LUG & TRUG

Folge 1 » Cybercrime «

Wie schütze ich mich vor Betrug?

In Zusammenarbeit von
„Sicher Leben in Graz“ und
der Grazer Kriminalpolizei

SICHER LEBEN IN GRAZ

POLIZEI

Impressum:

Herausgeber:
Graz: Sicher Leben!,
Eingetragener Verein
Körblergasse 10, 8010 Graz
ZVR: 066269364

www.sicherlebeningraz.at
www.facebook.com/sicherlebeningraz.at
www.twitter.com/SicherLebenGraz

Für den Inhalt verantwortlich:
Werner Miedl

Vorstand:
Dr. Klaus Gstirner
Obmann
Wofgang Schnelzer, MSc
Schriftführer
Franz Grossauer
Kassier
Mag.a Pauline Riesel-Soumaré
Beirätin, Migranten
Christian Loigge, MsC
Beirat
Werner Miedl
Geschäftsführer

Diese Information wurde in Zusammenarbeit mit den Beamten der Betrugsgruppe der Grazer Kriminalpolizei erstellt. Dank gilt vor allem Klaus Murtinger, Daniela Schuster, Kurt Kemeter und Gerd Lachomsek.

Druck: Offsetdruck Dorrong OG, Graz

Unsere Partner:

SICHER LEBEN IN GRAZ

Zur leichteren Lesbarkeit wurde auf geschlechtsneutrale Schreibweise verzichtet, womit keine Aussage über die tatsächliche Geschlechterverteilung von Straftätern und Straftäterinnen getroffen wird. Die aktuelle Gerichtsstatistik Österreichs weist 86% aller Verurteilten als männlich aus.

Sicherheit ist mir ein großes Anliegen, denn das persönliche Sicherheitsgefühl bestimmt die Lebensqualität in unserer Stadt. Deshalb versuchen wir auf vielen Ebenen diese Sicherheit in den Mittelpunkt zu stellen.

Wir fördern als Stadt Graz den jährlichen Präventionskongress, der alle Interessierten darüber informiert, was jede(r) selbst zur Sicherheit beitragen kann. Über das Projekt „Nachbar schafft Sicherheit" gibt es für Siedlungen auch die Möglichkeit ein Sicherheitsseminar vor Ort gratis abzuhalten.

Mit dem Verein „Sicher Leben in Graz" wollen wir die Sicherheitsarbeit in unserer Stadt um eine wesentliche Facette ergänzen. Die Grundsätze: Informieren statt sanieren, Angst nehmen statt zu schüren, aber auch Konsequenz dort wo sie nötig ist, werden durch die Arbeit der Profis in dem Verein umgesetzt.

Wir haben eine Ordnungswache ins Leben gerufen und wir bemühen uns mit dem Jugendamt in Kooperation mit der Polizei, das Jugendschutzgesetz auch tatsächlich zu kontrollieren und bei Vergehen vor allem auch die Eltern in die Pflicht zu nehmen. Daher ist das grundsätzliche Sicherheitsgefühl in Graz, das belegen alle unsere Studien, tadellos. Dabei ist besonders erfreulich, dass in Graz das Vertrauen in die eigenen Nachbarn groß ist. Trotzdem muss man auf der Hut sein, denn Betrüger und Gauner finden sich immer und überall.

Mit dieser Broschüre wollen wir Sie auf die wichtigsten Betrugsformen aufmerksam machen und Anleitungen geben, wie man sich vor Ihnen schützt.

Ihr

Mag. Siegfried Nagl
Bürgermeister der Stadt Graz

Sicherheit ist wesentlich um sich in einer Stadt wohlfühlen zu können. Um noch mehr Sicherheit zu gewährleisten, sind wir mit dem Verein „Sicher Leben in Graz“ eine Kooperation eingegangen. Gemeinsam mit der Grazer Stadtverwaltung und mit dem städtischen Sicherheitsmanagement, mit der Ordnungswache und mit der Polizei sollen in Zukunft alle Bürgerinnen und Bürger an der Kriminalitätsprävention mitwirken können. Fachkundige wissenschaftliche Beratung wird uns dabei unterstützen.

Die umfassende Information aller Grazerinnen und Grazer ist Grundvoraussetzung für diese Arbeit und die muss genau dort beginnen, wo aktuell die größten kriminalstatistischen Zuwachsraten zu verzeichnen sind: Beim Betrug im Allgemeinen und beim Betrug im Internet, dem Cybercrime, im Speziellen!

In Zukunft werden wir Sie daher rechtzeig und umfassend über aktuelle und neue Formen der Kriminalität informieren. Mit allen Mitteln werden wir den kriminellen Elementen ihr Treiben so schwer wie möglich machen!

Ich bin davon überzeugt, dass durch diese interdisziplinäre Zusammenarbeit eine neue Kraft für ein noch lebenswerteres Graz entsteht!

Ihr

Mag. (FH) Mario Eustacchio
Grazer Sicherheitsstadtrat

Dr. Klaus Gstirner,
Arzt und Psychotherapeut will als Obmann von „Sicher Leben in Graz“ einen Beitrag dazu leisten, dass wir uns in unserer Stadt auch weiterhin wohlfühlen können!

Lug und Trug. Täuschen und Lügen sind die Praktiken der Betrüger, denen wir mit dieser Broschüre das Leben schwer machen wollen. Erst wenn Sie ausreichend über Informationen verfügen, können Sie sich auch erfolgreich zur Wehr setzen.

Und genau darauf kommt es uns vom Verein „Sicher Leben in Graz“ an: Wir wollen mit der Polizei, der Stadt Graz, den Hilfsorganisationen und den Betroffenen gemeinsame Sache machen. Damit wir den Ganoven das Handwerk legen und Sie sich auf der sicheren Seite fühlen!

Ihr

Dr. Klaus Gstirner
Obmann

Die Geschichte des Betruges ist vermutlich so alt wie die Menschheit und offensichtlich ebenso anpassungsfähig. Mit der alltäglich gewordenen Nutzung elektronischer Hilfsmittel haben Betrüger auch die Nutzung dieser Medien für sich – also für kriminelle Zwecke – entdeckt.

Täglich wenden sich Opfer, die durch die Straftaten mitunter enorme Schäden erlitten haben, an die Polizei.

Wir – als Ermittler und Ermittlerin für Betrugsangelegenheiten – geben im Folgenden einen Überblick über häufig angezeigte Schadensfälle, und Sie erhalten Empfehlungen, wie Sie sich schützen und wie Sie im Schadensfall reagieren können.

Für alle Fälle gilt: Verständigen Sie im Bedarfsfall ohne Zögern die Polizei! Beim Stadtpolizeikommando Graz kümmert man sich gerne in jeder Polizeiinspektion und unter der Telefonnummer der Grazer Polizei 059-133-65-0 um Ihr Anliegen oder vermittelt Sie an eine zuständige Dienststelle.

