befragten angaben, inkludieren Abo-Fallen, das Hacking von Kreditkarte, PayPal, anderen Konten etc., eine Bestellung auf eigenen Namen, von der man nichts wusste, schlechte Produktqualität und nichtvorhandene Reklamationsmöglichkeiten.

### 3.3. Finanzieller Schaden

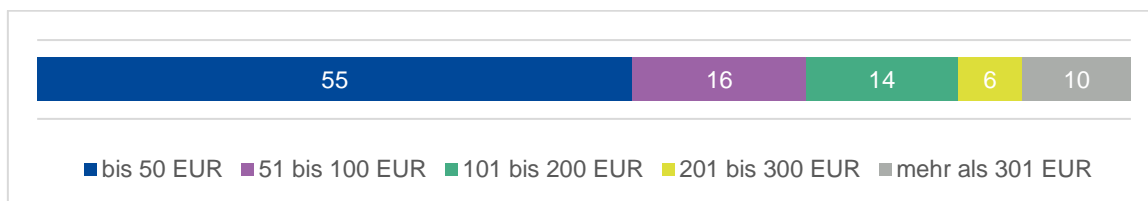


Abbildung 2: Erlittener finanzieller Schaden, Basis: vom Internet-Betrug betroffen, n=250, in %

**Aus der Befragung ist ersichtlich, dass der finanzielle Schaden, den die Befragten erlitten haben, im Durchschnitt 50 Euro beträgt.** 55 % der Befragten geben an, einen Schaden von bis zu 50 Euro erlitten zu haben. Weitere 16 % geben an, dass der erlittene Schaden zwischen 51 und 100 Euro betrug und 16 % geben an, einen Schaden von mehr als 200 Euro erlitten zu haben. **Besonders erwähnenswert ist, dass mehr als die Hälfte jener Personen, die einen hohen Schaden (ab 200 Euro) erlitten haben, tatsächlich Anzeige bei der Polizei erstattet haben.**

#### Fact Box Betroffenheit:

- 25 % der Befragten gaben an, bereits einen Schaden durch Betrug beim Online-Shopping erlitten zu haben.
- Die häufigsten Nennungen waren der Nicht-Erhalt bestellter Ware, falsche Lieferungen, gefälschte Produkte oder auch Betrug beim Online-Verkauf von Waren und Dienstleistungen, die der angebliche Käufer nie bezahlt hat.
- Der finanzielle Schaden betrug durchschnittlich 50 Euro.

### 3.4. Sicherheitsvorkehrungen

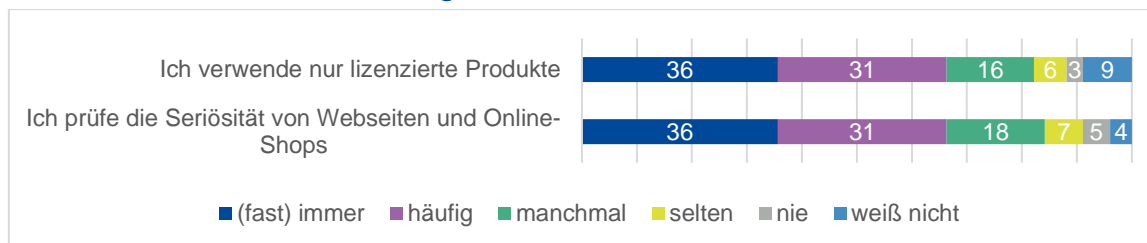


Abbildung 3: Verhalten beim Online-Shopping: Worauf die Nutzer achten, n=1.002

Aus Abbildung 3 ist ersichtlich, dass 67 % der Internet-Nutzer, die online einkaufen, zumindest häufig auf die Seriosität der Online-Shops achten und ein Drittel der befragten Personen diese manchmal bis gar nicht überprüft. Zwei Drittel (67 %) der Befragten geben auch an, häufig bzw. fast immer lizenzierte Produkte zu verwenden.

