POLIZEI
Nordrhein-Westfalen
Dortmund

Betrug über Verkaufsplattformen

Quelle: adobe stocks (Polizei NRW)

Verkaufsplattformen und Gefahren

POLIZEI
Nordrhein-Westfalen
Dortmund

Die Verwendung des Internets bietet zahlreiche Vorteile und vereinfachet das Leben von Millionen von Menschen in vielfältiger Weise. Allerdings entstehen dadurch auch viele Möglichkeiten, Opfer von Cyberkriminellen zu werden.

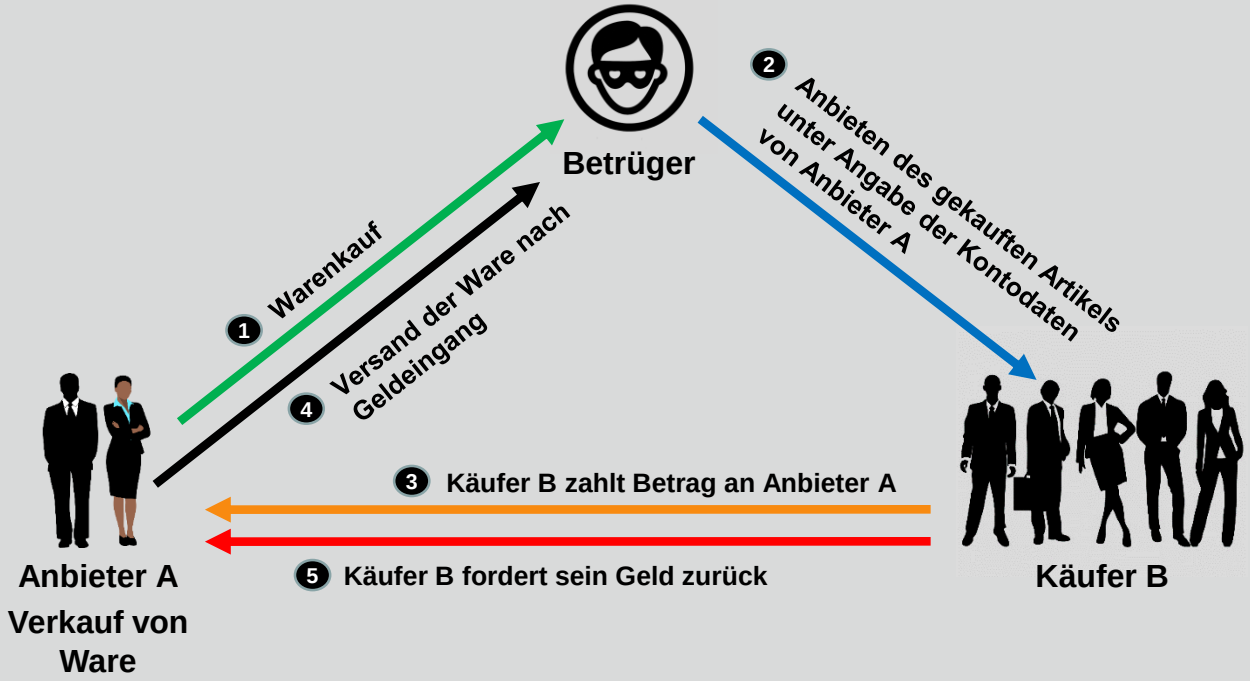
Gerade über Verkaufsplattformen und online Marktplätze verkaufen viele Menschen täglich zahlreiche Artikel und profitieren von großer Kundenreichweite und geringen Gebühren. Diese große Reichweite bietet aber auch Kriminellen eine Plattform, um mit gefälschten Anzeigen, E-Mails und zahlreichen Betrugsmaschen die ehrlichen Bürger zu betrügen.

Zu den bekanntesten Betrugsmaschen auf Verkaufsplattformen zählen:

- **Dreiecksbetrug**
- **Datendiebstahl**
- **Post-Trick**
- **Abholtrick**
- **PayPal Family & Friends**
- **Geisterkonten**

Jeder Betroffene sollte sich direkt an die Polizei wenden!

