Verbraucherzentrale Hamburg

Internetkriminalität: Vorsicht, Online-Betrug – so handeln Sie im Notfall!

Fake Shops, Identitätsklau, Phishing Mails – Betrügereien im Internet nehmen seit Jahren zu. Vor allem beim Online-Einkauf sollten Sie wachsam sein. Schnell ist Ihr Geld weg und Sie haben viel Ärger. Das sind die perfiden Maschen der Betrüger. So handeln Sie im Notfall!



© istock.com/Srdjanns74

Stand: 11.08.2025

Unser Leben ist heute digitaler als je zuvor. Internetkriminelle haben so ein leichtes Spiel. Der Online-Betrug ist mittlerweile eines der dominierenden Kriminalitätsfelder. Seien Sie im Netz daher besonders vorsichtig. Gehen Sie sparsam mit Ihren Daten um und fragen Sie sich immer, ob die Person, mit der sie kommunizieren oder der sie Geld überweisen möchten, wirklich vertrauenswürdig ist. Fallen Sie nicht auf diese Betrugsmaschen herein und handeln Sie umsichtig! Unsere digitalen Tools helfen Ihnen dabei.

Fake-Shops (gefälschte Online-Shops)



© Melanie Freund

Das neueste Smartphone, die angesagtesten Sneaker, die trendigen Gartenmöbel – und alles 20 bis 50 Prozent günstiger als in anderen Shops. Doch oft platzt der Traum vom Super-Schnäppchen. Kunden erhalten nach Zahlung per Vorkasse keine Ware. Ihr Geld sehen die meisten nicht wieder.

Zur Fake-Shop-Liste: Fake Shops: Wenn günstig richtig teuer wird!

China-Shops (dubiose Online-Shops)



© Melanie Freund

Wenn Sie im Internet nach neuen Klamotten und anderen Dingen stöbern, stoßen Sie schnell auf günstige Angebote. Dass es sich dabei um ausländische Shops – meist mit Sitz in China – handelt, ist nicht sofort zu erkennen. Schauen Sie lieber zweimal hin, bevor Sie etwas bestellen.

Mehr erfahren: China Shops: Günstig online shoppen?

Kleinanzeigen im Internet (Secondhand und Zweitmarkt)



© Melanie Freund

Die Inserate auf Kleinanzeigenportalen klingen oft verlockend. Doch Vorsicht ist geboten, denn bevor Sie die Ware in den Händen halten, müssen Sie erst einmal zahlen. Auch wer etwas verkaufen möchte, sollte auf der Hut sein.

Mehr erfahren: Betrugsmaschen mit Kleinanzeigen im Internet

Sollten Sie von dieser Betrugsmasche betroffen sein, unterstützen wir Sie mit unserem **Notfall-Check für Betrügereien mit Kleinanzeigen im Internet (Zweitmarkt).** Einfach den Reiter unten ausklappen, warten bis das Online-Tool geladen ist, Fragen beantworten und Felder ausfüllen – Checkliste herunterladen. Fertig.

Notfall-Checkliste für Kleinanzeigenbetrug erstellen

Beachten Sie: In dem Tool werden persönliche Daten verarbeitet und gespeichert. Informationen dazu finden Sie in unseren Datenschutzhinweisen.

Rechnungen für Bestellungen und Verträge (Warenbetrug)

In Ihrem Briefkasten liegen Rechnungen und Mahnungen von Online-Shops oder Briefe von Inkassounternehmen, obwohl Sie weder etwas bestellt noch über Paypal Geld angewiesen haben. Vielleicht wurde Ihre Identität gestohlen und jemand anderes war in Ihrem Namen auf Einkaufstour.