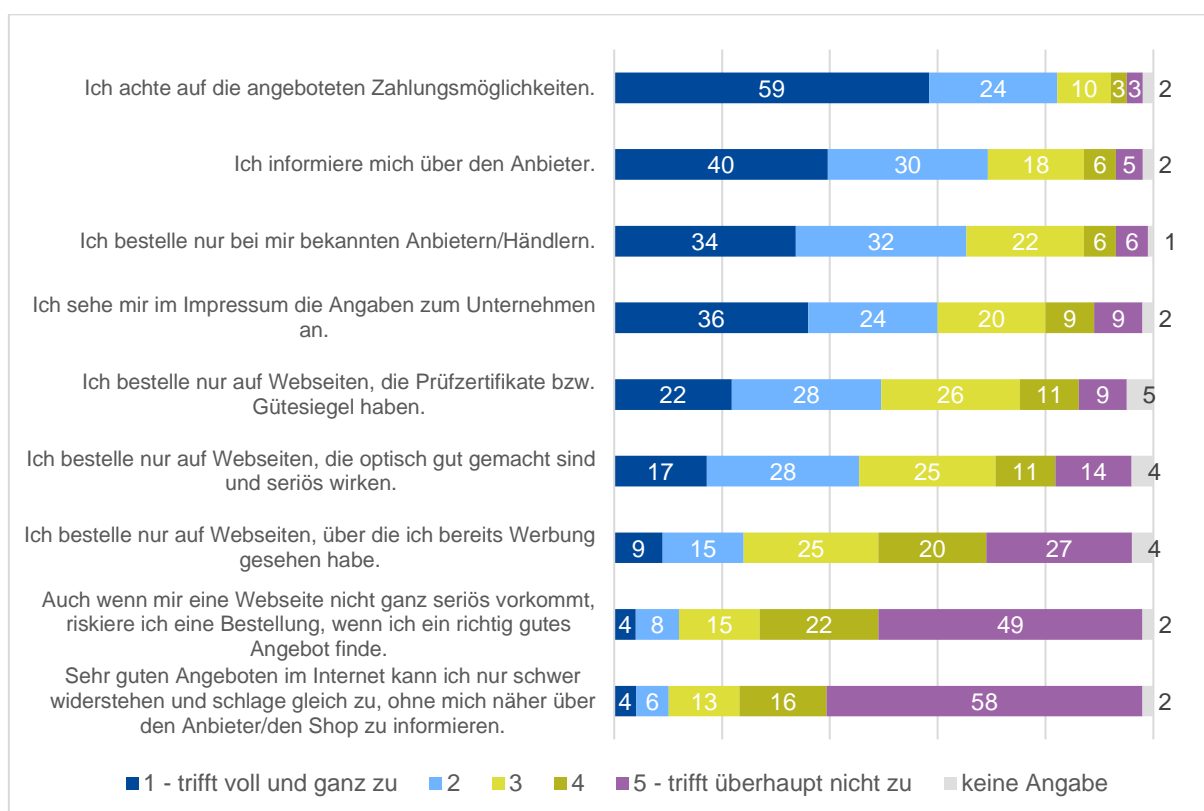


Abbildung 4: Sicherheitsmaßnahmen beim Online-Shopping, Basis: bestellt zumindest selten im Internet, n=938

In Bezug auf die allgemeinen Sicherheitsmaßnahmen und Verhaltensweisen beim Online-Shopping vermeldet **die Mehrheit der zumindest selten online einkaufenden Internetnutzer (83 %)**, auf die **angebotenen Zahlungsmöglichkeiten zu achten**. Weitere 70 % geben an, sich über den Anbieter zu informieren, zwei Drittel (67 %) der Befragten bestellen laut Eigenangabe nur bei **bekanntem Anbietern**. Des Weiteren geben fast zwei Drittel (60 %) der Befragten an, sich

im **Impressum** der Webseite über das jeweilige Unternehmen informiert zu haben, und genau die Hälfte der befragten Personen bestellt laut eigenen Angaben nur bei Webseiten mit **Gütesiegeln und Zertifikaten**

