

Wissen+Karriere

Magazin für Persönlichkeitsentwicklung, Motivation, Aus- und Weiterbildung

Dirk Kreuter, Speaker of the year

„Verkaufen bedeutet: Menschen (Kunden)
motivieren (Kauf-) Entscheidungen zu treffen!“



Grenzen sind zum Überschreiten da

Thomas Schlechter:
Wenn es schwierig wird,
versagt meist der Geist
zuerst, nicht der Körper



Im Keller des Lebens mit 28 Jahren

Dr. med. Petra Wenzel:
Psychisch gesunden
und mit Lebensfreude
stabil bleiben



LEBE motiviert

Matthias Herzog:
Wir lernen nicht mehr
für das Leben,
wir leben für das Lernen



So schützen Sie sich vor Internetkriminalität bei Online-Geschäften

Marco Löw: „Wechseln Sie öfters Ihre Passwörter“

Als langjähriger erfahrener Kriminalbeamter weiß ich um die hohe Zahl der Fälle von Internetbetrügereien zu Lasten der Verbraucher. Nicht ohne Grund haben viele Polizeipräsidien den Themenkomplex der Internetkriminalität aus den ursprünglich zuständigen Kriminaldienststellen ausgelagert und in den Zuständigkeitsbereich eigens gegründeter Spezialkommissariate eingegliedert. Während vor einigen Jahren Betrügereien im Internet noch von den allgemeinen Betrugskommissariaten mitbearbeitet wurden, ist es mittlerweile so, dass dies vielerorts allein schon quantitativ gar nicht mehr zu leisten wäre.

Die polizeiliche Kriminalstatistik weist für 2010 ca. 180.000 Fälle allein von Internetbetrug auf, der wiederum nur eine Form der vielfältigen Internetkriminalitätsformen darstellt. Die Tendenz ist dabei deutlich steigend. Durch das Bundesverfassungsgerichtsurteil zur Vorratsdatenspeicherung dürften sich die ohnehin von Jahr zu Jahr ansteigenden Fälle von Internetbetrügereien nochmals deutlich verschärfend in der Kriminalstatistik 2011 niederschlagen. Wenn man hierbei noch berücksichtigt, dass Dunkelziffern in der Kriminalstatistik nicht auftauchen, dann ist die Gefahr Opfer eines Internetbetrugs zu werden durchaus gegeben.

Der Klassiker ist natürlich nach wie vor der Verkauf von Ware über eine Internetbörse, bei denen der Käufer gezahlt, aber der Verkäufer nicht geliefert hat. Dabei besteht das Problem längst nicht nur bei Privatverkäufen. Immer öfter verkaufen auch Firmen günstige Artikel, ohne die Ware liefern zu können. Immer wieder werden Firmen extra zu diesem Zweck gegründet und dann auch



Wechseln Sie öfters Ihre Passwörter.

schnell wieder aufgelöst. Ziel dieser Betrüger ist es, durch Schnäppchenangebote eine kurzfristige Zahlungswelle auszulösen, die dann schnell abgeschöpft wird. Oftmals auch zur Beschleunigung der Zahlungseingänge mittels zeitlich begrenzter Schnäppchenangebote.

Viele Kunden machen den Fehler, bei Internetauktionen alleine aufgrund der Verkäuferbewertungen auf die Seriosität des Angebotes zu schließen. Dabei lassen sie außer Acht, dass oftmals gehackte Accounts von tatsächlich seriösen Personen durch Betrüger eingesetzt werden. Gehackte Accounts stellen eine vielfache Gefahrenquelle für Sie als Verbraucher dar. Wird beispielsweise Ihr eigener Account gehackt, so können Täter sowohl auf Ihren Namen Bestellungen aufgeben als auch in Ihrem Namen Verkäufe tätigen. Kaum bekannt ist, dass es auch immer wieder

Fälle gibt, bei denen es dem Täter nicht um eine Bereicherungsabsicht, sondern um Rache oder Stalking geht. So sollte man auch bei Trennungen oder Scheidungen vorsorglich schnellstmöglich die Kennwörter ändern. Große Liebe kann schnell in große Rache umschlagen, wenn ein Herz gebrochen wird.