Mehr erfahren: Identitätsmissbrauch: Wenn Sie nichts bestellt haben und trotzdem zahlen sollen

Unser **Notfall-Check** zeigt Ihnen, was Sie tun können, wenn jemand Ihre persönlichen Daten nutzt, um Verträge auf Ihren Namen abzuschließen. Die individuelle Checkliste enthält wichtige Maßnahmen: Sie erfahren, welche Möglichkeiten Sie haben, Ihr Geld zurückzubekommen und was Sie dafür tun müssen, worauf Sie bei der Beweissicherung achten sollten und wann eine Strafanzeige sinnvoll ist.

Einfach den Reiter unten ausklappen, warten bis das Online-Tool geladen ist, Fragen beantworten und Felder ausfüllen – Checkliste herunterladen. Fertig.

Notfall-Checkliste für nicht abgeschlossene Verträge

Beachten Sie: In dem Tool werden persönliche Daten verarbeitet und gespeichert. Informationen dazu finden Sie in unseren Datenschutzhinweisen.

Identitätsdiebstahl (gehackte Accounts)



© Melanie Freund

Seien Sie wachsam beim Umgang mit persönlichen Daten im Netz! Immer wieder kommt es zu Identitätsdiebstahl oder Identitätsmissbrauch, der hohe Rechnungen nach sich zieht. Bei gehackten Accounts ist schnelles Handeln gefragt.

Mehr erfahren: Identität geklaut und Account gehackt? Das sollten Sie tun!

Plötzlich kein Zugriff mehr auf Ihr E-Mail-, Social-Media- oder Shopping-Konto? Ein gehackter Account kann großen Schaden anrichten. Unser **Notfall-Check für gehackte Accounts** zeigt, wie Sie die Kontrolle über Ihr Konto zurückbekommen, wo Sie den Angriff melden sollten und welche Sofortmaßnahmen Sie schützen.

Einfach den Reiter unten ausklappen, warten bis das Online-Tool geladen ist, Fragen beantworten und Felder ausfüllen – Checkliste herunterladen. Fertig.

Notfall-Checkliste für gehackte Accounts erstellen

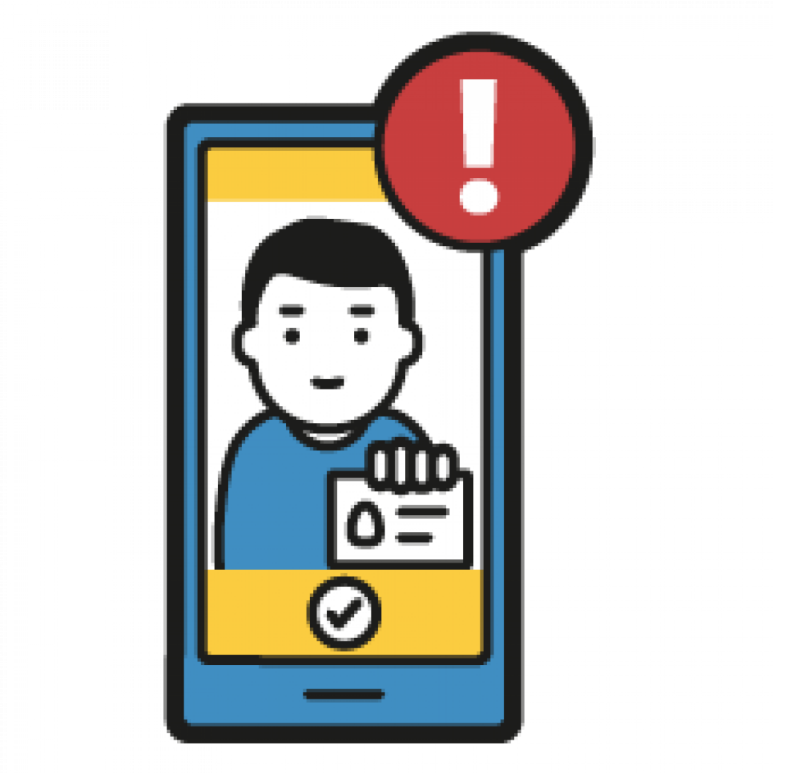
Beachten Sie: In dem Tool werden persönliche Daten verarbeitet und gespeichert. Informationen dazu finden Sie in unseren Datenschutzhinweisen.