### 3.5. Konsequenzen

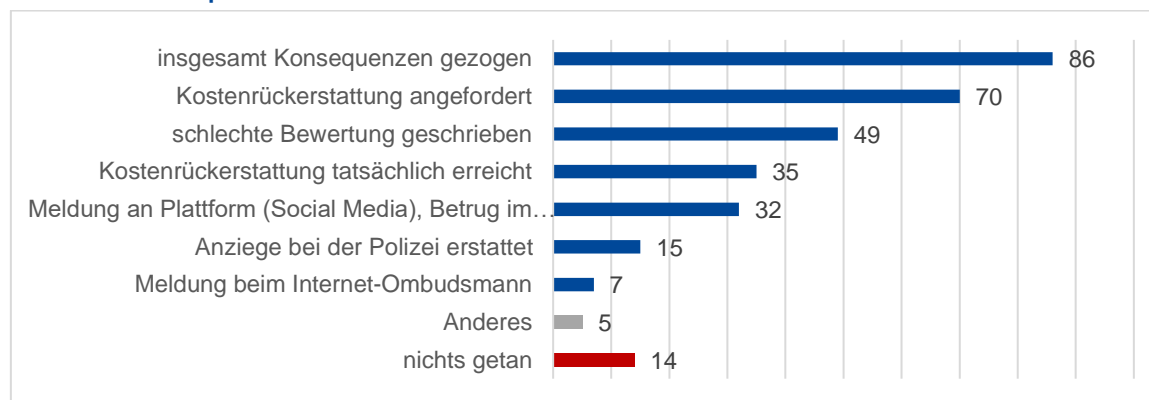


Abbildung 5: Angaben zur Frage "Was haben Sie getan, nachdem der Betrug passiert ist?" in % (mehrfache Nennungen), Basis: von Internet-Betrug betroffen, n=250

Wie aus Abbildung 5 ersichtlich, haben 86 % der Betroffenen tatsächlich Konsequenzen nach einem Betrugsfall gezogen. Von den Personen, die eine Kostenrückerstattung angefordert haben (70 % der Betroffenen), hat nur die Hälfte (35 %) diese auch tatsächlich erhalten. Weitere oft gesetzte Maßnahmen inkludieren das Schreiben schlechter Bewertungen (49 %) und die öffentliche Meldung des Betrugs auf Social Media (32 %).

**Von den Betroffenen haben allerdings nur 15 % Anzeige bei der Polizei erstattet.** Wie bereits in Kapitel 2.2.4 erwähnt, haben mehr als die Hälfte der Personen, die Anzeige erstattet haben (54 %), einen finanziellen Schaden von über 200 Euro erlitten. Nur 7 % der Betroffenen haben den Betrugsfall beim Internet-Ombudsmann gemeldet.

#### Fact Box Sicherheitsvorkehrungen & Konsequenzen:

- 67 % der Internet-Nutzer achten auf die Seriosität des Online-Shops.
- Zwei Drittel (67 %) der Befragten geben auch an, häufig bzw. fast immer lizenzierte Produkte zu verwenden.
- 83 % der Internet-Käufer achten auf die Zahlungsmodalitäten.
- 70 % der Internet-Käufer informieren sich über den Anbieter.
- 86 % der Internet-Käufer haben Konsequenzen gezogen. Am häufigsten wurde eine Kostenrückerstattung angefordert, gefolgt vom Schreiben schlechter Bewertungen im Internet. Nur 15 % der Betroffenen haben Anzeige bei der Polizei erstattet. Die Großzahl an Betroffenen, die Anzeige erstatten, haben einen Schaden von mindestens 200 EUR erlitten.

