Geschäfte mit der Angst

Kriminelle nutzen die Ängste und Sorgen der Bevölkerung während der Corona-Epidemie aus, um daraus Profit zu schlagen. Gefährdet sind besonders ältere Menschen.

Die Covid-19 Pandemie löst in den Menschen nicht nur Unsicherheiten, sondern auch Ängste aus. Betrüger versuchen, über verschiedene Kommunikationskanäle, wie E-Mails, *WhatsApp*-Gruppen oder Online-Partnerbörsen mit ihren Opfern Kontakt aufzunehmen. Mag. (FH) Claus Kahn, Büroleiter im Bundeskriminalamt für Betrug, Fälschung und Wirtschaftsdelikte, warnt vor den Betrügern und ersucht um erhöhte Achtsamkeit, vor allem bei älteren Menschen.

Enkel- oder Neffentrick. Beim Enkel- oder Neffentrick suchen die Betrüger im Telefonbuch nach alt klingenden Vornamen, wie Hildegard, Lieselotte, Josef oder Wilfried und solche, wo unter Umständen nur eine Festnetznummer angegeben ist. Die Täter rufen an, geben sich als Angehörige aus und täuschen meist eine Notsituation vor. „Durch eine geschickte Gesprächsführung mit gezielten Rückfragen wird das Gespräch so geleitet, dass am Ende die Personen zu einer Übergabe von Geld und Wertgegenständen verleitet wird“, erklärt Kahn. Zumeist wird Geld für eine Behandlung oder eine notwendige Anschaffung oder für die Rückkehr aufgrund der Corona-Krise benötigt. „Wie wir sehen, sind die Täter dabei sehr erfinderisch, gerne werden Bezüge zu aktuellen Themen hergestellt, um noch mehr die Dringlichkeit und Wichtigkeit zu unterstreichen“, führt Kahn weiter aus.

Der „Falsche-Polizisten-Trick“ ist eine weitere Form des Trickbetrugs. Die Betrüger gehen ähnlich wie beim Enkel- oder Neffentrick vor. Sie suchen sich eine Telefonnummer aus dem Telefonbuch und kontaktieren ihr potenzielles Opfer. Sie geben sich als Polizisten aus und erzählen ihrem Opfer, dass zum Beispiel eine Einbruchsliste bei einem Tatverdächtigen gefunden worden sei, auf der auch das Opfer stehen würde. Präventiv solle die Person alle Wertgegenstände und Vermögenswerte in einer Tasche oder einem Plastiksack verstauen. Nach dem Telefonat werde ein Abholer vorbeikommen, um die

Trickbetrüger versuchen, mit dem „Enkel- oder Neffentrick“ ältere Menschen zu betrügen.

Wertsachen zur Polizeiinspektion zur Verwahrung zu bringen.

„Corona-Tester“. In jüngster Zeit gab es auch Meldungen über Personen die an Türen läuten und behaupten, sie wären Corona-Tester, um sich dadurch Zugang zu den Wohnungen zu verschaffen. Derzeit liegen noch keine Schadensmeldungen vor, jedoch muss davor gewarnt werden. Besondere Vorsicht ist generell an der Haustür geboten. Gerade in Bezug auf Polizisten sollte man nach dem Dienstausweis fragen. Wenn dieser nicht vorgezeigt werden kann, sollte das Gespräch sofort beendet werden. Die Polizei übernimmt zu keinem Zeitpunkt Wertgegenstände oder Geld und sie kommt auch nicht für Testungen in die Wohnung.

