AUSTRALIAN COMPETITION & CONSUMER COMMISSION

Das kleine schwarze Buch der Betrügereien

Eine Anleitung im Taschenformat, mit der Sie Betrügereien erkennen, vermeiden und sich vor ihnen schützen können.

AUSTRALIAN COMPETITION & CONSUMER COMMISSION

Das kleine schwarze Buch der Betrügereien

Eine Anleitung im Taschenformat, mit der Sie Betrügereien erkennen, vermeiden und sich vor ihnen schützen können.

ISBN 978 1 920702 00 7

Australische Verbraucherschutzbehörde
(Australian Competition and Consumer Commission)
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

ACCC 12/16_1129

www.accc.gov.au

Inhalt

Einführung

Jedes Jahr kosten Betrügereien Australier, Unternehmen und die Wirtschaft Hunderte von Millionen Dollar und schädigen die Opfer und ihre Familien emotional.

Sie können sich am besten schützen, indem Sie sich informieren und aufgeklärt sind. Diese neue Ausgabe des *Kleinen schwarzen Buchs der Betrügereien (The Little Black Book of Scams)* wird Ihnen von der australischen Wettbewerbs- und Verbraucherkommission (Australian Competition and Consumer Commission - ACCC), der nationalen Verbraucherschutzbehörde Australiens, zur Verfügung gestellt. Das „Kleine schwarze Buch der Betrügereien" wird international als ein wichtiges Hilfsmittel für Verbraucher und kleine Unternehmen geschätzt, um mehr über Betrugsmethoden zu erfahren:

- die häufigsten Betrugsmethoden
- die verschiedenen Methoden, mit denen Betrüger Kontakt mit Ihnen aufnehmen
- die Mittel und Wege, die Betrüger verwenden, um Sie in die Falle zu locken
- die Warnzeichen
- wie Sie sich selbst schützen können, und
- wo Sie Hilfe erhalten können.

Das kleine schwarze Buch der Betrügereien ist im Internet unter www.accc.gov.au/littleblackbookofscams erhältlich.

So schützen Sie sich—melden Sie sich bei Scamwatch an

Um Betrügern immer einen Schritt voraus zu sein, besuchen Sie die Scamwatch-Website der ACCC—www.scamwatch.gov.au—und erfahren Sie mehr über Betrugsmethoden. Hier können Sie sich für kostenlose E-Mail-Benachrichtigungen über neue Betrügereien anmelden, die auf Verbraucher und kleine Unternehmen abzielen. Sie können Scamwatch auch auf Twitter unter @scamwatch_gov oder unter http://twitter.com/scamwatch_gov folgen.

Die wichtigsten Betrugsfallen, die es zu vermeiden gilt

Jeder ist anfällig für Betrügereien, daher benötigt jeder Informationen darüber, wie man Betrügereien erkennen und vermeiden kann. Manche Leute denken, dass nur leichtgläubige oder gierige Menschen Opfer von Betrügereien werden. In Wahrheit sind Betrüger jedoch sehr clever, und jeder, der nicht weiß, worauf er achten muss, kann Opfer eines Betrugs werden.

Haben Sie ein Angebot erhalten, das zu gut scheint, um wahr zu sein? Oder vielleicht einen Anruf, um Ihren Computer zu reparieren oder eine Drohung, Geld zu zahlen, das Sie nicht schulden, oder eine Warnung Ihrer Bank oder Ihres Telekommunikationsanbieters über ein Problem mit Ihrem Konto? Oder sogar eine Einladung, sich mit Ihnen anzufreunden oder online Kontakt aufzunehmen? Betrüger wissen genau, wie sie Sie dazu bringen, ihnen das zu geben, was sie wollen.

Betrüger werden immer raffinierter und entwickeln sich schnell weiter. Sie nutzen neue Technologien, neue Produkte oder Dienstleistungen, und wichtige Ereignisse, um glaubwürdige Geschichten zu erfinden, mit denen sie Sie überreden, ihnen Ihr Geld oder Ihre persönlichen Daten zu geben.

Dank der Zehntausenden von Anzeigen von Betrügereien, die jedes Jahr bei der ACCC eingehen, hat die ACCC eine Liste der häufigsten Betrugsmethoden erstellt, um die Methoden und Taktiken aufzudecken und bekanntzumachen, von denen Betrüger nicht wollen, dass Sie sie kennen.

Dating- und Beziehungsbetrug

Dating- und Beziehungsbetrug kostet Australier jedes Jahr Millionen von Dollar und kann Einzelpersonen und Familien ruinieren.

Wie der Betrug funktioniert

Dating- und Beziehungsbetrüger erstellen gefälschte Profile auf legitimen Dating-Websites, mobilen Anwendungen oder in sozialen Medien wie Facebook mit Fotos und Identitäten, die oft von anderen Menschen gestohlen wurden. Sie verwenden diese Profile, um eine Beziehung mit Ihnen einzugehen, die sich über Monate oder sogar Jahre erstrecken kann, nur um an Ihr Geld zu kommen. Die Betrüger werden Sie wegen Krankheit, Verletzung, Reisekosten oder einer Familienkrise um Geld bitten. Sie sind herzlos und lügen, um Ihr Mitgefühl auszunutzen.

Betrüger befinden sich in der Regel im Ausland und haben eine Ausrede dafür, warum sie dort sind, wie z.B. sind sie im Militärdienst, arbeiten dort als Ingenieur oder betreuen einen Freund oder Verwandten. Betrüger sind nie die Person, die sie vorgeben zu sein, und raffinierte Betrüger schicken Ihnen möglicherweise kleine Geschenke. Das ist ein Teil ihres Plans, später noch mehr Geld von Ihnen zu erschwindeln.