### 3.6. Risikogruppen

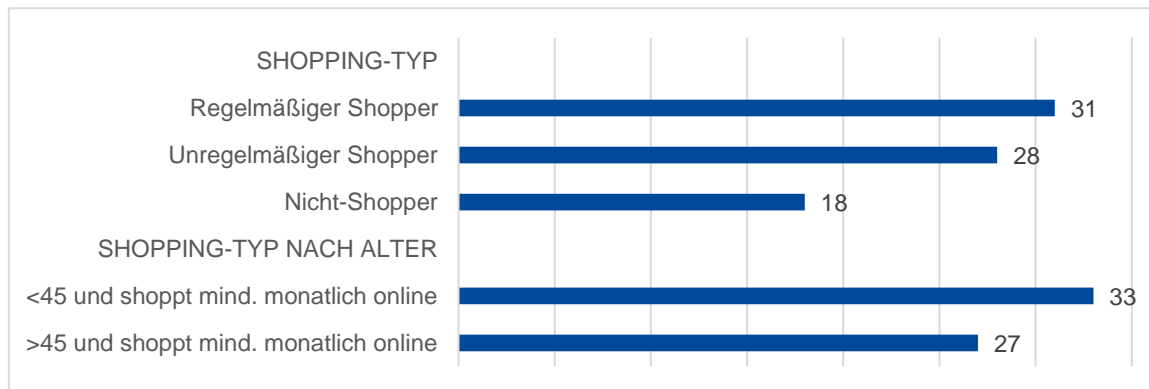


Abbildung 6: Nutzungstypen nach Shopping-Typ und Alter der vom Internet-Betrug Betroffenen in %, Basis: von Internet-Betrug betroffen, n=250

Eine besonders große Risikogruppe, die sich aus der Befragung herauskristallisiert hat, ist die Gruppe der unter 45-jährigen regelmäßigen Shopper. Insgesamt geben 31 % der befragten Opfer von Internet-Betrug an, regelmäßig im Internet einzukaufen, 33 % der unter 45-Jährigen geben an, mindestens einmal monatlich im Internet einzukaufen.

**Allgemein gibt ein Drittel (32 %) der Befragten an, eher (sehr) risikobereit zu sein. Demgegenüber gibt ein weiteres Drittel an, gar nicht risikobereit zu sein.**

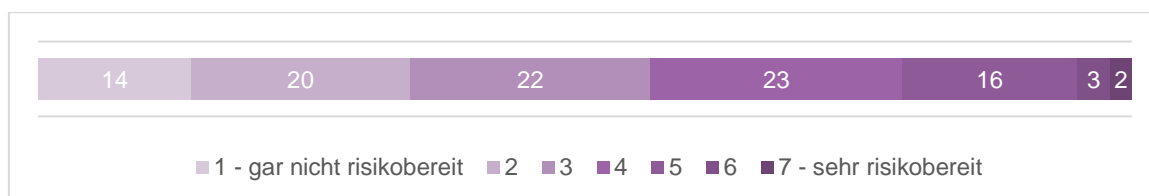


Abbildung 7: Selbsteinschätzung der Risikobereitschaft der Befragten, Basis: gesamt, n=1.002

Auf die Frage, wie häufig die befragten Internetnutzer riskante Webseiten besuchen, geben fast die Hälfte der Umfrageteilnehmer an, von monatlich bis fast täglich riskante Webseiten zu besuchen.

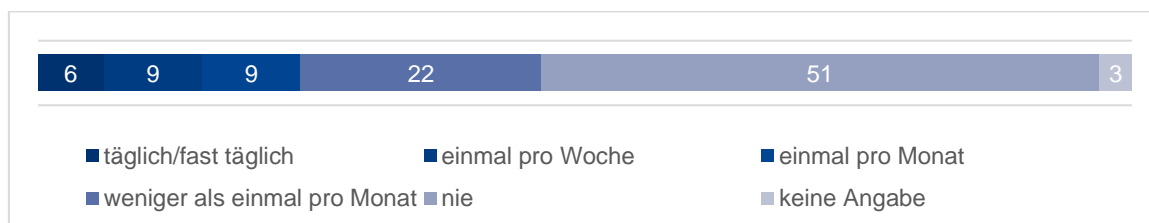


Abbildung 8: Angaben der Befragten zur Häufigkeit des Besuchs riskanter Webseiten, Basis: gesamt, n=1.002

