Liebesbetrug: Täter täuschen große Gefühle vor und machen lukrative Geschäfte mit der Einsamkeit vieler Internetnutzer.

Wenn Betrüger ins „Netz“ gehen

Daten, Emotionen, Mausklicks – mit digitalen Tricks machen Internetbetrüger alles Mögliche zu Geld. Etwa zwei Drittel der Zahl der angezeigten Cybercrime-Delikte sind Betrugsfälle im Internet.

In Zeiten, in denen Finanzgeschäfte zu großen Teilen im Internet abgewickelt werden, ist Erna S. nicht überrascht, als sie in ihrem E-Mail-Postfach die Aufforderung ihrer Bank findet, sie möge ihre Daten aktualisieren. Ein Link in der Nachricht führt Erna S. auf die Internetseite ihrer Bank. „Lieber Kunde, bitte geben Sie uns zur Aktualisierung Ihres Profils Ihre Benutzerdaten bekannt“, heißt es dort in roten Buchstaben. Frau S. tippt in das auszufüllende Formular neben Namen und Wohnadresse auch Verfügernummer und Passwort ihres Online-Banking-Accounts.

16.804 Anzeigen wegen Cyber-Kriminalität sind 2017 bei der Polizei eingegangen. In der Kriminalstatistik 2017 war in diesem Bereich der höchste Anstieg zu verzeichnen. Bei knapp zwei Drittel der Cybercrime-Delikte (11.761) handelt es sich um Betrugsfälle im Internet – um rund 3.000 mehr als 2016. Betrügereien im Internet werden als „Cybercrime im weiteren Sinn“ klassifiziert, oder als „cyber-enabled Crime“ bezeichnet, sagt Mag. (FH) Claus-Peter Kahn, der im Bundeskriminalamt das Büro für Betrug, Fälschung und Wirtschaftskriminalität leitet. „Rechtlich unterscheiden wir nicht zwischen Betrug und Internetbetrug, cyber-enabled Crime umfasst Delikte, bei denen das Internet eingesetzt wird, um eine Straftat zu begehen oder vorzubereiten. Darunter fallen Internetbetrug, Cybermobbing oder die Verbreitung von Kinderpornografie im Darknet“. Angriffe auf Computersysteme oder Infrastrukturen durch Viren, Trojaner oder Hacking sind im Gegensatz dazu als „Cybercrime im engeren Sinn“ zu verstehen.

Datenfischen. Im Fall von Frau S. war der Absender der Mail keine Bank, hinter der Nachricht stecken Internetbetrüger. Mit dieser Betrugsmasche haben es Kriminelle auf geheime Daten wie Passwörter für Online-Shops, soziale Netzwerke oder Online-Banking-Accounts abgesehen.

Beim „Phishing“ – ein Kunstwort aus den englischen Begriffen für Passwort ernten und fischen (password harvesting fishing) – versuchen Betrüger über gefälschte Webseiten, E-Mails oder Chatnachrichten an persönliche Daten der Benutzer zu gelangen. Sie betreiben Daten- und im Fall von Erna S. auch Identitätsmissbrauch. Die Absender der Phishing-Nachricht können in ihrem Namen Online-Überweisungen tätigen.

Post von der Bohrinsel. Gemeinsamkeiten, Zuneigung, Liebe – um an das Geld ihrer Opfer zu kommen, täuschen Betrüger große Gefühle vor. Liebesbetrug ist eine der gängigsten Betrugsformen im Internet. Mit Versprechen auf

Fotos: Wordley Calvo Stock/Fotolia

ein besseres, gemeinsames Leben erschleichen sich die Täter das Vertrauen ihrer Opfer und machen lukrative Geschäfte mit der Einsamkeit vieler Internetnutzer. Nationalität und Geschlecht spielen keine Rolle. „Vom reichen Ölbauingenieur, der ihnen ein Leben in Luxus verspricht, bis zum Mädchen aus einfachen Verhältnissen, das sie in den Westen holen sollen, die Täter sind in der Regel kreativ und anpassungsfähig“, berichtet Kahn.

Opfer würden horrende Summen an Angebetete überweisen, denen sie in der Realität nie begegnen. „Einmal ist es der Reisepass, der finanziert werden muss, ein anderes Mal das Visum, beim nächsten Mal trennt sie nur noch ein Zöllner von einem Treffen mit der Internetbekanntschaft, das später durch einen teuren Krankenhausaufenthalt wieder platzt.“ Laut dem Kriminalisten gebe es Tausende unterschiedliche Vorgehensweisen, die alle eines gemeinsam haben: „Die Betrüger hören erst dann auf, wenn das Opfer kein Geld mehr hat.“

Gewinne, die Verlust bedeuten. Gefälschte Gewinnspiele und falsche Gewinnversprechen gehören wie der Liebesbetrug dem Vorauszahlungsbetrug an. Egal, ob die Menschen dazu aufgefordert werden, ihre Kontodaten für eine Teilnahme preiszugeben, oder ob Nachrichten über vermeintliche Gewinne die Empfänger dazu verleiten, „Spesen“ zur Überweisung des versprochenen Gewinnes zu bezahlen – Menschen

Claus-Peter Kahn: „Die Betrüger hören erst dann auf, wenn das Opfer kein Geld mehr hat.“

werden mit ausgeklügelten Tricks um ihr Erspartes gebracht. Anstatt, wie versprochen, mit einem großen Plus am Konto, finden sie sich später häufig bei der Schuldenberatung wieder.

