Betrug
im Internet

So schützen Sie sich

Das Internet bietet viele Vorteile und erleichtert den Alltag. Damit Sie das Internet sicher nutzen können, ist es wichtig, über mögliche Gefahren Bescheid zu wissen. Dieser Folder erklärt häufige Betrugsmaschen im Internet und gibt Tipps, wie Sie sich davor schützen können.

www.watchlist-internet.at

Fake-Shops

Betrüger/innen geben vor, dass sie im Internet sehr günstige Produkte verkaufen. Ihre Websites sind aufwändig und professionell gestaltet. Wer Ware, die im Voraus bezahlt werden muss, erwirbt, verliert Geld, denn die angebotenen Produkte gibt es nicht.

- Bevor Sie bei einem Anbieter einkaufen, informieren Sie sich darüber, welche Erfahrungen andere Kunden gemacht haben. Geben Sie dazu in eine Suchmaschine zum Beispiel den Shopnamen und das Wort „Erfahrungen" als Suchbegriffe ein. Finden Sie keine oder vor allem negative Einträge, kann das ein Hinweis darauf sein, dass der Anbieter unseriös oder noch nicht etabliert ist.

- Vergleichen Sie die Preise auf Portalen, wie zum Beispiel geizhals.at oder idealo.at. Stellen Sie ungewöhnliche Preisunterschiede fest, spricht das für einen unseriösen Anbieter.

- Kontrollieren Sie die angebotenen Zahlungsmethoden des Online-Shops. Ist es am Ende des Bestellvorgangs nur möglich, den Warenpreis im Voraus zu bezahlen, sollte man besonders vorsichtig sein.

- Führen Sie eine Whois-Abfrage (z.B. auf www.whois.com/whois) durch, damit Sie sehen, wer die Domain des Online-Shops registriert hat. Stimmen die im Rahmen der Registrierung gemachten Angaben mit dem Impressum des Anbieters überein?

Markenfälschung

Auf der Suche nach günstiger Markenware können Konsument/innen auf Online-Shops stoßen, die hohe Rabatte auf ansonsten teure Produkte anbieten. Wer die günstige Ware bestellt, erhält eine Markenfälschung. Das Produkt ist mangelhaft und nicht zu gebrauchen. Der Zoll kann die gefälschte Ware beschlagnahmen, und, falls kein Widerspruch erfolgt, vernichten. Käufer/innen drohen hohe Zusatzkosten und rechtliche Konsequenzen. Markenfälscher sind anhand folgender Punkte zu erkennen:

- Jedes Produkt ist stark rabattiert und in ausreichender Stückzahl lagernd. Das gilt ebenso für ansonsten vergriffene Ware.
- Eine Suche zu dem Anbieter zeigt, dass es negative Kritiken von enttäuschten Kund/innen gibt.
- Auf der Website finden sich keine Angaben zum Webseitenbetreiber. Es ist lediglich möglich, diesen über ein Formular zu kontaktieren.
- Im Online-Shop finden sich Menüpunkte, wie Allgemeine Geschäftsbedingungen oder Datenschutz. Wenn Sie diese aufrufen, stellen Sie fest, dass es sich bei den Informationen um schlecht ins Deutsche übersetzte Texte handelt, die die genannten Punkte nicht thematisieren.
- Sie geben Ihre Daten über eine unverschlüsselte Verbindung bekannt. Das erkennen Sie an der Adresszeile Ihres Internetbrowsers, die über kein versperrtes Sicherheitsschloss und den Zusatz „https“ verfügt.