**Bei näherer Analyse bildet sich eine besonders ausgeprägte Risikogruppe heraus: jene der Risikobereiten, die bereits Opfer von Internet-Betrug waren.**

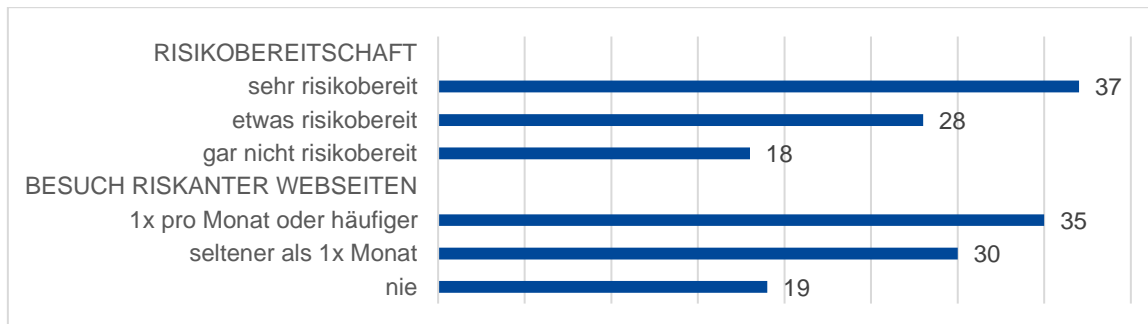


Abbildung 9: Risikobereitschaft der von Internet-Betrug betroffenen Internetnutzer in %, Basis: Opfer n=250

Wie aus Abbildung 9 ersichtlich, ist über ein Drittel (37 %) der Internetnutzer, die in ihrem Leben bereits von Internet-Betrug betroffen waren, tendenziell risikobereit, und 28 % geben an, etwas risikobereit zu sein. 35 % der Opfer vermelden, mindestens einmal im Monat riskante Webseiten besucht zu haben. Weitere 30 % geben an, riskante Webseiten zu besuchen, jedoch seltener als einmal im Monat.

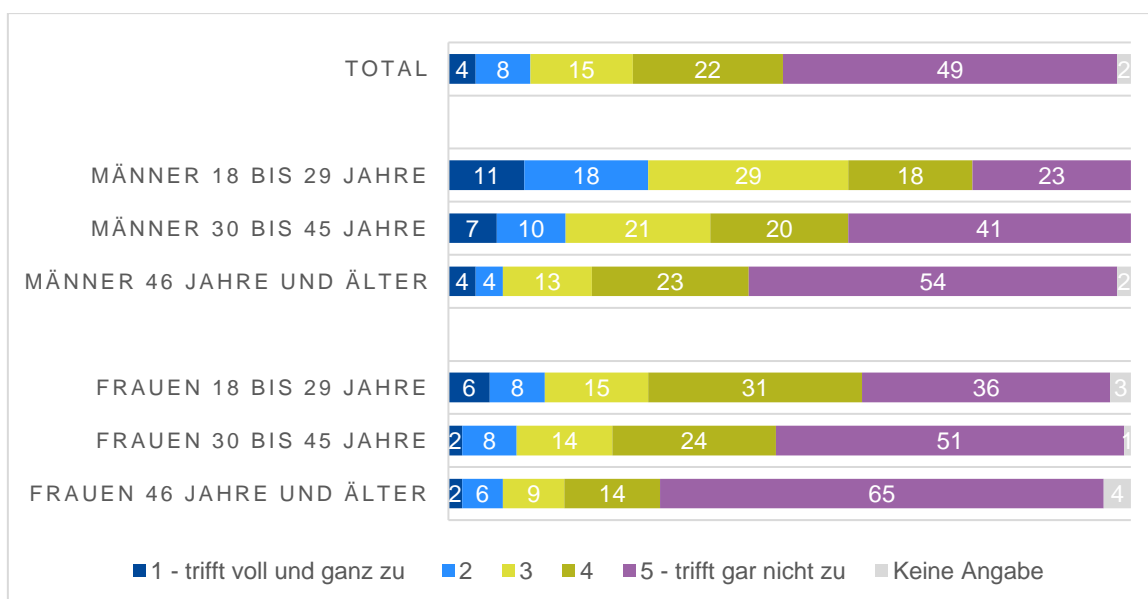


Abbildung 10: Angaben zur Frage: "Auch wenn mir eine Webseite nicht ganz seriös vorkommt, riskiere ich eine Bestellung, wenn ich ein richtig gutes Angebot finde." in % nach Geschlecht, Basis: gesamt, n=1.002