Ihr

Chefinspektor
Klaus Murtinger

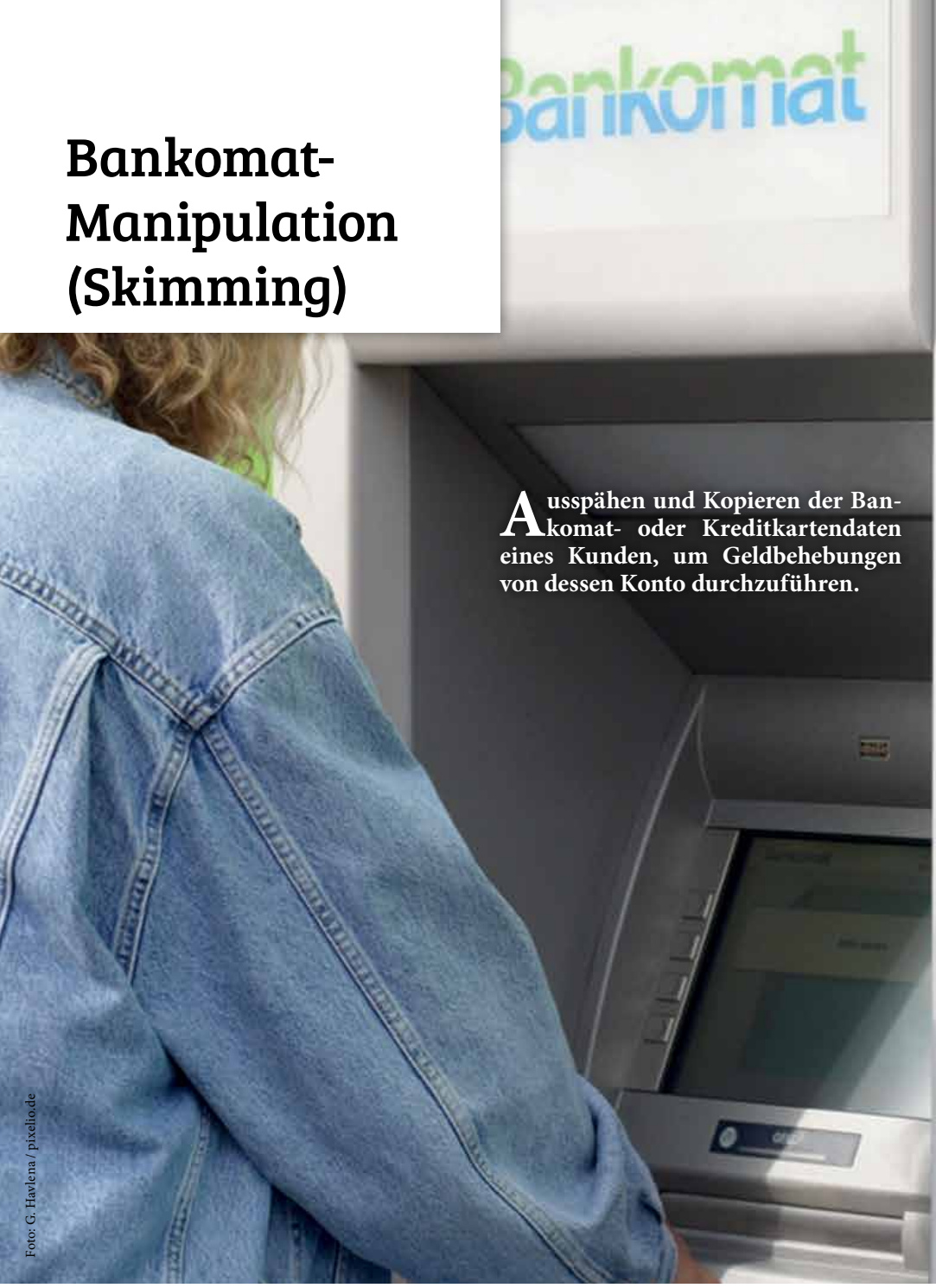
Leiter der Betrugsgruppe,
Stadtpolizeikommando Graz

Ihre

Abteilungsinspektor
Daniela Schuster

Betrugsgruppe,
Stadtpolizeikommando Graz

Bankomat-Manipulation (Skimming)



Ausspähen und Kopieren der Bankomat- oder Kreditkartendaten eines Kunden, um Geldbehebungen von dessen Konto durchzuführen.

Foto: G. Havlena / pixelio.de

Was ist passiert:

Auf meinem Kontoauszug sehe ich, dass mein Konto beinahe leer ist. Mehrere tausend Euro sind offenbar in Amerika behoben worden. Das kann aber nicht sein, ich war noch niemals außerhalb von Europa! Bei der Bank sagt man mir, dass die Bargeldbehebungen mit meinen Bankomatkartendaten vorgenommen wurden. Möglicherweise wurde meine Bankomatkarte von Betrügern kopiert.

Für die Rückzahlung des Betrages verlangt die Bank eine Anzeige bei der Polizei und meine eidesstattliche Erklärung, dass ich diese Behebungen nicht selbst getätigt habe.

Was liegt vor:

Offensichtlich haben Betrüger technische Vorrichtungen an einem Bankomaten angebracht, ohne dass die Bank oder die Kunden es bemerkt haben. Die Daten der Bankomatkarte sowie der PIN-Code wurden bei einer Behebung am manipulierten Bankomat gespeichert. Komplizen fertigen mit den so erlangten Kartendaten im Ausland ein Duplikat der Bankomatkarte an und führen Bargeldbehebungen an Automaten durch. Üblicherweise wird der Betrag bei diesem Schadensfall von der Bank oder der kartenausgebenden Stelle ersetzt.

In seltenen Fällen gelangen Betrüger auch über Zahlungsterminals (Bankomatkassen) an Kundendaten. Immer wieder werden auch Kunden von Tätern bei der PIN-Eingabe abgelenkt und beobachtet, um an die Daten zu kommen.

Die Polizei empfiehlt:

→ Decken Sie die Tastatur bei der Behebung ab.

→ Lassen Sie sich während der Behebung nicht von Unbekannten ablenken.

→ Bewahren Sie Karte und PIN-Code immer getrennt voneinander auf.

→ Kontrollieren Sie Ihren Kontostand regelmäßig.

→ Verständigen Sie im Schadensfall sofort Ihre Bank und stellen Sie der Polizei Kopien Ihrer Kontoauszüge zur Verfügung.

Kontoüberweisungs-Betrug

Bei dieser eher seltenen Form des Betruges entnehmen Betrüger Zahlscheine aus Überweisungsboxen oder Kontoauszüge aus Papierkörben, um mit den Daten des Opfers Übeweisungen zu dessen Lasten durchzuführen.

Die Polizei empfiehlt:

→ Werfen Sie Unterlagen mit finanziellen Daten oder persönlichem Inhalt nicht in der Öffentlichkeit weg.

→ Kontrollieren Sie Ihre Kontoauszüge regelmäßig.