Dreiecksbetrug

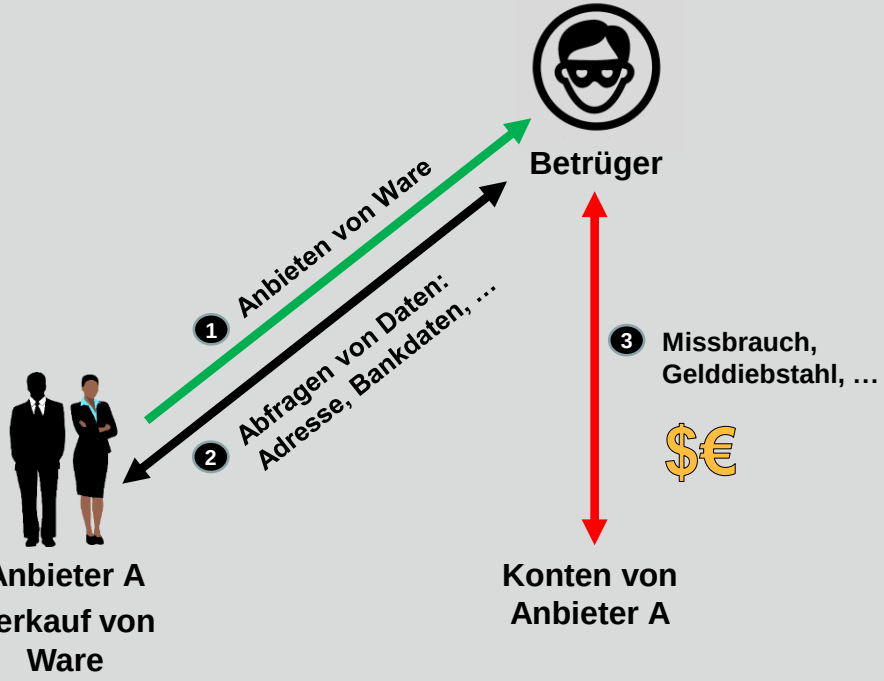


Der Betrüger spielt zwei Nutzer gegeneinander aus.

Sie stellen als Beispiel ein iPhone zum Verkauf. Der Betrüger entdeckt das Inserat und bietet daraufhin ebenfalls ein iPhone zum gleichen Preis an. Gleichzeitig gibt er sich bei Ihnen als Interessent aus.
Er verspricht, das Gerät gleich kaufen und bezahlen zu wollen und schlägt eine PayPal-Zahlung oder Banküberweisung vor. Sie geben ihm als Verkäufer die entsprechenden Kontodaten.
Damit hat der Betrüger das erste Ziel seines Plans erreicht.

Nun wartet der Betrüger darauf, dass ein Interessent das Gerät kauft, dass der Kriminelle selbst annonciert hat. Dieser Käufer bekommt dann vom Betrüger Ihre Zahlungsdaten und bezahlt das gekaufte Gerät.
Weil das Geld auf Ihrem Konto eintrifft, schöpfen Sie keinen Verdacht und versenden das iPhone. Damit ist der Betrug perfekt. Denn der Betrüger erhält Ihr iPhone, für das jemand anderes bezahlt hat.
Der eigentliche Käufer wartet aber vergeblich auf die Ware und verlangt nach einer Weile bei PayPal sein Geld zurück. Der Betrüger ist dann längst untergetaucht und nicht mehr zu erreichen.

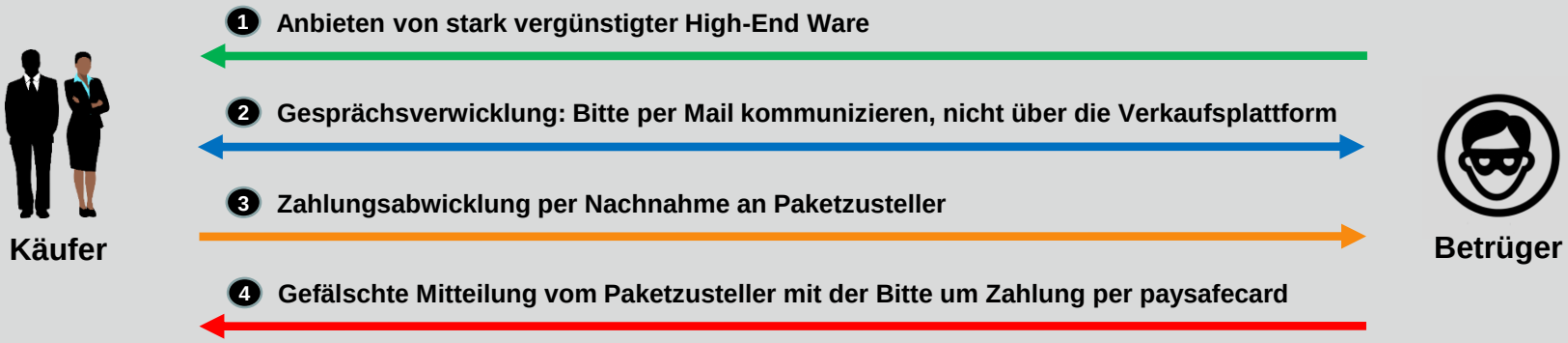
Datendiebstahl



Sensibler Datenklau

Der Verkäufer bietet seine Ware auf einer beliebigen Verkaufsplattform an. Die Betrüger fragen die Daten mit der Begründung ab, dass diese benötigt werden, um einen Geldboten zu beauftragen, welcher dann den gewünschten Betrag in Bar übergibt. Mit den Daten können die Cyberkriminellen dann weitere Straftaten begehen oder diese über spezielle Internetkanäle weiter verkaufen.