Auf die Frage, ob eine Bestellung riskiert wird, auch wenn die Webseite nicht seriös erscheint, antworteten 12 % der Befragten, dass das völlig oder eher zutrifft, weitere 15 % sind dabei neutral. Jedoch, wie aus der Unterteilung nach Geschlecht und Alter ersichtlich, sind Männer im Alter von 18 bis 29 Jahren die sorgloseste Risikogruppe, da sie zu 29 % völlig oder eher zustimmen und zu weiteren 29 % neutral sind.

**Fact Box Risikogruppen:**

- Männern, Personen mit höherem formalem Bildungsniveau, besonders risikobereiten Menschen und Menschen, die häufig auf riskanten Webseiten surfen, passiert Internet-Betrug tendenziell häufiger.
- Männer im Alter von 18 bis 29 Jahren bilden die sorgloseste Risikogruppe.
- Fast zwei Drittel der Betroffenen geben an, tendenziell sehr bzw. eher risikobereit zu sein.
- 35 % der Opfer geben an, mindestens einmal im Monat riskante Webseiten besucht zu haben.

## 4. Conclusio

### 4.1. Zusammenfassung der Ergebnisse

**Ein Viertel (25 %) der befragten Online-Nutzer geben an, persönlich bereits von Internet-Betrug betroffen gewesen zu sein. Auf die österreichische Gesamtbevölkerung hochgerechnet, entspricht dieser Prozentsatz 1,5 Millionen Personen.**

Die Ergebnisse der Studie zeigen: Allgemein besteht **ein großes Dunkelfeld, auch im Bereich der leichten Internet-Betrugsformen**. Es gibt jedoch eine „Grauzone“ zwischen tatsächlichen Betrugsfällen und Gewährleistungsfällen.

Die Betrugsfälle, von denen die Befragten laut eigenen Angaben am öftesten betroffen waren, inkludieren folgende Situationen:

- Gelieferter Artikel war nicht das, was man bestellt hatte.
- Besteller Artikel entsprach den Erwartungen nicht.
- Enttäuschung über schlechtes Kundenservice und Retouren-/Reklamationsmanagement

**Die Schadenshöhe ist in der Regel überschaubar und beträgt durchschnittlich 50 Euro.** Die Hälfte der Befragten gab an, einen Schaden von weniger als 50 Euro erlitten zu haben. Nur bei 17 % der befragten Personen betrug die Schadenssumme mehr als 200 Euro. Wenn Anzeige erstattet wurde, war der Schaden wesentlich höher (bei 54 % über 200 Euro).

**Zwei Drittel der Betroffenen bekamen die Kosten ihres Kaufs nicht rückerstattet.** Hochgerechnet betraf diese Problematik in den letzten 12 Monaten in Österreich rund 320.000 Menschen.

Die Personengruppen, die am meisten von Internet-Betrug betroffen sind, inkludieren Männer, Personen mit höherem formalem Bildungsniveau, allgemein besonders risikobereite Menschen und Menschen, die häufig auf riskanten Webseiten surfen.



## 4.2. Empfehlungen des KFV

### **Bewusstseinsbildung**

Die aktuelle Studie zeigt: Nur wenige von Internet-Betrug betroffene Menschen erstatten Anzeige bei der Polizei oder melden den Betrugsfall dem Internet-Ombudsmann. Mögliche Gründe dafür sind mangelndes Problembewusstsein und die allgemein verbreitete Meinung, dass diese Maßnahmen ohnehin nicht erfolgreich seien. Bei einer Aufklärungsquote von mehr als einem Drittel der angezeigten Betrugsfälle zeigt sich aber, dass eine Anzeige bei der Polizei sehr wohl sinnvoll ist. Eine Meldung beim Internet-Ombudsmann ist für die Prävention weiterer Betrugsfälle sehr hilfreich, da sich Internet-Käufer bei dieser Informationsquelle über Betrugsfälle und -versuche informieren können.