Falsche Ware. Auch „Fake-Shops“ erfreuen sich im Internet an hohen Klickzahlen. Angelockt werden Käufer beispielsweise mit Angeboten von extrem günstigen Markenprodukten. Im besten Fall sind die Produkte billige Nachahmungen, im schlimmsten Fall existieren sie überhaupt nicht. In der Regel handelt es sich bei den Anbietern nicht um Einzeltäter, sondern um organisierte kriminelle Gruppen mit arbeitsteiliger Vorgangsweise. „Da sich der Handel in den letzten Jahren immer mehr ins Internet verlagert hat, werden auch die Vorgangsweisen der Internetbetrüger immer professioneller“, sagt Kahn. „Arbeitsteilig heißt dann, dass es Leute gibt, die nur Kreditkartendaten ‚phischen‘, andere generieren Datensätze aus Adressdaten und Dritte hosten den Server, über den die Homepages online gestellt werden.“

Opfer sucht Täter. „Beim Betrug gibt es keine klassischen Opfer“, sagt Kahn. Generell gilt: Jede und jeder ist angreifbar. Das Opfer suche sich seinen Täter in gewisser Weise selbst. „Der eine fällt auf ein falsches Gewinnversprechen herein, weil er sich schon länger ein neues Auto wünscht, die andere muss überraschend ausziehen und mietet zu einem vermeintlich günstigen Mietpreis eine Wohnung, die nicht am Markt ist. Die Betrüger sind meistens gut, in dem was sie tun, und stellen sich perfekt auf die Bedürfnisse der Opfer ein.“

Weltweites Netz. Weil die Täter ständig ihre Vorgangsweisen ändern, müssen sich auch die Ermittler immer wieder an neue Gegebenheiten anpassen. Um Internetbetrüger aufzuspüren, arbeitet das Bundeskriminalamt eng mit internationalen Behörden zusammen. Im Gegensatz zu Trickbetrügern, die von Tür zu Tür gehen und die Hilfsbereitschaft der Menschen ausnutzen, sind die Spuren von Betrügern im Netz geografisch schwer nachvollziehbar. „Die Weiten des Internets und des Darknets dienen als Verstecke und erschweren die Verfolgung der Täter“, sagt Kahn. Umso größer sei der Erfolg, wenn eine international agierende Tätergruppierung ausgehoben werde.

Anna Freinschlag

INTERNETBETRUG

Präventionstipps

• *Achtung bei der Weitergabe von Informationen*
Achten Sie darauf, welche Daten Sie weitergeben. Zur Vorbereitung von Betrugshandlungen versuchen Täter häufig die Kontaktaufnahme via Anruf oder E-Mail. Geben Sie Ihre Kartendaten im Zweifelsfall nicht weiter. Achten Sie immer auf eine sichere Verbindung und übermitteln Sie niemals Ihre Kartendaten über eine unverschlüsselte E-Mail.

• *Die eigene Identität schützen*
Schützen Sie Ihre Identität im Netz. Sämtliche von Ihnen bekannt gegebenen persönlichen Daten im Internet oder in sozialen Medien erleichtern das Vorhaben der Täter. Übermitteln Sie niemals Kopien von persönlichen Dokumenten an Unbekannte. Bei Internetbekanntschaften sollten einem ersten persönlichen Treffen immer Telefonate vorausgehen und sie sollten immer an öffentlichen Orten stattfinden. Scheuen Sie sich nicht, im Ernstfall Anzeige zu erstatten.

• *Anbieter überprüfen*
Informieren Sie sich über den Verkäufer. Vergewissern Sie sich, dass Identität und Anschrift des Anbieters oder Garantie- und Gewährleistungsbedingungen online leicht auffindbar und verständlich sind. Hilfreich bei der Einschätzung des Anbieters sind auch Bewertungsprofile, wie sie bei Online-Marktplätzen üblich sind.

• *Vorsicht bei Gratisangeboten*
Seien Sie bei „Gratis“-Angeboten stets misstrauisch, besonders wenn Sie persönliche Daten angeben müssen – dieser Grundsatz gilt auch im Internet. Oft handelt es sich um Lockangebote, bei denen später laufende Kosten entstehen. Antworten Sie auch nicht auf dubiose E-Mail-Versprechungen mit ungewöhnlich hohen Profiten und löschen Sie derartige E-Mails.

• *„Watchlist Internet“*
„Watchlist Internet“ ist eine Plattform zu Internetbetrug und betrugsähnlichen Online-Fallen. Dort können Sie sich unter *www.watchlist-internet.at* über aktuelle Betrugsfälle wie zum Beispiel gerade im Umlauf befindliche Phishing-Mails informieren.

FOTO: GERD PACHAUER