→ Verständigen Sie im Schadensfall sofort Ihre Bank und erstatten Sie Anzeige bei der Polizei.

Dating-Betrug (love-scamming, Heirats-schwindel)

Ausnutzen einer vorgetäuschten Liebesbeziehung, um in einer angeblichen Notsituation finanzielle Hilfe zu ergaunern.

Foto: La-Liana / pixelio.de

Was ist passiert:

Vor ein paar Wochen habe ich eine Zufallsbekanntschaft im Internet gemacht. Aus der Bekanntschaft ist Sympathie geworden. Als ich noch dazu die entzückenden Fotos bekommen habe, bin ich überzeugt, dass ich die Partnerin fürs Leben kennen gelernt habe. Mittlerweile schreiben wir uns fast stündlich. Meine „Flamme", sie lebt im Ausland, kann es kaum erwarten, endlich zu mir nach Graz zu kommen.

Bald ist es so weit. Obwohl es ihr fast peinlich war, hat sie mich um Geld für ein Flugticket gebeten. Ich habe ihr das Geld aber sehr gerne geschickt. Leider hat sie den Flug verpasst, da sie bei der Ausreise Probleme mit dem Zoll hatte.

Jetzt muss sie auch noch Strafe zahlen. Natürlich werde ich ihr wieder helfen.

Was liegt vor:

Betrüger suchen in Online-Partnerbörsen oder sozialen Netzwerken nach Opfern. Die Männer geben gute Bildung und einen hohen sozialen Status vor. Die Frauen erscheinen regelrecht bezaubernd und sind angeblich in sozialen Berufen tätig. Der Umgangston wird schnell romantisch.

Sehr schnell wird von Liebe und einer gemeinsamen Zukunft gesprochen. Die Bilder, die sie verschicken, zeigen sie als attraktive Menschen. Doch die Bilder sind gestohlen, die Lebensgeschichten sind erfunden.

Noch bevor es zum ersten Treffen kommt, werden plötzlich große Probleme und finanzielle Schwierigkeiten behauptet:

Probleme am Zoll, Unfall und Krankheit, Todesfall in der Familie u.ä. Die Opfer werden ersucht, Kontoüberweisungen oder Bargeld-Transfers ins Ausland zu tätigen.

In keinem Fall kommt es zu einem Treffen: Die charmante Krankenschwester bzw. auch der erfolgreiche Geschäftsmann existieren nicht!

Die Polizei empfiehlt:

→ Werden Sie misstrauisch, wenn Sie binnen kürzester Zeit innige Liebesschwüre erhalten.

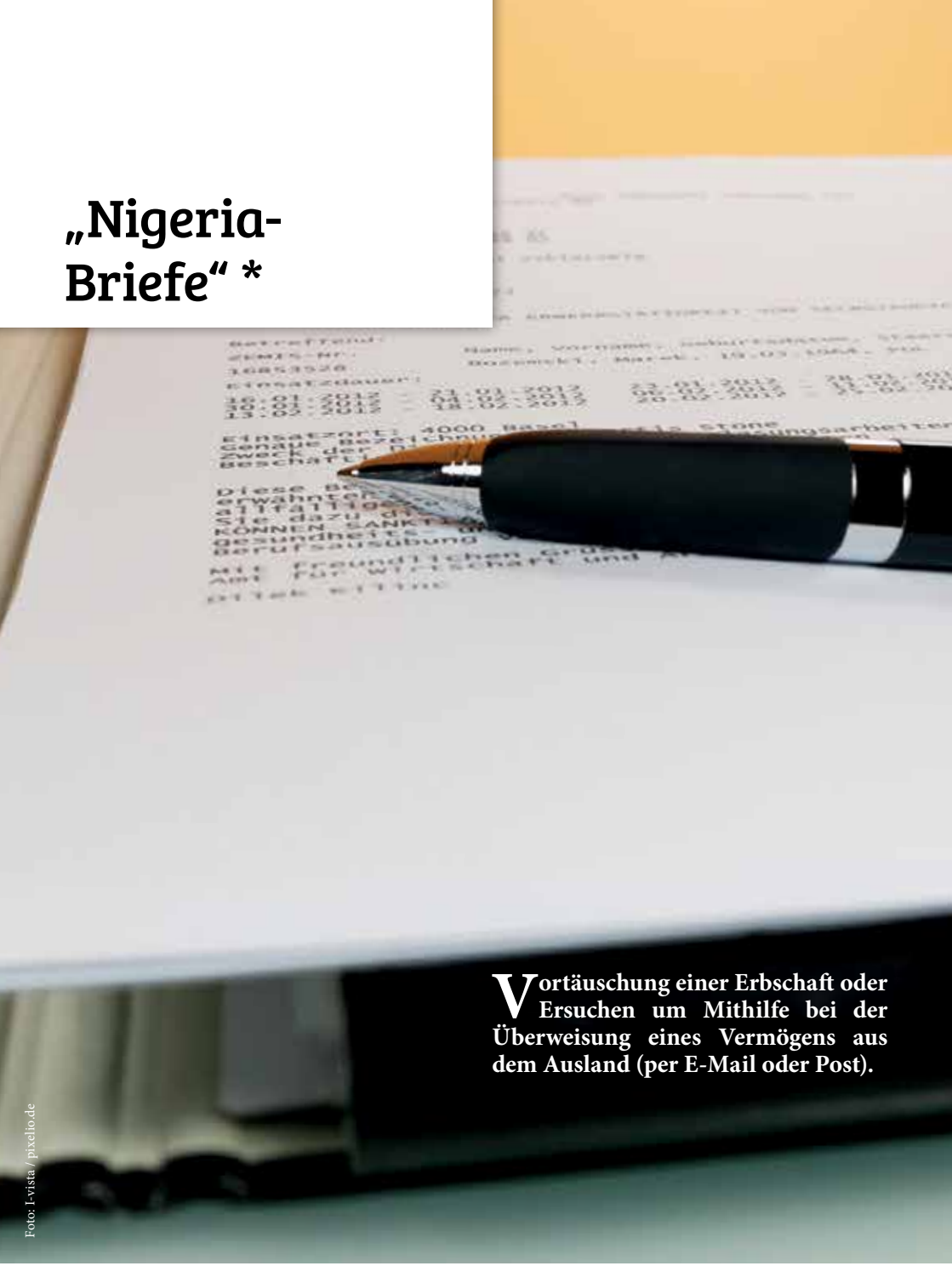
→ Überlegen Sie, ob die behauptete Verkettung von Schicksalsschlägen glaubhaft ist.

→ Brechen Sie sofort den Kontakt ab, sobald Sie unpassende Geldforderungen erhalten.

→ Überweisen Sie keinesfalls Geld. Recherchieren Sie im Zweifelsfall Namen und Fotos ihres Kontaktes im Internet.

→ Scheuen Sie sich nicht, im Schadensfall die Polizei zu verständigen. Stellen Sie den E-Mail-Schriftverkehr sowie allfällige Überweisungsbelege für die Ermittlungen zur Verfügung.