### **Auf Merkmale eines seriösen Online-Shops achten**

Leicht abrufbare AGBs, Produktbeschreibungen und Lieferzeiten, vorhandene Gütesiegel, verfügbares Impressum und Kaufbestätigung per E-Mail gehören zu den wichtigsten Merkmalen eines vertrauenswürdigen Online-Shops. Informieren Sie sich darüber und überprüfen Sie Online-Shops, die Sie noch nicht aus eigener Kauferfahrung kennen, möglichst genau auf deren Seriosität.

### **Risikoverhalten verringern**

Risikogruppen wie Männer, Personen mit höherem formalem Bildungsniveau und Menschen, die häufig auf riskanten Webseiten surfen, machen den Großteil der Opfer von Fake Shops aus. Umso wichtiger ist, dass diese Gruppen ihr Risikoverhalten verringern, vermehrt technische Sicherheitsmaßnahmen einsetzen und ihre Wachsamkeit erhöhen.

### **Licht ins Dunkelfeld werfen**

Informationen aus erster Hand erleichtern die Polizei- und Präventionsarbeit und erhöhen die Wirksamkeit der eingesetzten Maßnahmen. Daher ist es wichtig, im Falle eines Betrugsfalls umgehend Anzeige bei der Polizei zu erstatten bzw. den Betrugsfall zu melden (z.B. beim Verein für Konsumentenschutz oder bei der Internet-Ombudsstelle). Mit vereinten Kräften werden Wissen und Bewusstsein zum Thema Internet-Betrug intensiviert, Risiken und Schadensfolgen minimiert.

## Tabellenverzeichnis

Tabelle 1: Internet-Betrug - 2019 - Österreich - Anzahl der Straftaten; Quelle BMI, eigene Darstellung.....	5
Tabelle 2: Betroffenheit von Internet-Betrug inkl. Betrug beim Online-Shopping und andere Formen von Internet-Betrug, n=1.002 .....	9

## Abbildungsverzeichnis

Abbildung 1: Häufigste Betrugsformen in %.....	10
Abbildung 2: Erlittener finanzieller Schaden, Basis: vom Internet-Betrug betroffen, n=250, in % 10	
Abbildung 3: Verhalten beim Online-Shopping: Worauf die Nutzer achten, n=1.002.....	11
Abbildung 4: Sicherheitsmaßnahmen beim Online-Shopping, Basis: bestellt zumindest selten im Internet, n=938.....	11
Abbildung 5: Angaben zur Frage "Was haben Sie getan, nachdem der Betrug passiert ist?" in % (mehrfache Nennungen), Basis: von Internet-Betrug betroffen, n=250 .....	12
Abbildung 6: Nutzungstypen nach Shopping-Typ und Alter der vom Internet-Betrug Betroffenen in %, Basis: von Internet-Betrug betroffen, n=250 .....	13
Abbildung 7: Selbsteinschätzung der Risikobereitschaft der Befragten, Basis: gesamt, n=1.00213	
Abbildung 8: Angaben der Befragten zur Häufigkeit des Besuchs riskanter Webseiten, Basis: gesamt, n=1.002 .....	13
Abbildung 9 Risikobereitschaft der von Internet-Betrug betroffenen Internetnutzer in %, Basis: Opfer n=250 .....	14
Abbildung 10: Angaben zur Frage: "Auch wenn mir eine Webseite nicht ganz seriös vorkommt, riskiere ich eine Bestellung, wenn ich ein richtig gutes Angebot finde." in % nach Geschlecht, Basis: gesamt, n=1.002 .....	14