Accounts werden jedoch nicht nur auf regulärem Wege wie zum Beispiel durch unsichere Passwörter gehackt, sondern durchaus auch auf elegantere Art und Weise. Erkennen Account-Inhaber beispielsweise so genannte Phishingmails nicht rechtzeitig, so geben sie den Betrügern bereitwillig, wenn auch unfreiwillig ihre Daten.

Selbst nach Abschluss einer Auktion haben Betrüger noch Handlungsspielräume. Beispielsweise kann dem überbotenen Auktionsteilnehmer der

gleiche Artikel nochmals zum direkten Kauf angeboten werden. Dadurch umgehen Betrüger durch den Onlinehändler installierte Sicherheitsmaßnahmen.

Beurteilen Sie die Seriosität eines Verkäufers daher nicht nur anhand der Anzahl der positiven Bewertungen, sondern setzen Sie diese ins Verhältnis zur Dauer seiner Registrierung. Achten Sie auch darauf, welche Artikel zu welchen Preisen bisher durch den Verkäufer verkauft wurden.

Ein betrügerischer Verkäufer kann sich nicht über einen langen Zeitraum mit einem betrügerischen Account halten. Es gibt aber auch durchaus Betrüger, die erst mal ihren Keller entrümpeln und dadurch eine Vielzahl von einwandfreien Verkäufen tätigen, um für eine gute Reputation zu sorgen. Im Anschluss verkaufen sie dann wertvolle Ware an Kunden, liefern aber nicht.

Weil die meisten Menschen ehrlich sind, ist ihnen die Denkweise von Betrügern nicht vertraut. So können sie sich beispielsweise oft nicht vorstellen, dass ein Betrüger wegen verhältnismäßig geringen Geldbeträgen eine Straftat riskiert.

Als Betrugsermittler hatte ich im Rahmen einer personellen Aushilfe über einen längeren Zeitraum auch eine Vielzahl von Internetbetrügereien bearbeitet. In einem Fall bot der Verkäufer ein wertvolles vergoldetes Feuerzeug zu einem äußerst attraktiven Preis an, nämlich zu 10 Euro. Er verkaufte aber ein und dasselbe Feuerzeug bundesweit über fünftausend Mal. Nur drei Geschädigte haben Anzeige erstattet, da den meisten Betrugsoffern aufgrund des niedrigen Preises der Aufwand einer Anzeigenerstattung zu hoch erschien. Der Betrüger hätte es beinahe geschafft ohne Anzeige innerhalb kürzester Zeit um 50.000 Euro reicher zu werden.

Auch ist es so, dass viele Betrüger nicht in geordneten Verhältnissen leben. Manche denken nur von heute auf morgen und begehen Straftaten selbst

dann, wenn sie wissen, dass es nur eine Frage der Zeit ist, bis sie von einer Anzeige ereilt werden.

Anfangen sollte das Thema der Internetsicherheit schon mal beim richtigen Umgang mit Passwörtern. Gerade hier lauert ein enorm hoher Risikoherd. Viele Menschen können oder wollen sich nicht mehrere Passwörter auf einmal merken und verwenden daher beispielsweise bei Ebay, Amazon und anderen Anbietern immer dasselbe Passwort. Besonders fatal ist es dabei, wenn das Passwort zudem auch nicht sicher ist. Wird das Passwort einmal geknackt, können Betrüger damit einen ungeheuren Schaden anrichten. Deshalb sollten Sie unbedingt für jeden Account auch ein eigenes Passwort verwenden und dieses sollte jeweils den Mindeststandards für sichere Passwörter genügen. Das Passwort sollte also aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen bestehen und mindestens acht Zeichen lang sein.

Mit kleinen Tricks kann man sich auch sichere Passwörter gut merken. Beispielsweise könnte ich ISUS!011211: verwenden. Bestehend aus dem Vornamen meiner ersten Freundin rückwärts gesprochen, dem Datum meines Autokaufs und zwei Sonderzeichen. Für einen zweiten Account würde ich aber auf ein anderes Muster zurückgreifen. Vielleicht den Titel meines Lieblingsfilms und das Hochzeitsdatum meiner Mutter. Einen direkten Bezug zu Ihrer Person darf das Passwort auf keinen Fall aufweisen, damit es nicht erraten werden kann.