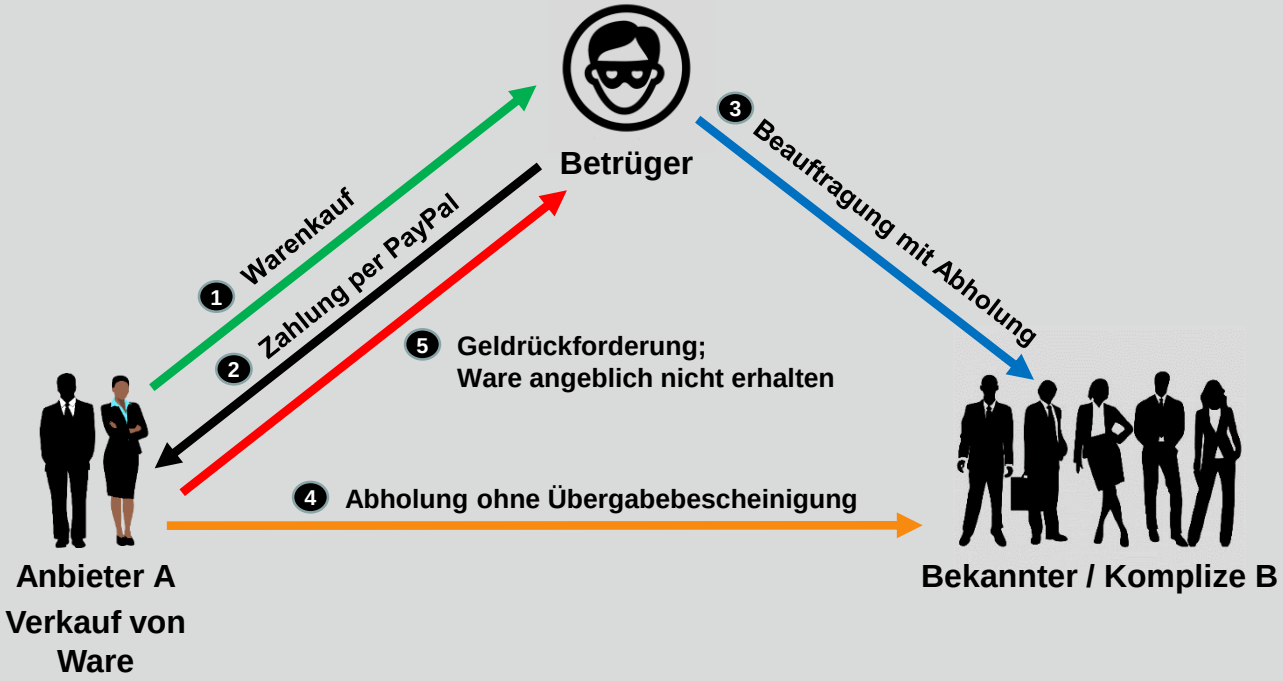
Post-Trick



Die gefälschte Versandbestätigung

Hierbei handelt es sich um zunächst echt wirkende Inserate, wobei die Kriminellen ihre Opfer meist mit stark vergünstigten High-End Produkten locken.
Wenn Nutzer dann Interesse an einem Produkt zeigen, folgt eine E-Mail oder SMS mit der bitte, künftig über eine bestimmte Mail-Adresse zu kommunizieren. Reagieren Käufer dann darauf, werden sie von den Betrügern in eine längere Unterhaltung verwickelt.
Wenn es um die Zahlungsabwicklung geht, wird eine Zahlung per Nachname über den Paketzusteller bevorzugt.
Im Anschluss wird eine gefälschte Mitteilung von einem Paketzusteller erstellt und an die Käufer versendet, in welchem sie zur Zahlung mittels einer paysafecard aufgefordert werden.
Sobald die Zahlung per paysafecard eingeleitet wurde, ist das Geld unwiderruflich weg, die versprochene Ware kommt nie an und die Betrüger sind nicht mehr zu erreichen.