„Nigeria-Briefe“ *



Vortäuschung einer Erbschaft oder Ersuchen um Mithilfe bei der Überweisung eines Vermögens aus dem Ausland (per E-Mail oder Post).

Foto: I-vista / pixelio.de

Was ist passiert:

Ich erhalte ein Schreiben eines ausländischen Anwaltes, der mich ersucht, bei der Überweisung eines Vermögens aus dem Ausland behilflich zu sein. Er sei Vermögensverwalter eines kürzlich verstorbenen Klienten, der zufällig denselben Familiennamen gehabt hätte wie ich. Da keine Erben bekannt seien, würde das Vermögen von 10 Millionen Dollar wohl in das Staatsvermögen übergehen.

Sollte ich mein Konto als „Ersatzerbe" für den Geldtransfer zur Verfügung stellen, würde ich rund 30 % des Vermögens erhalten. Das sind ungefähr 3 Millionen Euro!

Ich bin begeistert und gebe dem Anwalt weitere Daten von mir bekannt. Kurz darauf erfahre ich, dass Kosten für die Beglaubigung der Erbschaft in Höhe von ein paar hundert Dollar zu bezahlen sind.

Ich überweise das Geld und bekomme prompt eine Kopie der beglaubigten Urkunde. In der Folge werde ich gebeten, weitere Zahlungen (Bank-Depotgebühr, Bestechung eines Beamten ua.) zu leisten.

Ich habe mittlerweile über 5.000 Euro überwiesen und warte seit Wochen auf mein neues Vermögen. Kürzlich habe ich von einer Betrugsform mit der Bezeichnung „Nigeria-Briefe" erfahren.

* Die Briefe werden in der Fachwelt so benannt, weil diese Kriminalitätsform dort ihren Ausgang fand. Es liegt uns fern, damit ein Land oder seine Bevölkerung zu diskriminieren.

Was liegt vor:

Unter dem Begriff „Nigeria-Briefe" ist der Polizei folgende Betrugsform bekannt:

Betrüger haben die Kontaktdaten (Name, Adresse, E-Mail) von Personen erlangt und stellen die Überweisung eines größeren Vermögens in Aussicht. Es handelt sich um Massensendungen, die an alle den Betrügern zur Verfügung stehenden Adressen geschickt werden. Weder die Anwaltskanzlei noch das Vermögen existieren tatsächlich.

Die Betrüger bereichern sich an den vermeintlich notwendigen Gebühren, die als Vorschusszahlungen geleistet werden müssen.

Bereits überwiesene Geldbeträge können nur selten zurückgeholt werden, da die angegebenen Konten meist mit gefälschten Daten geführt werden.

Die Polizei empfiehlt:

→ Reagieren Sie nicht auf derartige (Massen)Sendungen.

→ Geben Sie keinesfalls persönliche Daten oder Bankverbindungen bekannt.

→ Sichern Sie im Schadensfall den E-Mail-Verkehr und stellen Sie ihn der Polizei zusammen mit den Kopien der Überweisungsbelege für die Ermittlungen zur Verfügung.

Polizei-Trojaner (Vortäuschen behördlicher Ermittlungen)

Infizieren eines PC mit Schadsoftware und Forderung von Strafgebühr an die Behörde.

Was ist passiert:

Ich surfe gerade im Internet, als plötzlich eine Information der Polizei am Bildschirm aufscheint. Der PC reagiert nicht mehr, die Seite lässt sich nicht schließen. Ich lese, dass ich beschuldigt werde, illegale Seiten besucht zu haben und eine Strafe zahlen muss. Erst nach der Zahlung von 100 Euro wird die Polizei meinen PC wieder freischalten.

Ich soll Wertbons für den Internet-Zahlungsverkehr kaufen und den Zahlungs-Code per E-Mail an die angegebene Adresse schicken. Ich habe ein schlechtes Gewissen und folge den Anweisungen. Ich habe 100 Euro gezahlt, aber mein PC funktioniert trotzdem nicht.

Was liegt vor:

Der sogenannte Polizei-Trojaner wird von Betrügern mit einem Email-Anhang verschickt und auf dem PC gespeichert, oder das Schadprogramm installiert sich während der Internet-Nutzung unbemerkt selbst. Diese Software sperrt den Computer und täuscht dem Nutzer die Information vor, dass die Polizei kriminelle Handlungen registriert habe. Zur Freischaltung müsste nun eine Strafgebühr von 100 Euro durch Übermittlung von Wertkarten bezahlt werden.

In Wirklichkeit liegt keine amtliche Ermittlung vor. Keine Behörde fordert auf diese Weise Geld!

Trotz Zahlung des geforderten Geldes bleibt der Computer (natürlich) gesperrt, und die vom Opfer gekauften Codes werden von den Betrügern im Internet verwertet oder verkauft.

Die Polizei empfiehlt:

→ Zahlen Sie den geforderten Betrag keinesfalls. Weder Polizei, Justiz oder Finanz noch seriöse Unternehmen fordern auf diese Art und Weise Geld.

→ Öffnen Sie keine Anhänge, die Sie von Unbekannten per Email erhalten haben.

→ Verwenden Sie seriöse Virenschutzprogramme, und halten Sie diese aktuell.

→ Achten Sie darauf, welche Software (Apps) Sie installieren.

→ Verständigen Sie im Schadensfall die Polizei. Eventuell wird Ihr Computer zur Datensicherung benötigt.

Hinweis:

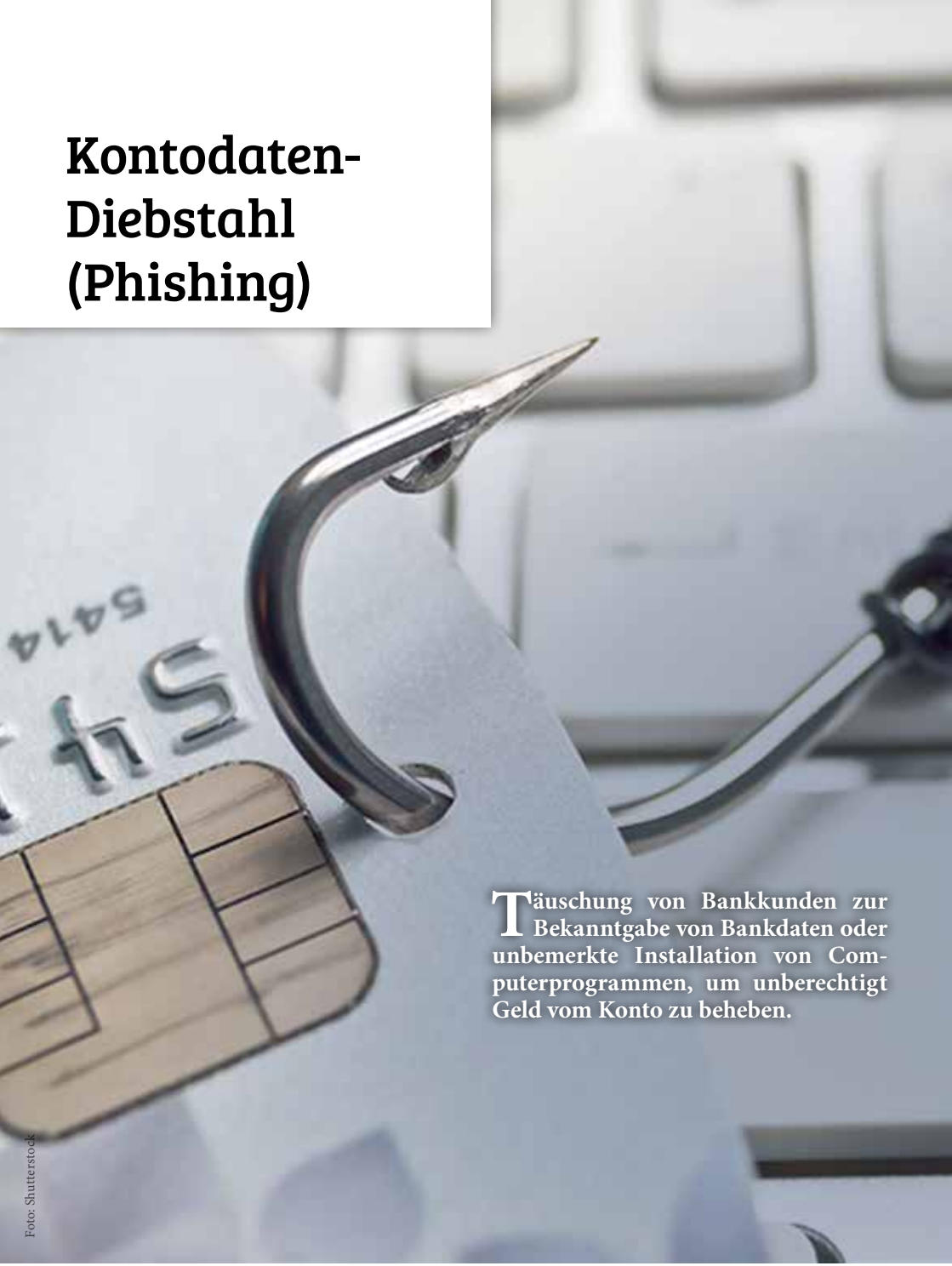
Für die Entfernung der Schadsoftware gibt es im Internet zahlreiche Anleitungen, vor allem unter den Websites:

→ https://www.botfrei.de/
→ http://www.bka-trojaner.de/

bzw. auf YouTube sind entsprechende Informationen zu finden, die laufend angepasst und aktualisiert werden.

Wenn Sie bereits Codes gekauft haben, besteht die Möglichkeit, die PINs von der Firma sperren zu lassen – sofern die Codes noch nicht eingelöst worden sind.

Kontodaten-Diebstahl (Phishing)



Täuschung von Bankkunden zur Bekanntgabe von Bankdaten oder unbemerkte Installation von Computerprogrammen, um unberechtigt Geld vom Konto zu beheben.

Foto: Shutterstock

Was ist passiert:

Ich sehe meinen Kontoauszug an und stelle fest, dass ein Riesenbetrag an einen mir nicht bekannten Empfänger abgebucht wurde. Bei der Bank sagt man mir, dass diese Online-Überweisung mit meinen persönlichen Bankdaten genehmigt worden ist. Ich fordere die Rückzahlung des Betrages, da ich diese Überweisung sicher nicht veranlasst habe. Der Bankmitarbeiter kann aber nicht garantieren, dass das Geld zurück geholt werden kann.

Was liegt vor:

Für diesen Schadensfall gibt es mehrere Möglichkeiten, wie Betrüger an die Kontodaten gelangen konnten.

Häufig locken Betrüger Kunden durch Versenden von Emails auf gefälschte Bankseiten, wo der Kunde zur angeblichen Verbesserung der Datensicherheit zur Eingabe und Bestätigung seiner Bankdaten aufgefordert wird. Tatsächlich können die Betrüger mit diesen Daten Geld vom Konto des Kunden überweisen. In anderen Fällen verschicken die Betrüger Emails an Bankkunden, die versteckte Computerprogramme zur Ausspähung von Informationen enthalten. So gelangen die Täter, vom Kunden unbemerkt, an seine Bankdaten und können Überweisungen veranlassen.

Zusätzlich wird das Handy durch Anbieten von Gratis-Programmen (Apps) „infiziert". Dadurch können die Betrüger auch auf Bankdaten (vor allem TAN-Codes) zugreifen, die an das Handy geschickt werden.

Die Polizei empfiehlt:

→ Keine Bank fordert Sie zur Eingabe von Bankdaten auf. Die Bank kennt Ihre Daten!

→ Öffnen Sie Bankseiten immer nur durch Eingabe der offiziellen Adresse.

→ Folgen Sie keinen Links, die Sie per Email erhalten haben.

→ Werden Sie auf jeden Fall misstrauisch, wenn das angebliche Schreiben Ihrer Bank Rechtschreibfehler aufweist oder in unkorrektem Deutsch verfasst ist.

→ Verwenden Sie seriöse Virenschutzprogramme auf PC und Handy und halten Sie diese aktuell.

→ Achten Sie darauf, welche Software (Apps) Sie auf PC und Handy installieren.

→ Kontrollieren Sie regelmäßig Ihren Kontostand.

→ Verständigen Sie im Schadensfall sofort Ihre Bank.

→ Stellen Sie der Polizei im Schadensfall PC und Handy unverändert zur Datensicherung zur Verfügung.

Gewinnversprechen (Vorauszahlungsbetrug)

Mitteilungen über den Gewinn von höheren Bargeldbeträgen, Kraftfahrzeugen udgl. telefonisch, per E-Mail oder Post (Spanische Lotterie, Versandhäuser ua.).

Was ist passiert:

Ein E-Mail eines ausländischen Anwaltes findet sich in meinem Posteingang. Anfangs skeptisch öffne ich das Schreiben und kann es dann kaum fassen. Ich habe tatsächlich gewonnen. Ich nehme Kontakt mit der Anwaltskanzlei auf und erfahre, dass ich lediglich Bearbeitungsgebühren überweisen muss. Danach soll mir der Gewinn zugestellt werden. Ich überweise den Betrag und erfahre, dass mich jetzt nur noch eine weitere Zahlung (Transaktionskosten, Überstellungskosten oder Steuern) vom ersehnten Gewinn trennt. In Summe habe ich mittlerweile über 1.000 Euro überwiesen, den Gewinn aber immer noch nicht erhalten. Langsam bekomme ich Bedenken.

