Kontakt:

Bundeskriminalamt
Josef-Holaubek-Platz 1
1090 Wien

Tel: +43 (0)1 24836-85025

against-cybercrime@bmi.gv.at

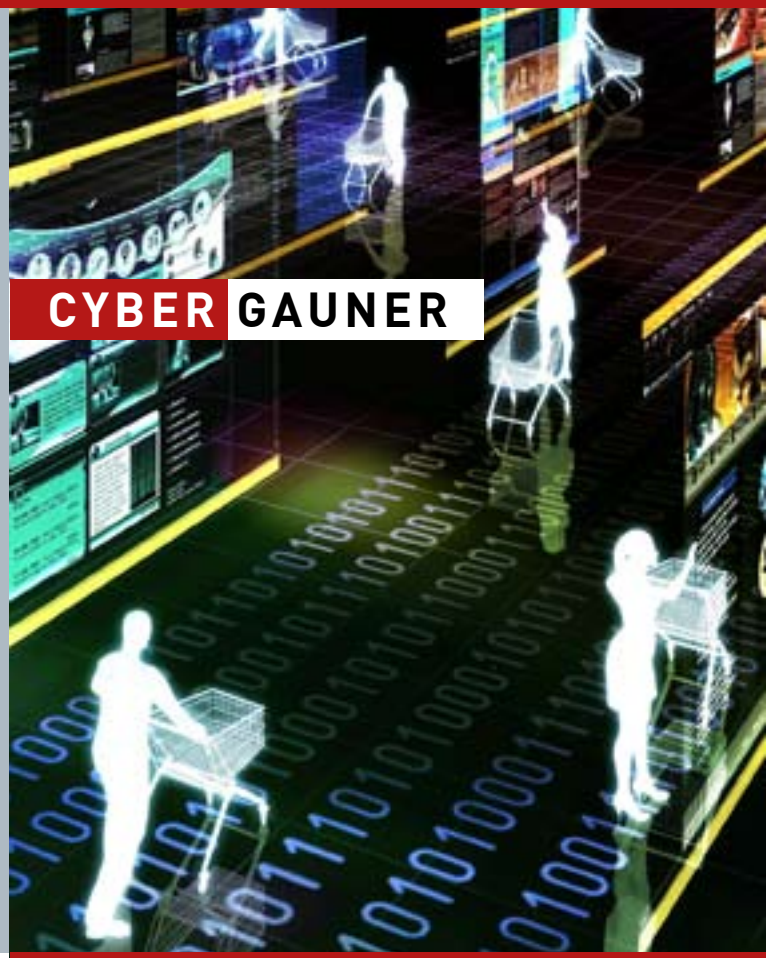
www.bundeskriminalamt.at
www.facebook.com/bundeskriminalamt

Wie können Sie sich vor Internetbetrug schützen?

- Installieren Sie Virenschutzprogramm und Firewall auf Ihrem Computer und führen Sie regelmäßig Updates durch.
- Öffnen Sie keine Dateianlagen von E-Mails unbekannter Herkunft und klicken Sie nicht auf darin enthaltene Links.
- Gehen Sie mit vertraulichen Daten sorgsam um und geben Sie diese nur auf vertrauenswürdigen und verschlüsselten Seiten („https“) bekannt.
- Übermitteln Sie keine Kopien von Ausweisen und persönlichen Dokumenten.

Sollten Sie Geschädigter eines Internetbetrugs sein, erstatten Sie Anzeige bei der nächstgelegenen Polizeidienststelle.

.BK BUNDESKRIMINALAMT



HERZLICHEN GLÜCKWUNSCH, SIE HABEN GEWONNEN!

INTERNETBETRUG – DIE ABZOCKE IM NETZ

.BK REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
BUNDESKRIMINALAMT

Das mach ich sicher.
Kuratorium Sicheres Österreich
www.dasmachichsicher.at

Impressum
Herausgeber: Bundesministerium für Inneres, Bundeskriminalamt, Josef-Holaubek-Platz 1, 1090 Wien, www.bundeskriminalamt.at, www.facebook.com/bundeskriminalamt; **Fotos:** © Nmedia - Fotolia.com, © pn_photo - Fotolia.com, © WavebreakMediaMicro - Fotolia.com; **Druck:** gugler GmbH, Auf der Schön 2, 3390 Melk; **Stand:** April 2012.