Wichtig ist es auch die Passwörter spätestens alle drei Monate zu wechseln. Mag es noch zu bequem sein, denken Sie daran, dass Bequemlichkeit und Vertrauensseligkeit Menschen schnell zu Betrugsoffern werden lassen.

Bitte notieren Sie sich auch nirgends Ihre Passwörter, auch nicht in einer Datei auf Ihrem Computer. Wenn es gar nicht anders geht und Sie sich Ihre Passwörter nicht merken können, dann benötigen Sie ein gutes und sicheres Versteck in Ihrer

Wohnung. Ihre Geldbörse, Handtasche oder Aktentasche ist sicher eine der schlechtesten Aufbewahrungsorte für sensible Daten, denn die Gefahr von Verlust oder Diebstahl ist allgegenwärtig.

Versuchen Sie sich bestmöglich über den Verkäufer zu informieren. Alle wesentlichen Daten des Verkäufers wie Identität, Anschrift, Garantie-, Widerrufs- und Rückgaberecht sollten durch diesen transparent gemacht werden. Der Bundesverband des Deutschen Versandhandels vergibt in Kooperation mit dem EHI Retail Institute das Gütesiegel „Geprüfter Online Shop“. Führt ein Händler dieses oder ein ähnlich fundiertes Siegel, dann ist dies für die Vertrauensbildung zwischen Kunde und Verkäufer sicherlich als sehr positiv zu bewerten, wenngleich dies nicht als alleinige Grundlage zur Verkäufereinschätzung herangezogen werden sollte.

Vorsicht ist bei Käufen über Internetplattformen immer geboten, wenn der Preis für ein Produkt ohne nachvollziehbare Gründe ungewöhnlich günstig ist. Denken Sie immer dran, dass grundsätzlich niemand etwas zu verschenken hat und jedes Produkt ein gewisses Mindestpreisniveau haben muss. Andernfalls muss man sich die Frage stellen, aus welchen Gründen der Verkäufer sich mit weniger Bezahlung zufrieden gibt als es angemessen wäre und warum er so günstig produzieren bzw. einkaufen kann.

Ein weiteres Problem sind im Ausland ansässige Verkäufer. Es ist sowohl zivilrechtlich als auch strafrechtlich schwierig gegen einen im Ausland ansässigen Anbieter vorzugehen. Selbst wenn Sie die korrekten Daten der Person haben sollten, wäre es mit einem enormen finanziellen und organisatorischen Aufwand verbunden, zivilrechtlich zu klagen. Strafrechtlich ist es ebenfalls schwierig, weil es außer bei sehr schwerwiegenden Straftaten kaum möglich ist, den Beschuldigten vor ein deutsches Gericht zu bekommen und die ausländische Justiz nur selten zu Ihrer Zufriedenheit arbeiten wird. Bei Geschäftsabwicklungen mit im Ausland ansässigen Verkäu-

fern müssen Sie sich auch unbedingt über ggf. entstehende Zusatzkosten wie beispielsweise die genaue Höhe von Steuern und Zollgebühren informieren, wenn Sie keine bösen Überraschungen erleben wollen.

Wenn es ans Bezahlen geht, so führen Sie Transaktionen nur über sichere Kanäle durch. Besonders eignen sich dabei Zahlungsweisen per Kreditkarte, Bankeinzug, Rechnung und PayPal. Bitte tätigen Sie auf gar keinen Fall eine Bezahlung mittels Bargeld-Transfer, wie beispielsweise über Western Union. Ein Bargeld-Transfer kommt nur gegenüber solchen Personen in Frage, denen Sie besonders vertrauen können. Dies wird zwischen Verkäufern und Käufern, außer im privaten Rahmen, höchst selten der Fall sein.

Bezahlen Sie aber grundsätzlich immer erst nach Erhalt der Ware. Zwar gibt es nicht wenige Verkäufer, die auf einer Vorabüberweisung bestehen, aber Sie sollten sich über das Risiko eines solchen Geschäftes immer im Klaren sein. Liefert der Verkäufer nicht, so können Sie das Geld nicht zurückholen und müssen die Rückerstattung des Betrages oftmals auf dem Zivilrechtsweg erlangen. Bei Nachnahmebezahlungen stellt sich ein ähnliches Problem. Sie müssen bei dieser Bezahlform die Ware bezahlen, bevor Sie sie prüfen konnten. Ist die Lieferung fehlerhaft, werden Sie womöglich Schwierigkeiten haben Ihr Geld oder Teilbeträge wieder zurückzubekommen.