Was liegt vor:

Betrüger haben Kontaktdaten (Name, Adresse, E-Mail) vieler Personen erlangt und stellen die Überweisung eines größeren Vermögens in Aussicht. Es handelt sich um Massensendungen, die an alle den Betrügern zur Verfügung stehenden Adressen geschickt werden. Weder die Anwaltskanzlei noch der Gewinn existieren tatsächlich. Die Betrüger bereichern sich an den vermeintlich notwendigen Gebühren, die als Vorschusszahlungen geleistet werden müssen. Bereits überwiesene Geldbeträge können nur selten zurückgeholt werden: Die angeblichen Treuhandkonten gehören natürlich keiner Anwaltskanzlei an sondern werden mit gefälschten Daten geführt.

Die Polizei empfiehlt:

→ Reagieren Sie nicht auf derartige (Massen-)Sendungen.

→ Haben Sie an einem Gewinnspiel teilgenommen? Wer nicht mitgespielt hat, kann auch nicht gewonnen haben!

→ Seien Sie auch kritisch, wenn Ihnen gesagt wird, dass Sie zufällig unter allen Kunden des genannten Unternehmens als Gewinner ermittelt worden sind.

→ Geben Sie keinesfalls persönliche Daten oder Bankverbindungen bekannt.

→ Leisten Sie keine Vorauszahlungen, kein seriöses Unternehmen verlangt diese zur Gewinnauszahlung.

→ Sichern Sie im Schadensfall den E-Mail-Verkehr und stellen Sie diesen mit Kopien der Überweisungsbelege für die polizeilichen Ermittlungen zur Verfügung.

Einkaufen im Internet (Online-Shopping)

Angebot von Dienstleistungen (Wohnungsvermietung, Kfz-Verkauf, hochpreisige Elektronikgeräte ua.) und Waren.

Was ist passiert:

Ich sitze vor dem Computer und durchstöbere das Internet, da ich auf der Suche nach einem Schnäppchen bin. Ich stoße auf ein tolles Angebot und denke: Jetzt muss ich aber schnell zugreifen, bevor mir jemand zuvorkommt. Ich trete mit dem Verkäufer in Kontakt und sichere mir den Zuschlag. Dass ich in diesem Fall eine Anzahlung leisten soll, versteht sich von selbst.

Da der Verkäufer zurzeit im Ausland ist, gehe ich in die Stadt und schicke das Geld über seine Empfehlung mit einem Bargeldtransfer an ihn. Jetzt ist mehr als eine Woche vergangen, meine gekaufte Ware ist trotz anfänglicher Beteuerungen des Verkäufers nicht bei mir eingetroffen, und auch mein Verkäufer ist plötzlich nicht mehr erreichbar.

Was liegt vor:

Mit solchen oder ähnlichen Fragen wenden sich täglich Personen, die offensichtlich Opfer eines Betruges geworden sind, an die Polizei. Das Angebot (Wohnung, Auto, Handy usw.) gibt es in Wirklichkeit nicht. Es erfolgt keine Lieferung, oder es werden beschädigte, alte Geräte oder leere Kartons geliefert. Der Kontakt zum Verkäufer kann nicht wieder hergestellt werden, weil dieser nach einem gelungenen Betrug den ohnehin erfundenen Namen und die E-Mail-Adresse aufgibt. Das überwiesene Geld wurde bereits vom Betrüger unter Verwendung eines falschen Namens behoben und kann nicht mehr zurückgeholt werden.

Die Polizei empfiehlt:

→ Misstrauen Sie allzu günstigen Angeboten, kein Verkäufer hat etwas zu verschenken.

→ Überdenken Sie Ihre Kaufentscheidung, bevor Sie Bargeld versenden.

→ Im Zweifel recherchieren Sie im Internet nach Betrugshinweisen zu diesem Thema oder zu dem Namen, den der Verkäufer im Inserat verwendet hat.

→ Denken Sie an sichere Alternativen zur Zahlungsabwicklung (zB: Zahlung über Treuhanddienste, die das Geld erst nach Einlangen der Ware freigeben).

→ Sichern Sie den E-Mail-Verkehr und stellen Sie ihn der Polizei zusammen mit den Kopien der Überweisungsbelege für die Ermittlungen zur Verfügung.

Inkasso-Betrug

Vortäuschen einer rechtsanwaltlichen Inkassotätigkeit zur Begleichung vorgeblicher Rechnungen.