Was ist Internetbetrug?

Es mehren sich die Delikte rund um Computer und Internet. Der Großteil der Straftaten entfällt auf Betrugsdelikte – Betrügereien beim Anbieten von Waren und Dienstleistungen – Kreditkartenbetrug bis hin zum Identitätsdiebstahl.

Die häufigsten Arten von Betrug im Internet und wie Sie sich davor schützen können.

Betrug auf Verkaufsportalen

So gehen die Täter vor:
Die Täter bieten nichtexistente Waren über das Internet an. Die Opfer werden zur Vorauskasse aufgefordert – die Ware bzw. ihr bezahltes Geld sehen sie aber nie.

So verhalten Sie sich richtig:

- Überprüfen Sie, ob Sie Ihren Geschäftspartner kennen und ihn als seriös einschätzen. Versichern Sie sich, ob dieser auf der Internetseite eine Firmenadresse sowie eine Telefon- und eine Faxnummer hat.
- Lesen Sie immer das Kleingedruckte. Denn schon mit einem Mausklick stimmen Sie den Allgemeinen Geschäftsbedingungen Ihres Geschäftspartners zu.
- Geben Sie persönliche Daten nur sehr sparsam weiter. Dazu zählen die Kreditkartennummer, Geburtsdaten und Bankverbindungen. Wenn Sie persönliche Daten weitergeben müssen, dann nur auf verschlüsseltem Weg über sichere Verbindungen (zu erkennen an den Buchstaben „https“ in der Adresszeile der Website).
- Schicken Sie keinesfalls Bargeld oder Schecks an jemanden, bevor Sie nicht die Ware oder die Dienstleistung erhalten haben.

Phishing

So gehen die Täter vor:
Via E-Mail werden Internetuser aufgefordert, Konto-, Kreditkarten- und sonstige private Daten bekanntzugeben. Durch einen in der E-Mail angegebenen Link gelangt man auf eine gefälschte Website, die offiziellen Seiten von Banken oder Kreditkartenfirmen täuschend ähnlich sehen und auf denen dann die Daten eingegeben werden sollen.

So verhalten Sie sich richtig:

- Allgemein gilt: Anfragen zur Bekanntgabe von Kontodaten oder Kreditkartendaten werden von Bankinstituten, Kreditkartenfirmen und sonstigen seriösen Unternehmen nie in dieser Form gestellt.
- Wenn Sie E-Banking durchführen, verwenden Sie immer die Adresse Ihrer Bank oder das Lesezeichen des Browsers.
- Wenn Sie ein Phishing-Mail erhalten und bereits einen TAN-Code bekanntgegeben haben, setzen Sie sich sofort mit Ihrer Bank in Verbindung, um die TAN-Codes und PIN-Codes sperren zu lassen.

Spam-Mails mit Betrugsabsicht

So gehen die Täter vor:
Der Absender gibt in einer Massenmail vor, im Besitz einer hohen Geldmenge zu sein und ersucht um Unterstützung, um diesen Betrag ins Ausland transferieren zu können. Dafür wird Provision zugesichert. Eine weitere Betrugsform sind Gewinnverständigungen, die von Lotteriegesellschaften versandt werden und zur Vorauszahlung auffordern. Bei diesen Anboten erfolgt die Aufforderung zur Bekanntgabe von persönlichen Daten und zur Zahlung diverser Gebühren, die für die Freigabe des Geldes bzw. Gewinnes erforderlich sein sollen.

So verhalten Sie sich richtig:

- Reagieren Sie nie auf solche Angebote!
- Geben Sie keinesfalls persönliche Daten, Bankverbindungen und sonstige Daten bekannt, weil damit weitere Betrugshandlungen gesetzt werden könnten.

Partnervermittlungsbetrug

So gehen die Täter vor:
Beim Partnervermittlungsbetrug, dem Love Scam, wird der Benutzer in eine Affäre verwickelt und dann finanziell ausgebeutet. Die Kontaktaufnahme erfolgt oft über offizielle Internetportale. Nach Aufbau einer Vertrauensbasis und Zusage eines Treffens wird unter dem Vorwand einer Notsituation um finanzielle Unterstützung ersucht.

So verhalten Sie sich richtig:

- Schützen Sie im Netz Ihre eigene Identität.
- Einem ersten persönlichen Treffen sollten immer Telefonate vorausgehen.