Wenn Sie dagegen eine Einzugsermächtigung erteilen, können Sie im Regelfall das Geld mindestens sechs Wochen lang, je nach AGB der Bank, wieder zurückholen. Es sollte übrigens selbstverständlich sein, dass Sie Ihre Kontoauszüge regelmäßig auf unberechtigte Abbuchungen überprüfen, um ggf. noch die Möglichkeit zu haben erfolgreich Gegenmaßnahmen zu ergreifen.

Wenn Sie Daten übermitteln, dann muss diese Übermittlung sicher sein. Vermeiden Sie daher nach Möglichkeit solche Anbieter, die eine verschlüsselte Datenübertragung nicht ermöglichen.

Ein kleines Schlosssymbol in der unteren Browserleiste oder das Kürzel https:// in der Adresszeile des Browsers geben Hinweise auf eine sichere Datenübermittlung.

Seien Sie misstrauisch und äußerst vorsichtig, falls Sie per E-mail aufgefordert werden, vertrauliche Daten wie Passwörter oder Infos zu Ihrer Kreditkarte in ein Formular oder per Link zu übertragen. Diese Art der Datenabfrage ist unter seriösen Unternehmen höchst unüblich.

Lassen Sie sich nicht von gut gemachten Homepages blenden. Entscheidend sollte nicht die Qualität der Homepage, sondern deren Inhalt sein. Eine Homepage hat im Grunde nur den Zweck zu informieren. Fragwürdig ist es, wenn das Impressum auf der Homepage versteckt wird oder wenn es nicht die volle Identität des Verantwortlichen und seiner Firma preisgibt. Kaufen Sie beispielsweise auf gar keinen Fall, wenn der Verkäufer im Impressum seiner Firma nur per Postfach genannt ist, oder nur eine Postfachadresse der Firma, womöglich auch noch im Ausland, existiert. Sämtliche Pflichtangaben, die ein Onlineshopbetreiber machen muss, können in § 6 Telemediengesetz nachgelesen werden.

In diesem Artikel konnte ich Ihnen nur einen kleinen Ausschnitt zu der Thematik präsentieren. Meine Intention war es hierbei, Ihnen die wichtigsten Informationen zur Thematik zu vermitteln. Selbstverständlich kann ein solcher Artikel jedoch keine persönliche Schulung oder Beratung für den Einzelfall ersetzen, weshalb ich um Verständnis bitte, dass ich keine Haftung für die in diesem Artikel genannten Ratschläge übernehmen kann. Ich kann Ihnen aber versichern, dass ich die in diesem Artikel genannten Tipps nach bestem Wissen und Gewissen zusammengestellt habe. Ich hoffe, dass es mir gelungen ist, Sie für die Thematik zu sensibilisieren. Sensibilisierungen tragen einen erheblichen Teil dazu bei, Menschen davor zu bewahren, Opfer von Straftaten zu werden, ganz gleich ob es sich hierbei um Internetkriminalität oder andere Delikte handelt. ■



Marco Löw

ZUR PERSON

Marco Löw, Autor und dreifach ausgezeichnete Vernehmungsexperte, sammelte seinen Erfahrungsschatz in langjähriger Tätigkeit bei der Kriminalpolizei. Er ist Inhaber von Löw & Partner, einem Unternehmen für forensisches Präventionsmanagement und der deutsche Experte für taktische Gesprächstechniken zur Sachverhaltsklärung und Glaubwürdigkeitsüberprüfung. Löw ist Mitglied der Top-100-Trainer (Trainers Excellence) bei Speakers Excellence. Er coacht und trainiert Personalverantwortliche und Führungskräfte in forensischen Befragungstechniken.



KRIMINALISTISCHE BEFRAGUNGSTAKTIKEN FÜR DIE WIRTSCHAFT

Verlag Books on Demand (BoD)
ISBN: 978-3000334177

39,95 EURO