Gestohlene Identität

Online-Kriminalität. Internet-Betrugsdelikte unter missbräuchlicher Verwendung persönlicher Daten steigen sprunghaft an. Die Täter lassen sich immer wieder neue Maschen einfallen.

Andreas S. aus Mistelbach bekommt eine besorgniserregende E-Mail von seiner guten Freundin Martina H. Darin schreibt sie, dass sie sich gerade in Barcelona aufhält und ausgeraubt worden ist. Alles Wichtige ist weg: Geldbörse, Pass und Handy. Nun braucht sie dringend Geld, um das Hotel und den Rückflug zu finanzieren. Ob er ihr kurzfristig aushelfen und 1.600 Euro auf ein Konto bei Western Union überweisen könne, will sie wissen. Andreas grübelt kurz und wählt dann ihre Handynummer. Tatsächlich geht Martina selbst ans Telefon und ist recht erstaunt, als Andreas sie fragt, ob sie denn ihre Wertsachen wiederbekommen habe. Es stellt sich heraus, dass sie sich nicht in Barcelona aufhält, sondern wie gewohnt an ihrem Arbeitsplatz in Wien. Bestohlen worden ist sie auch nicht.

Ein klassischer Fall von Identitätsdiebstahl im Netz: Jemand hat sich in den E-Mail-Account von Martina gehackt und die Nachricht an ausgewählte Kontaktpersonen aus ihrem Umfeld gesendet – in der Hoffnung, sich eine stattliche Summe zu ergaunern.

Die Zahl von Betrugsdelikten wie diesem ist in den letzten Jahren in die Höhe geschnellt. Die Fälle von Cybercrime häufen sich. Und sie spielen sich nicht nur im anonymen Darknet ab (das durch solche Vorfälle in Verruf gekommen ist), sondern auch im von uns allen genutzten Clearnet, das wir als „das Internet" kennen. Im Jahr 2017 gab es laut einer Statistik des österreichischen Bundeskriminalamtes 16.804 Anzeigen zu Kriminalität im Netz – ein Plus von 28 Prozent gegenüber dem Jahr davor. Wobei Experten von einer hohen Dunkelziffer ausgehen.

Einkauf auf fremde Rechnung

Einen riesigen Brocken davon machen Bestellbetrügereien beim Online-Shopping aus. Dann flattern beispielsweise Mahnungen ins Haus, in denen es heißt, man möge gefälligst die Rechnung für ein sündhaft teures Designerkleid begleichen. Nur dass man selbiges nie gekauft hat. Auch bei diesem Beispiel hat sich jemand eine Identität aus dem Internet angeeignet und hat unter diesem Namen eingekauft. Das hierzulande sehr beliebte Bezahlen auf Rechnung macht's möglich. Manch ein Versandhändler bietet diese Option auch bei Neukunden an. Folglich ist es kein Problem, Ware unter Angabe des Namens einer fremden Person zu ordern, wobei sich Liefer- und Rechnungsadresse unterscheiden.

Für die Online-Händler selbst gibt es bis dato noch kein angemessenes elektronisches Verfahren, mit dem sie eine hundertprozentig sichere Identitätsprüfung durchführen könnten.

Phishing und Fake-Shops

Sind Name und Wohnadresse bekannt, droht aber auch von anderer Seite Gefahr: Phishing (gebildet aus den englischen Wörtern „password" und „fishing" = angeln) werden Versuche, Daten zu ergaunern, auf Neudeutsch genannt. Die Verbrecher probieren es über diverse Wege: über Mails oder Kurznachrichten oder über offen zur Schau gestellte Informationen auf Facebook und Co. Nicht zu vergessen die vielen gefälschten Webseiten, die nur dem Zweck dienen, den Besuchern persönliche Daten zu entlocken. Nachrichten, die einen dazu verleiten sollen, möglichst viel von sich preiszugeben, wirken jedenfalls umso authentischer, je mehr korrekte Daten sie bereits enthalten. Die Falle muss also nicht zwingend gleich beim ersten Mal zuschnappen. Im Darknet werden derlei Daten als Ware angeboten. Der Handel mit gestohlenen Identitäten hat sich zu einem lukrativen Geschäftsmodell entwickelt.

Fake-Seiten anderer Art gibt es im E-Commerce-Bereich leider zuhauf. In gefälschten Online-Shops werden begehrte Waren zu äußerst günstigen Preisen angeboten. Wer bezahlt, bekommt bestenfalls minderwertige gefälschte Produkte zugesandt. In der Regel sieht er aber weder die Ware, noch erhält er sein Geld wieder. Meist verschwinden diese Shops rasch wieder, tauchen aber in vergleichbarer Gestalt unter neuem Namen und mit einer anderen Internetadresse wieder auf. Ein überprüfbares Impressum haben sie nicht und die Allgemeinen Geschäftsbedingungen (AGB) bestehen aus einer Sammlung nichtssagender Texte. Auch fehlt in der Regel die https-Verschlüsselung. Dafür locken sie mit Angeboten, bei denen sich selbst die gewieftesten Schnäppchenjäger die Augen reiben. Besonders raffiniert sind „Shops" mit Kurzzeit-Sonderangeboten, denn die erzeugen Druck und verleiten zu unüberlegten Käufen. Grundsätzlich gilt: Ein Preis,

VKI-Tipps für den sicheren Online-Einkauf

Versuchen Sie festzustellen, ob der Anbieter seriös ist: Gibt es eine Anschrift, ein Impressum sowie verständliche AGBs und eine Datenschutzerklärung? Googeln Sie nach dem Anbieternamen und allfälligen (glaubhaft klingenden) Erfahrungsberichten und Bewertungen anderer Kunden.