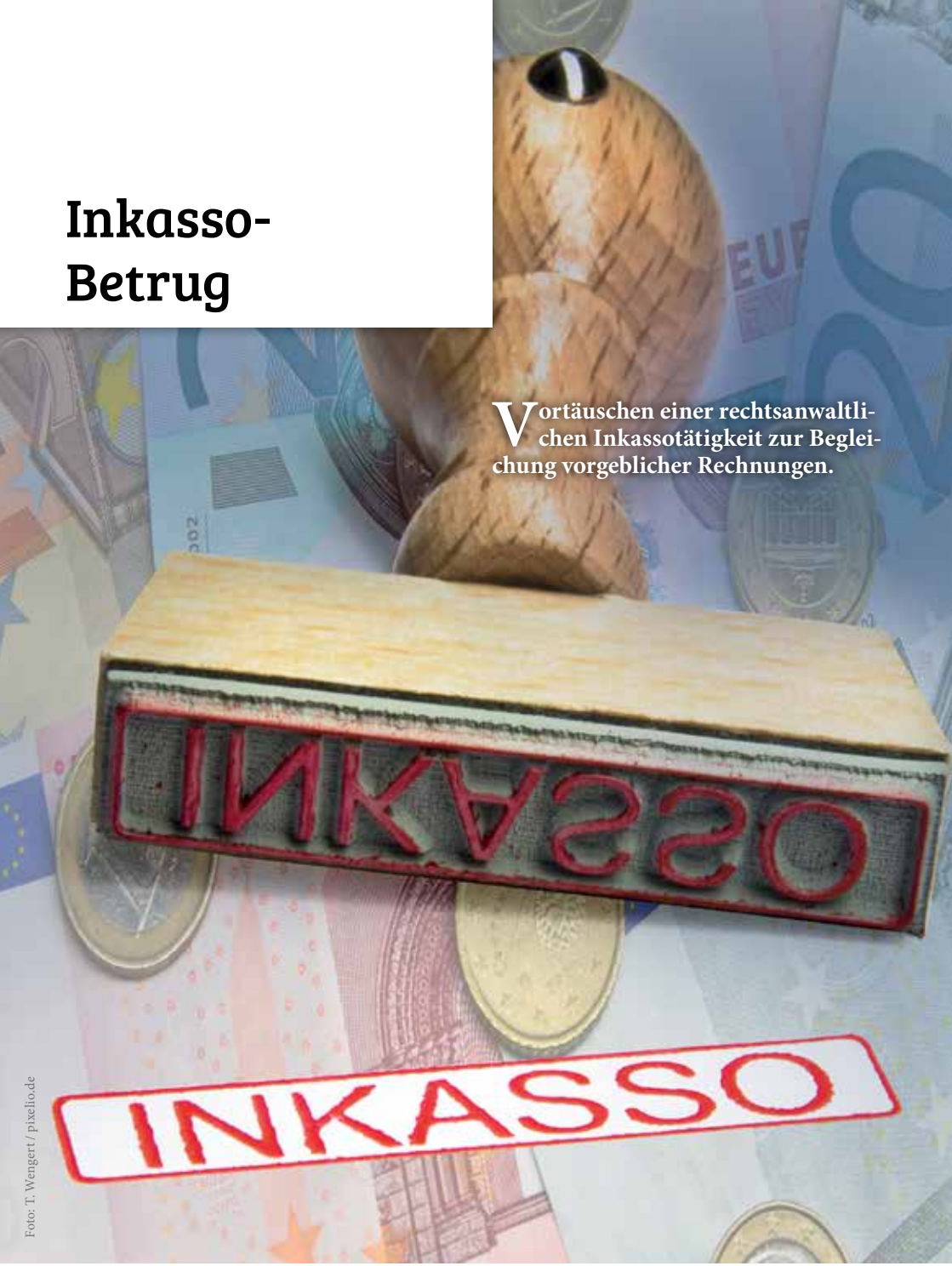


Foto: T. Wengert / pixelio.de

Was ist passiert:

Über mehrere Monate hinweg erhalte ich immer wieder Anrufe und Briefe von einer deutschen Anwaltskanzlei, in denen ich aufgefordert werde, eine offene Rechnung zu begleichen. Angeblich habe ich an einem kostenpflichtigen Gewinnspiel teilgenommen und nicht bezahlt.

Nachdem ich mich zunächst geweigert habe, der Forderung nachzukommen, droht mir nun der Anwalt, mich vor Gericht zu bringen.

Was liegt vor:

Betrüger geben sich als Rechtsanwälte, Inkassobüros uä. aus, um von den Opfern Geldforderungen einzutreiben, die überhaupt nicht existieren sondern schlicht erfunden sind.

Beispielsweise wird die Bezahlung von Teilnahmegebühren für Gewinnspiele gefordert oder die Kosten für Mehrwert-Telefonie, Strafen für die Verletzung von Urheberrechten oder den illegalen Download von pornografischem Material.

Zum Teil wird das Opfer massiv psychischem Druck ausgesetzt.

Die Polizei empfiehlt:

→ Zahlen Sie keine Rechnungen, die Sie nicht verursacht haben.

→ Notieren Sie sich die Telefonnummern des Anrufers sowie die Zeitpunkte der Telefonate.

→ Erstatten Sie Anzeige bei der Fernmeldebehörde und der Polizei. Stellen Sie die Mahnschreiben sowie die Telefonliste für die Ermittlungen zur Verfügung.

→ Wechseln Sie erforderlichenfalls Ihre Telefonnummer oder lassen Sie Ihre Eintragung im Telefonbuch löschen.

Time-Sharing-Betrug* (Betrug mit Teilzeit-Wohnrecht)

Fallweise werden Urlauber am ausländischen Urlaubsort (insbesondere in Spanien) mit derartigen Betrugsversuchen konfrontiert. Time-Sharing ist ein Urlaubsmodell, von dem es zahlreiche Abwandlungen gibt. Grundsätzlich erwirbt der Kunde das Recht, eine Ferienwohnung oder -anlage für eine vereinbarte Zeit zu nutzen.

Neben seriösen Unternehmen – dieses Modell existiert wirklich – bieten Betrüger nicht vorhandene oder nicht verfügbare Immobilien an und locken den Kunden meist mehrere tausend Euro für die angebliche Eintragung im Grundbuch, Ausstellung einer Urkunde u.ä. heraus.

*Diese Betrugsform ist in Österreich rückläufig.

Kreditkarten-Betrug

Kopieren von Daten einer Kreditkarte und Herstellung von Kartenduplikaten (oder Verwendung der Kartendaten im Internet) zu Lasten des Opfers.

Was ist passiert:

Bei der Überprüfung meiner Kreditkartenabrechnung stelle ich fest, dass es unerklärliche Abbuchungen gibt: Fahrkarten für die Bahn, Spieleinsätze bei einem Internet-Wettportal, Einkäufe in einer Luxus-Boutique und eine Flugreise.

Ich beeinspruche die Rechnung sofort. Der Mitarbeiter der Kreditkartenfirma verlangt eine polizeiliche Anzeigenbestätigung für die Schadensregelung.

Was liegt vor:

Betrüger können auf verschiedene Weise an Kreditkartendaten gelangen.

Zum einen können Kreditkarten von einem Betrüger kopiert werden, der als Kassier, Kellner oder Hotelangestellter arbeitet. Mit diesen Daten fertigen Komplizen wiederum Duplikate an, die mit falschen Namen versehen und zur Bezahlung von Einkäufen verwendet werden.

In anderen Fällen gelangen Betrüger auf illegale Weise (Hacking) an Kartendaten, die nach Einkäufen im Internet gespeichert bleiben. Diese Datensätze werden von den Betrügern entweder selbst verwendet oder im Internet weiter verkauft.

In allen Fällen wird das Konto des eigentlichen Karteninhabers mit den Umsätzen belastet.

Die Polizei empfiehlt:

→ Achten Sie bei Verwendung Ihrer Kreditkarte – besonders im Ausland – darauf, dass der Umsatz in Ihrer Anwesenheit und unter Ihrer Beobachtung gebucht wird.

→ Im Normalfall sollte Ihre Karte für eine redliche Transaktion nur ein Mal gezogen oder gesteckt werden müssen.

→ Verwahren Sie Ihre Karte so, dass Unbeteiligte keinen Zugang zu Ihren Daten haben.

→ Verwenden Sie Ihre Kartendaten im Internet nur bei seriösen Firmen. (Es gibt verschiedene Gütesiegel, die anzeigen, dass der Händler geprüft wurde und Sicherheitsstandards erfüllt. Achten Sie darauf, dass der Händler die Verschlüsselung Ihrer Kartendaten anbietet.)

→ Verwenden Sie bei Zahlung im Internet einen Dienstleister, der Ihre Zahlungen treuhändisch abwickelt.

→ Überprüfen Sie Ihre Abrechnungen in aktuellen Zeiträumen und regelmäßigen Abständen.

→ Wenden Sie sich im Schadensfall sofort an die Bank und das Kreditkartenunternehmen. Erstatten Sie Anzeige bei der Polizei. Stellen Sie Bestellunterlagen, Kreditkartenabrechnungen und etwaigen E-Mail-Verkehr für die Ermittlungen zur Verfügung.

Scheckbetrug

Verwendung gefälschter Schecks zur Bezahlung von im Internet angebotenen Waren und Dienstleistungen (Fahrzeuge, Reisen, Hotelzimmer ua.)

Was ist passiert:

Auf mein Inserat meldet sich schon nach kurzer Zeit ein ausländischer Interessent. Welche Freude, der Mann will mein Motorboot ohne Preisverhandlung kaufen. Über die Transportkosten brauche ich mir auch keine Sorgen zu machen, er wird auf eigene Rechnung für die Abholung des Bootes sorgen.