Schadsoftware

Mit gefälschten Rechnungen, manipulierten Websites oder infizierten Programmen wollen Kriminelle Schadsoftware auf fremden Computern hinterlegen. Gelingt ihnen das, können sie das befallene Endgerät für Verbrechen nützen. Beispielsweise ist es den Verbrecher/innen möglich, dass sie wichtige Zugangsdaten ihrer Opfer stehlen, Dokumente verschlüsseln, Lösegeld für die Wiederherstellung von Dokumenten fordern oder den Computer für die Verbreitung illegaler Inhalte nutzen. Damit Sie das verhindern, ist es wichtig, dass Sie einige Punkte beachten:

- Öffnen Sie keine Dateianhänge von angeblichen Rechnungen oder sonstigen Schreiben, die Sie nicht betreffen können, denn darin verbergen Kriminelle Schadsoftware.
- Sichern Sie in regelmäßigen Abständen wichtige Dokumente und Dateien auf einem externen Datenträger ab. Das verhindert, dass Sie einen kompletten Datenverlust erleiden, wenn Schadsoftware Ihren Computer befällt.
- Aktualisieren Sie Ihr Betriebssystem und Ihre Programme. Andernfalls können Verbrecher/innen Sicherheitslücken nützen, um Ihren Computer mit bösartigen Programmen zu infizieren.
- Nutzen Sie ein Administratoren- und ein Benutzerkonto. Das erste kann Änderungen am Betriebssystem vornehmen. Das zweite ist für die alltägliche Arbeit am Computer geeignet. Nutzen Sie das Benutzerkonto, kann sich Schadsoftware nicht unbemerkt von Ihnen installieren.
- Verwenden Sie ein Antivirenprogramm und aktualisieren Sie es.

Tipp für Schadsoftware und Phishing

Wenn Sie Kund/in bei einem Unternehmen sind, von dem Sie eine unerwartete Nachricht erhalten haben, klicken Sie keinen Link in der Nachricht an. Öffnen Sie stattdessen den Browser und melden Sie sich auf der Seite

Phishing

Beim Phishing (engl. Password + Fishing) versuchen Unbekannte, die Zugangsdaten von Internet-Nutzer/innen zu stehlen. Dazu verschicken sie beispielsweise gefälschte Nachrichten von Banken, Online-Händlern oder E-Mail-Providern. In diesen Nachrichten nennen sie einen angeblichen Grund, der es notwendig macht, eine Website aufzurufen und persönliche Zugangsdaten bekannt zu geben. Diese Website ist gefälscht und imitiert bekannte Internetauftritte. Wenn Sie darauf die abgefragten Daten bekannt geben, verfügen die Kriminellen über diese.
Beachten Sie:

- Seriöse Unternehmen verlangen von Ihnen niemals, dass Sie persönliche Daten auf einer Internetseite angeben/bestätigen.
- Kontrollieren Sie, wer Ihnen eine Nachricht sendet. Stimmen der Absendername und die Absenderadresse tatsächlich überein oder ist das nicht der Fall?
- Phishingmails sind meistens unpersönlich gehalten (Sehr geehrter Kunde). Unternehmen benennen Adressat/innen direkt bei ihrem Namen.
- Fahren Sie mit Ihrer Computermaus über den in der Nachricht angeführten Link. Ein Dialogfenster zeigt Ihnen an, wohin er führt. Dadurch können Sie verdächtige Links erkennen.
- Kontrollieren Sie die Adresszeile Ihres Internetbrowsers und informieren Sie sich darüber, auf welcher Website Sie tatsächlich sind.

des Unternehmens in Ihrem Kundenkonto an. Wenn die Nachricht echt ist, sollten Sie im Kundenkonto dieselben Informationen vorfinden. Im Zweifel können Sie auch den Kundenservice unter der auf der Internetseite des Unternehmens genannten Telefonnummer anrufen.

Abo-Fallen

Auf den ersten Blick kostenlose Angebote führen nach der Registrierung zu einem teuren Abo. Der Kostenhinweis ist im Kleingedruckten versteckt, sodass Konsument/innen ihn nicht sofort erkennen können. Die Websiten-Betreiber/innen versenden hohe Rechnungen und drohen rechtliche Konsequenzen an, wenn Nutzer/innen den geforderten Betrag nicht bezahlen.