Fake Shops. Wie die polizeiliche Kriminalstatistik 2018 zeigt, ist die Internetkriminalität und vor allem die Zahl der Fälle von Internetbetrug im Steigen. „Die Täter sehen, dass die Menschen vermehrt zu Hause sind und der persönliche Kontakt derzeit nicht möglich ist, daher haben sie sich angepasst. Kriminelle Tätigkeiten werden nun noch mehr ins Internet verlagert“, erklärte Büroleiter Kahn. Unter dem Deckmantel „Corona“ versuchen Kriminelle die derzeitige Lage auszunutzen, um sich rechtswidrig zu bereichern. Viele Fake Shops werben mit attraktiven Angeboten und (Sonder-)Artikeln, die nur schwer oder kaum erhältlich sind – etwa mit medizinischen Schutzmasken oder Desinfektionsmitteln. Sie akzeptieren nur Vorauskassa als Zahlungsmittel und bieten keine Zahlungsalternativen an. Als sicheres Zahlungsmittel gelten der Kauf auf Rechnung, Lieferung per Nachnahme, Kreditkartenzahlung oder *Paypal*. Zudem enthalten die Webseiten oft Rechtschreib- und Grammatikfehler oder verwenden keine Umlaute. Man sollte besonders auf ein vollständiges Impressum achten und auf die verschiedenen Gütezeichen sowie auf eine sichere Internetverbindung, die durch „https“ gekennzeichnet ist. Da diese Merkmale auch auf falschen Angaben beruhen können, sollte man auf unabhängigen Plattformen, *wie Trusted Shops (www.trustedshops.at)* oder das „Österreichische E-Commerce-Gütezeichen“ *(www.guetezeichen.at)* sowie die Umsatzsteuer-Identifikationsnummer oder den Firmennamen mittels einer Suchmaschinenabfrage überprüfen.

Love- oder Romance-Scam. In Zeiten wie diesen, in denen sich das gesamte Leben eine zeitlang auf die eigenen vier Wände beschränkt und sich der soziale Kontakt dadurch auf soziale Medien oder sonstige Plattformen reduziert, ist die Gefahr größer, Opfer eines Love-Scams zu werden. Die modernen Heiratsschwindler nehmen in sozialen Netzwerken oder Partnervermittlungsbörsen Kontakt zu ihren Opfern auf, fädeln eine amouröse Kommunikation ein und bauen eine Vertrauensbasis auf, um sie um Geld zu bitten.

Die Täter setzen alles daran, dass sich Gefühle der Liebe und der Zuneigung bei ihren Opfern aufbauen. Die Vorbereitungen erstrecken sich nicht selten über Wochen oder Monate. Im Laufe der Kontakte kommt es eventuell auch zu intimen Handlungen. Bilder oder Videos werden ausgetauscht, häufige Telefonanrufe oder Nachrichten lassen das Opfer denken, die Beziehung wäre echt. Das Vertrauen soll ein Hinterfragen oder Anzweifeln, warum oder wofür nach Geld gefragt wird, verhindern. Wenn das Opfer auf ein persönliches Treffen drängt, wird vom Täter häufig vorgeschlagen, nach Österreich auf Besuch zu kommen. Die Reise- so-

FOTO: BURITORA/STOCK.ADOBE.COM

wie Folgekosten, wie etwa für Reisepass, Visum und Aufenthalt, werden beiläufig erwähnt und erst zu einem späteren Zeitpunkt wird mitgeteilt, dass diese Ausgaben vom Betrüger nicht gedeckt werden können. Der Besuch kann nur zustande kommen, wenn das Opfer zumindest einen Großteil der Kosten übernimmt. „Die Betrüger werden alles unternehmen, um ihren Opfern etwas vorzuspielen, ihr Vertrauen zu erschleichen und es emotional unter Druck zu setzen, indem sie eine Notlage vortäuschen. Spätestens dann, wenn Geld gefordert wird, muss klar werden: Das ist keine Liebe“, erklärt Kahn. Es bleibt auch nicht bei einer einmaligen Geldforderung, sondern die Forderungen werden häufiger und die Beträge höher.

Da in Zeiten von Corona persönliche Treffen mit Personen, die nicht im selben Haushalt wohnen, untersagt sind, wird das persönliche Kennenlernen auf später verschoben, wenn die Reisebeschränkungen wieder aufgehoben sind. „Frauen sind von dieser Betrugsmasche genauso betroffen wie Männer; bei den Frauen sind häufig Militärgeneräle, Wissenschaftler oder Ingenieure die vermeintlichen Liebhaber“, erklärt Kahn. Da diese im Ausland arbeiten ist das Internet für sie die einzige Kommunikationsmöglichkeit.

Die Polizei rät, vorsichtig zu sein, welche persönlichen Informationen man preisgibt, und Daten zu schützen. Um Unsicherheiten auszuräumen, geben Sie den Namen oder das Foto Ihres Gegenübers in eine Suchmaschine ein. Bei Suchtreffern können Sie davon ausgehen, dass Sie nicht der einzige Chatpartner sind. Wichtig ist auch, dass Sie keinesfalls kompromittierende Fotos oder Videos von sich selbst übermitteln, da diese unter Umständen gegen Sie verwendet werden können.