Auf seinen Wunsch akzeptiere ich die Bezahlung mittels Scheck. Bei der Zustellung stelle ich fest, dass der Scheck auf einen höheren Betrag ausgestellt ist. Der Käufer erklärt, dass er irrtümlich 2.000 Euro zu viel eingesetzt hat. Er ersucht mich, ihm das überschüssige Geld mittels Bargeld-Transfer zurück zu schicken. Auch die Kosten für die Sendung darf ich von seinem Geld abziehen.

Ich löse den Scheck bei meiner Bank ein und erhalte prompt den gesamten Betrag gutgeschrieben. Ich behebe 2.000 Euro und sende diese wie besprochen an den Käufer zurück. Zwei Wochen später fordert meine Bank das Geld wieder zurück, da der Scheck gefälscht war. Jetzt habe ich einen Schaden von 2.000 Euro.

Was liegt vor:

Betrüger antworten auf Inserate oder bestellen diverse Waren und Dienstleistungen, ohne tatsächlich Interesse an dem jeweiligen Angebot zu haben. Sie schicken einen gefälschten Scheck zur Bezahlung, der auf einen höheren Betrag ausgestellt ist als der vereinbarte Kaufpreis. Die Absicht der Betrüger liegt darin, das Opfer möglichst schnell zur Überweisung des Differenzbetrages zu veranlassen. Sobald die Bank den Scheck als Fälschung erkennt, verlangt sie vom Einreicher den gesamten zur Auszahlung gekommenen Geldbetrag zurück.

Somit erleidet das Opfer (der Verkäufer) einen Schaden in Höhe des Geldbetrages, der an den vermeintlichen Käufer zurück überwiesen wurde.

Die Polizei empfiehlt:

→ Bedenken Sie, dass Preisverhandlungen sowie eine vorherige Besichtigung des Kaufobjektes üblich sind und überlegen Sie, ob der Kauf Ihrer Ware durch einen ausländischen Interessenten plausibel ist.

→ Bestehen Sie auf sicheren Zahlungsverkehr (zB. Kontoüberweisung).

→ Lassen Sie sich nicht zu Bargeld-Rücküberweisungen drängen, bevor die Echtheit des Schecks geprüft ist (die Bankprüfung dauert bis zu drei Wochen, bis dahin gilt die Auszahlung nur unter Vorbehalt).

→ Sichern Sie im Schadensfall den E-Mail-Verkehr und stellen Sie ihn der Polizei zusammen mit den Kopien der Überweisungsbelege für die Ermittlungen zur Verfügung.

Finanzagent

Anwerben von Personen, die ihr Konto für betrügerische Geldtransaktionen zur Verfügung stellen sollen.

Was ist passiert:

Ich habe im Internet ein Jobangebot von einem ausländischen Finanzunternehmen bekommen. Ich muss nur mein Girokonto für Überweisungen aus dem Ausland zur Verfügung stellen. Sobald das Geld auf meinem Konto ist, muss ich es beheben und als Bargeld-Zahlung weiterleiten. Als Bezahlung erhalte ich rund 15 % der überwiesenen Beträge. Es geht wohl darum, Steuern zu sparen.

Als ich das Geld von meinem Konto beheben will, wartet bereits die Polizei in der Bank auf mich. Ich muss zu einem Verhör mitkommen und mit einer Anzeige wegen Geldwäsche rechnen.

Was liegt vor:

Personen werden von Betrügern per E-Mail mit dem Angebot einer Nebenbeschäftigung kontaktiert. Die Tätigkeit besteht lediglich darin, das Girokonto für eine Überweisung zur Verfügung zu stellen und nach Weiterleitung des Geldes mit einer verlockenden Provisionszahlung entlohnt zu werden. Das Geld stammt aus strafbaren Handlungen (vorwiegend Konto-Phishing), somit macht sich der angeworbene Finanzagent möglicherweise

selbst strafbar (Geldwäsche) und muss damit rechnen, dass er den gesamten Schadensbetrag bei der Bank erstatten muss.

Die Polizei empfiehlt:

→ Angebote, die unüblich viel Geld für wenig Arbeit bieten, sind zumeist nicht seriös.

→ Antworten Sie nicht auf dubiose Jobangebote.

→ Lehnen Sie Angebote immer ab, bei denen Sie Ihr Konto zur Verfügung stellen müssen.

→ Prüfen Sie Ihre Kontoumsätze auf unerwartete Gutschriften und veranlassen Sie Rückbuchungen nur auf das Ursprungskonto.

→ Stellen Sie der Polizei im Schadensfall E-Mail-Schriftverkehr und Kontounterlagen zur Verfügung.

Vortäuschung einer Notlage

Not- und Katastrophenbettelei per SMS oder E-Mail (Kettenmails oder Briefe mit Spenden- oder Hilfeaufrufen).

Was ist passiert:

Ich erhalte gerade ein E-Mail, in der meine gute Bekannte ihr Leid klagt: Sie ist auf Urlaub, und ihre Tasche samt Ausweisen, Handy und Geldbörse wurde gestohlen. Sie bittet mich um Zusendung von Geld über einen Bargeldtransfer, damit sie ein Ticket für den Heimflug kaufen kann. Natürlich helfe ich gerne und überweise das Bargeld an die angegebene Adresse.

Mir erscheint es komisch, dass sich meine Bekannte auch Wochen später weder bei mir bedankt noch das Geld zurückgezahlt hat.

Was liegt vor:

Ihre Bekannte befindet sich mit größter Wahrscheinlichkeit in keiner Notlage. Die E-Mail-Kontakte Ihrer Bekannten (darunter auch Ihre E-Mail-Adresse) sind einem Betrüger in die Hände gelangt.

Dieser benutzt die Kontakte unter dem Namen Ihrer Bekannten, um Ihre Hilfsbereitschaft auszunutzen. Das von Ihnen gesendete Bargeld wird dann meist im Ausland unter einem falschen Namen behoben und kann nicht mehr zurückgeholt werden.

Die Polizei empfiehlt:

→ Versuchen Sie Kontakt zu Ihrer Bekannten herzustellen oder finden Sie heraus, ob sie sich tatsächlich in dem angegebenen Land auf Urlaub befindet, bevor Sie eine Bargeldüberweisung veranlassen.

→ Machen Sie Ihre Bekannte auf den Betrugsversuch aufmerksam, damit sie ihre anderen Kontakte warnen kann.

→ Sichern Sie den E-Mailverkehr und stellen Sie ihn der Polizei zusammen mit den Kopien der Überweisungsbelege für die Ermittlungen zur Verfügung.

SICHER LEBEN IN GRAZ

www.sicherlebeningraz.at
www.facebook.com/sicherlebeningraz

Graz: Sicher Leben! • Eingetragener Verein • Körblergasse 10, 8010 Graz • ZVR: 066269364