Abholtrick

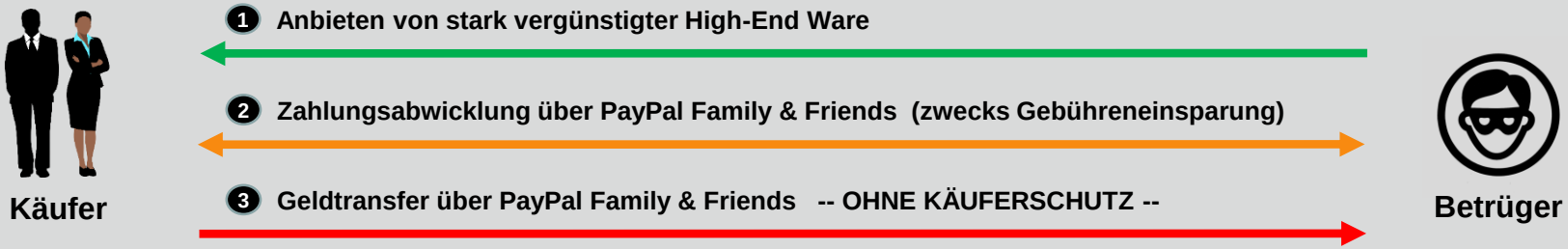


Beim Abholtrick wollen die Kriminellen unbedingt per PayPal bezahlen.

Die Betrüger überweisen die fällige Summe und schlagen vor, dass ein „Bekannter" die Ware abholt. Geht die Übergabe wie verabredet über die Bühne, schnappt die Falle zu. Denn die Betrüger behaupten später, die Ware nie erhalten zu haben. So bekommen sie das Geld von PayPal zurück und haben sowohl die Ware als auch das Geld. Der Verkäufer hat schlechte Karten, da er nicht beweisen kann, den Artikel wirklich übergeben zu haben.

Bei einem versicherten Paketversand wäre der Sachverhalt anders, da hat der Verkäufer einen Beleg samt Sendungsnummer als Beweis. Akzeptieren Sie bei einer Abholung am Besten nur Bargeld oder eine vorab ausgeführte Überweisung.

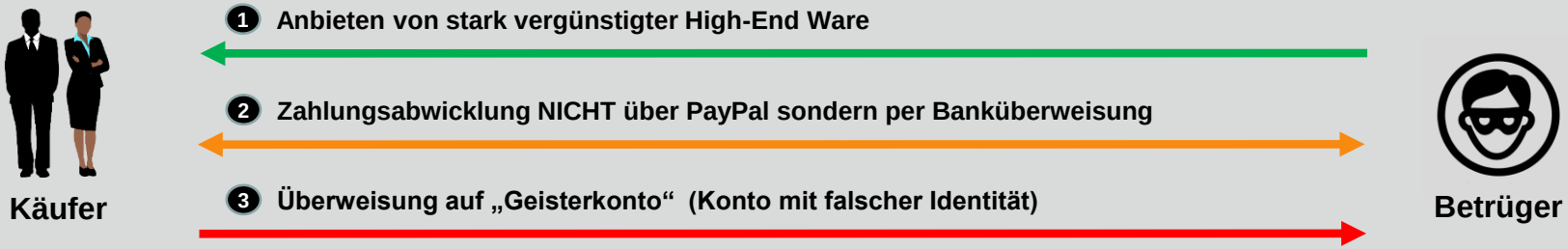
PayPal Family & Friends



Geldtransfer ohne Käuferschutz

Bei PayPal gibt es derzeit zwei Bezahloptionen. Die erste ist die Variante **„Freunde und Familie“**. Hier kann man Geld an bekannte private Personen überweisen. Das kostet keine Gebühren, allerdings entfällt dabei auch der von PayPal angebotene Käuferschutz. Wer nicht auf diesen Käuferschutz verzichten möchte, der kann sich für die Option **„Waren und Dienstleistungen“** entscheiden. Bei dieser Variante gehen Sie auf Nummer sicher! Im Gegenzug dafür erhält PayPal 1,9 Prozent des überwiesenen Betrags zu Lasten des Verkäufers. Und genau hier setzen die Betrüger an. Im persönlichen Kontakt wird den Käufern der angebotenen Ware vorgegaukelt, dass diese doch gerne die PayPal-Gebühren sparen wollen und bitten höflich um eine Bezahlung via „Freunde und Familie“-Option. Lassen sich jetzt gutgläubige Kunden darauf ein, sind sie ihr Geld los, ohne jemals ihre Ware zu erhalten. Die Kriminellen verschicken die angebotenen Artikel nicht und sind nach erfolgreicher Transaktion auch nicht mehr auffindbar. Und da der Käuferschutz hier nicht greift, wird auch PayPal kein Geld zurückerstatten.