Falsche Paket-SMS

Im Internet bestellt, am nächsten Tag geliefert. Doch Vorsicht: Falsche Paket-SMS können Sie viel Geld kosten. In den gefälschten Nachrichten werden Sie aufgefordert, per Link eine Lieferung zu bestätigen. Aber über einen Klick auf den Link werden oft persönliche Daten für Kontoabbuchungen und Abofallen abgegriffen. Links in Nachrichten unbekannter Absender sollten Sie daher niemals öffnen.

Mehr erfahren: Achtung, Paket-SMS kann teuer werden!

Plattformen für Krypto, Aktien und Trading



© Melanie Freund

Dubiose Trading-Plattformen werben im Internet und auf sozialen Netzwerken mit verlockenden Versprechungen von einfachen und schnelle Gewinnen. Sie behaupten, dass der Handel mit Aktien, Optionen, CFDs oder Kryptowährungen zum großen Reichtum führt. Dabei wird man um sein Erspartes gebracht.

Mehr erfahren: Dubiose Trading-Plattformen: Wie Betrüger mit schnellen Gewinnen locken

---

Erpressung mit Schadsoftware



© Melanie Freund

Hatten Sie auch schon einmal einen Microsoft-Mitarbeiter oder anderen IT-Experten am Telefon, der Viren von Ihrem Computer löschen wollte? Oder ist plötzlich eine Warnmeldung auf Ihrem Rechner aufgeploppt. Achtung, hier sind Betrüger am Werk! Mittels einer Software verschaffen sich diese Zugang zu ihrem Computer und verlangen für ihre „Dienstleistung“ Geld. Übrigens: Auch mit Pornos und Nacktbildern versuchen Kriminelle, Kasse zu machen.

Mehr erfahren: Microsoft: Bei Anruf 250 Euro

Sie haben eine Erpresser-Mail erhalten oder werden unter Druck gesetzt? Unser **Notfall-Check für Erpressungen** hilft Ihnen, die Bedrohung einzuordnen und richtig zu reagieren. Die Checkliste zeigt, welche Schritte Sie unternehmen sollten – von der Beweissicherung über eine mögliche Strafanzeige bis hin zum Schutz Ihrer Daten.

Einfach den Reiter unten ausklappen, warten bis das Online-Tool geladen ist, Fragen beantworten und Felder ausfüllen – Checkliste herunterladen. Fertig.

Notfall-Checkliste für Erpressungen erstellen

Beachten Sie: In dem Tool werden persönliche Daten verarbeitet und gespeichert. Informationen dazu finden Sie in unseren Datenschutzhinweisen.

Phishing, Smishing und Quishing



© Melanie Freund

Beim Phishing (über Links), Smishing (über SMS) und Quishing (über QR-Codes) geht es oft um Ihr Konto. Es kann aber auch andere Zugangsdaten betreffen, beispielsweise die Daten zu Ihrem Benutzerkonto bei Ebay, Paypal oder anderen Diensten im Internet. Wie beim Fischen hoffen die Täter, dass ihnen einige arglose Verbraucherinnen und Verbraucher ins Netz gehen.

Mehr erfahren: Phishing-Angriff aufs Konto – auch als Brief per Post

GUT ZU WISSEN

Wir arbeiten eng mit der Polizei Hamburg zusammen, um Straftaten in der digitalen Welt vorzubeugen. So rücken wir die Internetkriminalität in den Fokus der Öffentlichkeit. Auf der Website der Polizei Hamburg finden Sie weitere Informationen.

Gefördert durch:

Bundesministerium
der Justiz und
für Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

© Verbraucherzentrale Hamburg e. V.

https://www.vzhh.de/themen/telefon-internet/probleme-festnetz-handy-internet/internetkriminalitaet-vorsicht-online-betrug-so-handeln-sie-im-notfall