Phishing. Auch beim Phishing nutzen Kriminelle die Coronakrise für ihre Betrügereien und versenden Phishing-Mails im Namen von Unternehmen. In erster Linie geht es ihnen um das Herauslocken geheimer Daten, die zum Beispiel für Online-Banking, Online-Shops oder soziale Netzwerke genutzt werden. In den betrügerischen E-Mails wird dazu aufgefordert, Links oder Dateianhänge zu öffnen und seine persönlichen Daten einzugeben. Derzeit kursieren Phishing-Mails von gefälschten *A1*-Angeboten, betrügerische *DHL*-Benachrichtigungen, E-Mails von *Amazon* und von der *Raiffeisen Bank*. Die in den Mails enthaltenen Links locken auf die Phishing-Webseite; es können sich hinter diesen auch Downloads und somit Schadsoftware verbergen. „Sollten Sie E-Mails bekommen, bei denen Ihre Zugangsdaten von einem Unternehmen gefordert werden, stellen Sie sich die Frage, ob diese Zugangsdaten dem Unternehmen nicht eigentlich bekannt sein müssten“, erklärt Büroleiter Kahn.

Betrüger machen sich in Krisenzeiten vermehrt an „einsame Herzen“ heran, um ihnen durch vorgetäuschte Liebes-Versprechen Geld abzuluchsen.

Es ist wichtig, bevor Links angeklickt oder Daten eingegeben werden, den Inhalt und den Absender zu hinterfragen. Ist das vorliegende Schreiben glaubwürdig und nachvollziehbar? Ebenfalls geprüft werden sollte die Absenderadresse. Beim ersten Blick mag sie plausibel aussehen, beim genaueren Betrachten erkennt man jedoch, dass sie von keiner offiziellen E-Mail-Adresse versendet wurde. Da Phishing-Mails massenhaft verschickt werden, wird vom Absender eine unpersönliche Anrede verwendet. Dies ist ein weiteres Indiz für ein betrügerisches E-Mail.

„Generell gilt, E-Mails, die im Spamordner landen sind verdächtig, bei diesen E-Mails dürfen Sie auf keinen Fall auf einen Link im E-Mail klicken“, sagt Kahn. Wenn Sie dennoch einmal Zugangsdaten eingegeben haben und sich unsicher sind, ob nun nicht vielleicht ein Phishing vorliegt, dann kontaktieren Sie den Betreiber der Homepage oder ändern Sie die Zugangsdaten sofort. Im Falle von Bankomatkarten- oder Kreditkarteninformationen wird geraten, sofort Kontakt zur Bank herzustellen und zu besprechen, ob die Karte sofort gesperrt werden soll, um eine illegitime Abbuchung zu verhindern. Falls jedoch bereits abgebucht wurde, ist eine schnelle Vorgehensweise noch wichtiger und generell gilt, zuerst die Bank zu kontaktieren und dann bei der Polizei Anzeige zu erstatten.

Positive Entwicklung. Neben all den negativen Trends gibt es jedoch auch Positives zu vermelden: Während die genannten Betrugsformen in Zeiten der Corona-Krise in den Vordergrund treten, ist seit Mitte März eine deutliche Reduktion der Zahl anderer strafbarer Handlungen gegen fremdes Vermögen, wie etwa Diebstahl, Einbruch oder Raubdelikte zu verzeichnen. Reisebeschränkungen und Präventionsmaßnahmen, wie etwa die vom Innenministerium und der *Wirtschaftskammer Österreich* veröffentlichten Tipps für Seniorinnen und Senioren für sichere Geldgeschäfte, zeigen ihre Wirkung.

Kontakt. Wer Opfer einer Straftat wurde, sollte in der nächsten Polizeiinspektion Anzeige erstatten. Es sind die derzeit geltenden Corona-Regeln zu beachten: Beim Betreten der Dienststelle ist eine Schutzmaske zu tragen. Bei Verdacht eines Internetbetrugs kann man sich an die Cybercrime-Meldestelle des Bundeskriminalamts wenden: *against-cybercrime@bmi.gv.at*; weitere Präventionstipps gibt es unter *www.bundeskriminalamt.at*. *Romana Tofan*