- Informieren Sie sich vor einer Registrierung über einen Anbieter. Das kann Ihnen dabei helfen, dass Sie eine Abo-Falle rechtzeitig erkennen.
- Geben Sie bei Diensten, die normalerweise gratis sind, keine persönlichen Daten bekannt.
- Lassen Sie sich von unbegründeten Rechnungen nicht einschüchtern und bezahlen Sie diese nicht.
- Ignorieren Sie die Androhung rechtlicher Schritte.
- Nehmen Sie im Bedarfsfall Kontakt mit Einrichtungen wie z.B. der Arbeiterkammer (www.arbeiterkammer.at) oder dem Internet Ombudsmann (www.ombudsmann.at) auf und lassen Sie sich von diesen beraten.

Kleinanzeigenbetrug

Wer privat Waren im Internet kaufen oder verkaufen möchte, kann an kriminelle Vertragspartner/innen gelangen. Sie erklären, dass sie im Ausland sind und schlagen vor, den Kauf über ein neutrales Unternehmen abzuwickeln. Es soll die Ware und das Geld erhalten. Erst wenn es beides hat, leitet es den Vertragsparteien die versprochene Leistung weiter. In Wahrheit gibt es das Unternehmen nicht. Es sind die Kriminellen, die gefälschte Nachrichten versenden. Sie erhalten ohne Gegenleistung das Geld oder die Ware.

- Betrügerische Vertragspartner/innen erkennen Sie daran, dass sie vorgeben, im Ausland zu sein.
- Die Kriminellen inserieren auffällig günstige oder sehr teure Ware. Damit können Sie entweder viele Opfer finden oder hohe Geldsummen erbeuten.
- Der Kauf soll über ein vermeintlich neutrales Unternehmen erfolgen, das den Zahlungs- oder Wareneingang bestätigt und Sie auffordert, dass Sie Ihre Gegenleistung erbringen.
- Bezahlen Sie niemals Waren im Voraus oder versenden Sie niemals ein Produkt, bevor Sie nicht auf Ihrem Bankkonto einen Zahlungseingang feststellen können.
- Am sichersten ist es, wenn Sie sich mit Ihren Vertragspartner/innen persönlich treffen und Ihre Leistungen vor Ort erbringen.

Internet-Betrug hat viele Facetten. Findige Betrüger/innen lassen sich immer wieder neue Tricks einfallen, um Internetnutzer/innen in die Falle zu locken. In den meisten Fällen geht es um Geld oder um das Herauslocken persönlicher Daten. Aber keine Angst – wenn Sie ein paar Grundregeln beherzigen, dann steht einer sicheren Internetnutzung nichts im Wege!

Weitere Tipps & Hilfe

Watchlist Internet
Aktuelle Meldungen zu Internet-Betrug: App und wöchentlicher E-Mail-Newsletter: www.watchlist-internet.at/newsletter

Internet Ombudsmann
Hier erhalten Sie Hilfe bei Problemen mit Internet-Shops und Internet-Betrug: www.ombudsmann.at

Arbeiterkammern
Kostenlose Konsument/innen-Beratung, unter anderem auch zu Konsumentenschutz im Internet und am Handy: www.arbeiterkammer.at

Bundeskriminalamt
Meldestelle Against Cybercrime: against-cybercrime@bmi.gv.at
Straftaten können auf jeder Polizeidienststelle zur Anzeige gebracht werden.

Broschüre gefördert durch

Watchlist Internet – Internet-Betrug, Fallen & Fakes im Blick
INTERNET OMBUDSMANN
Bundesministerium Soziales, Gesundheit, Pflege und Konsumentenschutz

Weitere Partner

AK Österreich
WILLHABEN
netidee OPEN INNOVATIONS

Gratis App „Watchlist Internet“:
Google play
App Store

Impressum
ÖIAT, Ungargasse 64, 1030 Wien - www.watchlist-internet.at