

INFORMIEREN. AGIEREN. VORBEUGEN.



[Vom Smartphone bis zum Tablet-PC >](#)
[< Phishing - so können Sie sich schützen](#)

Gier und Neugier

Welche menschlichen Schwächen Internetbetrüger ausnutzen



Die psychologischen Tricks sind einfach, aber wirkungsvoll

© Renee Jansoa, fotolia

Tricks rund um vermeintlich unschlagbare Schnäppchen, verführerisch lukrative Jobangebote, Nachrichten mit angeblich top-aktuellen und intimen News über Promis oder verblüffend persönlich gehaltene Warnmeldungen – all das und noch viel mehr findet sich im Arsenal der Internetbetrüger. Die rasante technische Entwicklung und die offene Bereitschaft vieler Internetnutzer, persönliche Informationen preiszugeben, machen es den Gaunern zusätzlich leicht, mit ihren psychologischen Tricks erfolgreich zu sein.

Das Spiel mit der Sensationslust

„Wenn du das nicht liest, wirst du es bereuen“

Betrüger verschicken Nachrichten, in denen beispielsweise mit Anzeigen wegen frei erfundenen Straftaten gedroht wird oder die Vernichtung von Daten auf dem Rechner angekündigt wird. Auch vor Erpressungen mit angeblich belastendem Fotomaterial oder anderen vermeintlich unangenehmen Informationen scheuen Online-Kriminelle nicht zurück. Viele Betrüger wollen durch diese Aktionen ihre Opfer dazu bringen, infizierte Mailanhänge oder manipulierte Internetseiten zu öffnen, um dann beispielsweise Spionagesoftware auf fremden Rechnern zu platzieren. Oft handelt es sich aber auch um regelrechte Erpressungen, bei denen direkte Geldzahlungen gefordert werden.

Das Spiel mit der Neugier

„Brandneu – das musst du unbedingt sehen“

Betrüger verschicken Mails, MMS oder sonstige Nachrichten mit Anhängen oder platzieren Links in Social Networks, die zum Anklicken verleiten – wer das tut, findet allerdings nicht die gewünschte Information vor, sondern lädt Schadsoftware auf seinen Rechner.

In diese Kategorie fallen beispielsweise angebliche Fotos von Prominenten in intimen Situationen (etwa Nacktfotos von Britney Spears oder anderen Pop-Größen), vermeintliche Videoclips von Blockbustern wie „Harry Potter und der Halbblutprinz“ oder Links zu Youtube-Videos mit Spekulationen über die Ursache des plötzlichen Tods von Michael Jackson. Ebenfalls gerne genutzt von den Computerbetrügern: Nachrichten mit angeblichen Hintergrundinfos zu Epidemien wie Schweinegrippe oder SARS, zu dramatischen Unfällen wie dem Absturz eines Air France Airbus in den Atlantik oder – schon einige Jahre zurückliegend – Naturkatastrophen wie dem Tsunami in Südostasien oder dem Hurrikan Katrina.



Das Spiel mit der Geldgier

„Der Reichtum liegt doch auf der Straße“

Betrüger verführen ihre Opfer dazu, ihnen ihre Konten zur Verfügung zu stellen, um internationale Überweisungen abzuwickeln. Der eigentliche Zweck: Opfer durch Vorabzahlungen abzuzocken oder Gelder, die beispielsweise aus Phishing-Angriffen auf Bankkunden stammen, zu waschen. Wer auf die Offerte der Kriminellen einsteigt, verliert oft nicht nur Geld, sondern macht sich möglicherweise sogar strafbar. In diesem Bereich ist das „Social Engineering“ besonders gefährlich: Immer öfter stellen sich die Betrüger so präzise auf ihre Opfer ein, dass diese sich persönlich angesprochen fühlen und das Gefühl haben, tatsächlich ein seriöses, auf sie individuell abgestimmtes Angebot zu erhalten. Ein Klassiker in diesem Bereich sind die bereits legendären Aktivitäten der so genannten „Nigeria Connection“. In afrikanischen Staaten ansässige Betrüger versenden E-Mails, in denen die Opfer aufgefordert werden, ihr Konto gegen hohe Provisionen für Auslandstransaktionen zur Verfügung zu stellen.

Aktuelle Beispiele für betrügerische Aktivitäten im Internet finden Sie auf den Seiten des [Internetportals „Computerbetrug.de“](#)

Folgende Artikel könnten Sie auch interessieren:

-  [Ursachen und Formen von Cybermobbing](#)
-  [Falsche Freunde im Internet](#)

[Alle Artikel dieser Kategorie](#)

Weitere Infos zum Thema Internet und Mobil



Das Smartphone vor Schadsoftware schützen

Vorsicht beim App-Download!

Spannende Spiele, unterhaltsame Chatprogramme und clevere...[\[mehr erfahren\]](#)



Hoaxes und Kettenbriefe erkennen

Falschmeldungen im Internet

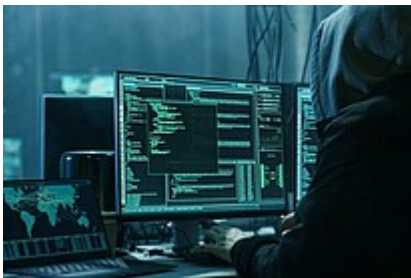
Sie erhalten eine Mail von einem Kollegen, in der eine Stiftung...[\[mehr erfahren\]](#)



Die Täter sehen alles

Digitales Stalking

Eine unangenehme Vorstellung: Jemand verschafft sich heimlich Zugriff...[\[mehr erfahren\]](#)



Im Team gegen Internetkriminelle

Die neue Abteilung Cybercrime im BKA

Seit April gibt es im Bundeskriminalamt (BKA) die neue Abteilung „CC“...[\[mehr erfahren\]](#)



Immer mehr Jugendliche sind gefährdet

Medien- und Internetsucht

Surfen, zocken, chatten: Nach Angaben der Bundeszentrale für...[\[mehr erfahren\]](#)

Cookie Einstellungen

- Statistiken
- Essentiell

Wir nutzen Cookies auf unserer Website, die in unserer [Datenschutzerklärung](#) beschrieben sind. Wir verwenden anonyme Statistiken, um unsere Website zu verbessern. Bitte unterstützen Sie unsere wichtige Präventionsarbeit und akzeptieren Sie alle Cookies. Vielen Dank!

Nur essentielle Cookies akzeptieren