Seien Sie skeptisch, wenn Verkäufer die Ware ausschließlich auf Vorkasse anbieten. Sicherer ist die Bezahlung mit Kreditkarte, PayPal, Nachnahme oder Zahlschein. Verwenden Sie bei PayPal jedoch keinesfalls die Option „Geld an Freunde oder Familie senden". Hier gilt nämlich der PayPal-Käuferschutz nicht.

Hände weg von Bargeldtransfer-Diensten wie Western Union, MoneyGram & Co!

Die Übertragung persönlicher Daten bei Käufen im Netz sollte verschlüsselt erfolgen. Das ist an dem Kürzel https in der Adresszeile des Browsers und einem Vorhängeschloss-Symbol erkennbar.

Kaufen Sie Markenware entweder direkt beim Produzenten oder von ihm lizensierten Händlern.

Zertifikate und Gütesiegel wie „Trusted Shops", das Österreichische E-Commerce-Gütezeichen oder das deutsche EHI-Siegel sind mangels einheitlicher europaweiter Regelung bedingt hilfreich.

Zum möglichen Abgleich gibt es eine (nicht vollständige) Liste von Fake-Shops im Internet unter www.watchlist-internet.at/news/liste-betruegerischer-online-shops/. Besuchen Sie außerdem unser Forum „Spam, Phishing, Betrug" unter www.konsument.at/jforum/forums/list.page.

der zu schön klingt, um wahr zu sein, ist in der Regel auch nicht reell.

Was tun, wenn's passiert ist?

Wenn Sie Opfer eines Betrugs geworden sind, bei dem Ihre Identität missbräuchlich verwendet wurde und/oder Sie einen wirtschaftlichen Schaden erlitten haben, sollten Sie den Fall bei der Polizei anzeigen. Falls es sich um Zahlungen mit Bankomat- oder Kreditkarte handelt, ist dringend zu empfehlen, den Vorfall der Bank bzw. dem Kartenausgeber zu melden. Dort können Sie auch die Rückbuchung der missbräuchlichen Umsätze veranlassen. Ebenfalls wichtig: Stellen Sie am Wochenende bzw. außerhalb der Öffnungszeiten einen Kartenmissbrauch fest, rufen Sie umgehend die Sperrhotline an!

Foto: Rawpixel.com/Shutterstock.com

VKI-Tipps zum Schutz der digitalen Identität

Egal ob Computer oder Smartphone: Halten Sie das Betriebssystem und alle Anwendungen und Apps stets mithilfe von (automatischen) Updates auf dem neuesten Stand.

Firewall und Virenschutz sollten auf jedem Computer eine Selbstverständlichkeit sein, der Virenschutz auch auf dem Smartphone (siehe auch www.konsument.at/test-sicherheitsapps012018).

Nutzen Sie den Spam-Filter Ihres E-Mail-Accounts bzw. Ihres E-Mail-Programms. Öffnen Sie keine Datei-Anhänge von unbekannten Mail-Versendern und antworten Sie nicht auf Spam.

Achten Sie auf die Passwort-Sicherheit. Dazu gehört, nicht für jede Anwendung dasselbe Passwort zu wählen (siehe auch www.konsument.at/passwortmanager042018).

Geben Sie nicht zu viel von sich preis. Aktionen wie das Hochladen, Liken oder Kommentieren von Beiträgen in sozialen Medien immer vorher überdenken.

Ändern Sie die Einstellungen in den sozialen Medien dahin gehend, dass ein Maximum an Privatheit gewährleistet wird (siehe auch www.konsument.at/computer-telekom/facebook-eine-spur-privater).

Gehen Sie sorgsam mit Adresse, Mail-Adresse, Bank- und Kreditkartendaten um: weder auf unseriösen Webseiten eintragen noch im Netz veröffentlichen, per WhatsApp oder per E-Mail versenden.

Im Zweifelsfall nutzen Sie eine Wegwerf-Mail-Adresse. Sie wird nach einer vordefinierten Anzahl von Zusendungen bzw. nach dem Ablaufen einer gewissen Zeitspanne ungültig (www.spamgourmet.com; www.byom.de; https://tempr.email).

Tätigen Sie keine Bankgeschäfte, wenn Sie sich in einem öffentlichen WLAN befinden.

MEHR ZUM THEMA

Handbuch Datenschutz. Wo die Datenkraken in unseren Alltag eingreifen und was Sie tun können, um Ihre Privatsphäre zu wahren (204 Seiten, € 19,90, www.konsument.at/hb-datenschutz).

Rat und Hilfe für Verbraucher in Europa
ECC-Net
Finanziell unterstützt durch die Europäische Union

Dieser Artikel wurde aus den Mitteln des Verbraucherprogramms der Europäischen Union (2014 – 2020) gefördert.

VKI