## Literaturverzeichnis

- Akdeniz, Y. (2002). Anonymity, Democracy, and Cyberspace. *Social Research: An International Quarterly* (69), S. 223-237.
- BMI/BK. (2020). *Polizeiliche Kriminalstatistik 2019*. Wien: Bundesministerium für Inneres, Bundeskriminalamt. Abgerufen am 28. Oktober 2020 von [https://bundeskriminalamt.at/501/files/Broschuere\\_PKS\\_2019.pdf](https://bundeskriminalamt.at/501/files/Broschuere_PKS_2019.pdf)
- Bundeskriminalamt Deutschland. (2020). *Kriminalstatistisch-kriminologische Analysen und Dunkelfeldforschung*. Abgerufen am 10. November 2020 von [https://www.bka.de/DE/UnsereAufgaben/Forschung/ForschungsprojekteUndErgebnisse/Dunkelfeldforschung/dunkelfeldforschung\\_node.html](https://www.bka.de/DE/UnsereAufgaben/Forschung/ForschungsprojekteUndErgebnisse/Dunkelfeldforschung/dunkelfeldforschung_node.html)
- Hildebrandt, A. & Kolf, F. (02. November 2017). *Wie man sich vor Fake-Shops schützt*. Abgerufen am 10. November 2020 von Handelsblatt: <https://www.handelsblatt.com/unternehmen/handel-konsumgueter/online-handel-wie-man-sich-vor-fake-shops-schuetzt/20531168.html?ticket=ST-10645000-pTHmBRJOltzaMSgglb0v-ap5>
- Internet Ombudsmann. (24. März 2020). Coronavirus: Online-Shopping boomt – Betrüger nützen Notlage. Wien: APA OTS. Abgerufen am 10. November 2020 von [https://www.ots.at/presseaussendung/OTS\\_20200324\\_OTS0034/coronavirus-online-shopping-boomt-betruenger-nuetzen-notlage](https://www.ots.at/presseaussendung/OTS_20200324_OTS0034/coronavirus-online-shopping-boomt-betruenger-nuetzen-notlage)
- Köllisch, T. (2004). Vom Dunkelfeld ins Hellfeld. Anzeigeverhalten und Polizeikontakte bei Jugenddelinquenz. Freiburg: Albert-Ludwigs-Universität.
- Regiodata Research GmbH Österreich. (5. Dez 2019). <https://www.regiodata.eu/>. Abgerufen am 21. Okt 2020 von REGIODATA STUDIE: ONLINEHANDEL IN ÖSTERREICH: [https://www.regiodata.eu/attachments/article/1174/RegioData\\_PRA\\_Onlinehandel\\_AT\\_05\\_12\\_2019.pdf](https://www.regiodata.eu/attachments/article/1174/RegioData_PRA_Onlinehandel_AT_05_12_2019.pdf)
- Schallbruch, M. (2018). *Schwacher Staat im Netz: Wie die Digitalisierung den Staat in Frage stellt*. Wiesbaden: Springer Fachmedien Wiesbaden GmbH.
- Watchlist Internet. (2020). *Fake-Shops*. Abgerufen am 10. Oktober 2020 von Internet-Betrug, Fallen & Fakes im Blick: <https://www.watchlist-internet.at/fake-shops/>



KfV (Kuratorium für Verkehrssicherheit)

Schleiergasse 18

1100 Wien

**T** +43-(0)5 77 0 77-DW oder -0

**F** +43-(0)5 77 0 77-1186

**E-Mail** [kfv@kfv.at](mailto:kfv@kfv.at)

**www.kfv.at**

**Medieninhaber und Herausgeber:** Kuratorium für Verkehrssicherheit

**Verlagsort:** Wien

**Herstellung:** Eigendruck

**Redaktion:** Dr. Georg Plattner

**Grafik:** Kuratorium für Verkehrssicherheit

**Cover-Foto:** Mohamed Hassan / Pixabay

**Copyright:** © Kuratorium für Verkehrssicherheit, Wien. Alle Rechte vorbehalten.

**SAFETY FIRST!**