Geisterkonten



Deutsche Konten mit falscher Identität

Die Betrüger locken Ihre Opfer meist mit stark vergünstigten High-End Produkten, die im freien Verkauf deutlich teurer sind und reagieren auf Anfragen sehr schnell, um Seriosität vorzutäuschen. Dabei geben die Verbrecher an, kein PayPal-Konto zu besitzen, um so den Verkauf per Banküberweisung abzuwickeln. Die Betrüger besitzen meist deutsche Konten, welche unter falschem Namen und mit gestohlenen Identitäten aus dem Internet eröffnet wurden, um so ihre Opfer in falscher Sicherheit zu wägen. Sobald das Geld transferiert worden ist, bricht der Kontakt ab und das Geld ist weg.

Wie kann man sich schützen?

POLIZEI Nordrhein-Westfalen Dortmund

Starke Passwörter verwenden

Stark ist ein Passwort, wenn es aus mindestens neun Zeichen unter Nutzung von Klein- und Großbuchstaben, Ziffern und Sonderzeichen besteht. Bitte keine Namen, Geburtsdaten oder Passwörter aus dem Wörterbuch verwenden und auf keinen Fall an Dritte weiter geben. Es wird empfohlen, für verschiedene Onlinezugänge auch unterschiedliche Nutzernamen und Passwörter zu verwenden. Diese Passwörter sollten auch an geeigneten Stellen und vor Dritten geschützt aufbewahrt werden. Optimal ist auch die Verwendung eines Passwortmanagers mit Schlüsselbundfunktion.

Verwenden Sie keine Passwörter, die in der Vergangenheit schon einmal benutzt wurden und vermeiden Sie die „Passwort merken“-Funktion von Anwendungen im Browser und in Applikationen (Apps). Bevorzugt werden sollten auch Dienste, welche die Zwei-Faktor-Authentifizierung unterstützen.

Privatsphäre schützen

Richtige Sicherheitseinstellungen auf den Endgeräten sowie in den Sozialen Medien reduzieren das Risiko, zu viele Informationen von sich selbst preiszugeben. Ein sorgfältiger Umgang mit seinen Profildaten und Bildern ist unerlässlich.

=> Seien Sie sparsam mit der Weitergabe Ihrer persönlichen Daten!

[Profilbild, personenbezogene Daten, Freunde-Einstellungen, öffentliche-Daten, Selfies, Likes]

Misstrauisch sein

Bei Anfragen von Unbekannten immer misstrauisch sein! Cyberkriminelle verstecken sich in erster Linie hinter anonymen, gefälschten und unseriösen Profilen. Aus diesem Grund sollte jede Kontaktanfrage immer kritisch hinterfragt und keine sensiblen Daten herausgegeben werden. Auch E-Mails von Unbekannten sollten weder geöffnet, noch sollten Anhänge und Links in keinster Weise angeklickt werden. Hier verbirgt sich oftmals Schadsoftware, mit der Absicht Passwörter zu erbeuten, um weitere, kriminelle Handlungen durchzuführen. Oftmals lassen sich Betrüger auch durch die unkorrekte Schreibweise der E-Mailabsenderadresse, deren Inhalt, falsche Umlaute, kryptische Buchstaben oder anhand der Linkadresse erkennen. Eine sichere Website erkennt man am „**s**“ (secure) in der Kopfadresse bei http**s**://...

Wo gibt es Hilfe?

POLIZEI
Nordrhein-Westfalen
Dortmund

Wenn man Opfer von Cybercrime geworden ist, stehen einem die gleichen umfangreichen Hilfs- und Unterstützungsangebote zur Verfügung, wie den Opfern von Straftaten in der realen Welt.

Bei akuter Bedrohung, wählen Sie 110! Die Polizei wird alles Erforderliche tun, um Sie zu schützen.

- Zeigen Sie die Straftat bei der Polizei an (Strafanzeige ist bei jeder Polizeidienststelle möglich)
- Existierendes Datenmaterial, wie z. B. E-Mails, Chat-Verläufe in Messenger-Diensten, digitale Fotos oder Videos sind wichtige Beweismittel, die Sie bis zum ersten Kontakt mit der Polizei bestenfalls komplett unverändert lassen.
- Bringen Sie das gesicherte Beweismaterial am besten gleich zur Anzeigenerstattung mit. Das ist wichtig für die weiteren Ermittlungen, um den Verlust von Spuren im Netz zu vermeiden.

Quelle: ProPK