So schützen Sie sich

- Senden Sie niemals Geld und geben Sie niemals Ihre persönlichen Daten an jemanden weiter, den Sie nur online kennengelernt haben.
- Seien Sie vorsichtig, wenn ein „Bewunderer“ aus dem Internet nach nur wenigen Kontaktaufnahmen oder Gesprächen mit Ihnen außerhalb der Dating-Website oder der sozialen Medien-Plattform kommunizieren möchte – es könnte ein Betrüger sein.
- Suchen Sie nach dem Bild Ihres Bewunderers, um festzustellen, ob er wirklich der ist, der er vorgibt zu sein. Sie können dazu Bildsuchdienste wie Google oder TinEye benutzen.
- Seien Sie vorsichtig damit, intime Fotos oder Videos online zu teilen. Betrüger sind dafür bekannt, ihre Opfer mit Fotos oder Videos zu erpressen, die niemand sonst sehen soll.

Investitionsbetrug

„Risikofreie Anlage"
oder Unglücksfalle?

Wie der Betrug funktioniert

Investitionsbetrug gibt es in vielen Formen, darunter Kryptowährungskauf, Handel mit binären Optionen, Business Ventures, Rentenpläne, verwaltete Fonds und der Verkauf oder Kauf von Aktien oder Immobilien. Betrüger verkleiden die „Gelegenheiten" womöglich mit professionell aussehenden Broschüren und Webseiten, um ihre betrügerischen Aktivitäten zu verschleiern. Der Betrug beginnt oft aus heiterem Himmel mit einem Telefonanruf oder einer E-Mail eines Betrügers, der eine „nicht zu verpassende" Gelegenheit, „hohe Rendite" oder „garantierte" Chance verspricht. Der Betrüger operiert in der Regel von Übersee aus und hat keine australische Lizenz für Finanzdienstleistungen.

Vorhersage-Software-Betrug verspricht die genaue Vorhersage von Börsentrends oder den Ergebnissen von Pferderennen, Sportveranstaltungen oder Lotterien. Diese sind einfach eine Form des Glücksspiels, die als Investitionen getarnt ist. Die meisten der Softwareprogramme oder Vorhersagemethoden funktionieren nicht und Käufer erhalten ihr Geld nicht zurück. In vielen Fällen verschwindet der Anbieter einfach.

Rentenbetrug bietet Ihnen einen frühen Zugang zu Ihrem Rentenfond, oft über einen selbst verwalteten Rentenfond oder gegen eine Gebühr. Der Betrüger bittet Sie zum Beispiel, einer Geschichte zuzustimmen, um die vorzeitige Freigabe Ihres Geldes zu erwirken, und veranlasst dann Ihren Rentenfond, die Leistungen direkt an ihn auszuzahlen, indem er sich als Ihr Finanzberater ausgibt. Sobald er Ihr Geld hat, erhebt der Betrüger entweder eine hohe „Gebühr“ oder behält einfach Ihr Geld.

So schützen Sie sich

- Lassen Sie sich von niemandem dazu drängen, Entscheidungen über Ihr Geld oder Ihre Investitionen zu treffen – vor allem dann nicht, wenn das Angebot aus heiterem Himmel kommt.
- Bevor Sie Ihr Geld aushändigen, recherchieren Sie die Investitionsgesellschaft und besuchen Sie www.moneysmart.gov.au, um herzufinden, ob sie eine australische Finanzdienstleistungslizenz hat. Fragen Sie sich selbst: Wenn ein Fremder ein Geheimnis weiß, wie man viel Geld macht, warum würde er es dann mit Ihnen teilen?

Wenn Sie unter dem Rentenalter sind, seien Sie vorsichtig mit Angeboten, die einen einfachen Zugang zu Ihren Rentenleistungen versprechen. Wenn Sie unrechtmäßig frühzeitig auf Ihre Rente zugreifen, könnten Ihnen steuerrechtliche Sanktionen auferlegt werden.

Strafandrohungsbetrug

Wenn eine Behörde oder ein vertrauenswürdiges Unternehmen Ihnen sagt, dass Sie etwas bezahlen müssen, denken Sie einen Moment nach und überprüfen Sie die Forderung.

Wie der Betrug funktioniert

Anstatt einen Preis, Geld oder eine Rückzahlung anzubieten, verwenden diese Betrüger Drohungen, um Sie dazu zu bringen, aus Angst Ihr Geld auszuhändigen. Der Betrüger ruft Sie zum Beispiel an und droht Ihnen mit Verhaftung, oder er sendet Ihnen eine E-Mail, in der er behauptet, Sie müssen einen **Bußgeldbescheid** für eine Geschwindigkeitsüberschreitung bezahlen oder Sie hätten **Steuerschulden** oder eine **unbezahlte Rechnung**.

Betrüger versuchen, Sie am Telefon unter Druck zu setzen, damit Sie sofort bezahlen, und drohen damit, die Polizei zu Ihrem Haus zu schicken, wenn Sie es nicht tun. Solche Betrüger kontaktieren gerne wehrlose Menschen in der Gemeinschaft, wie zum Beispiel neue Einwanderer. Sie geben vor, Beamte der Einwanderungsbehörde zu sein und drohen ihren Opfern mit **Abschiebung**, wenn diese nicht Gebühren bezahlen, um angebliche Fehler in ihrem Visum zu korrigieren. Andere Betrüger geben vor, vom australischen Finanzamt zu sein und teilen ihren Opfern mit, sie hätten eine ausstehende Steuerschuld.

Betrüger geben auch gerne vor, für **vertrauenswürdige Unternehmen** wie Ihre Bank oder Ihren Gas-, Strom-, Wasser- oder Telefonanbieter zu arbeiten. Sie drohen Ihnen damit, Ihren Service zu kündigen oder Ihnen übermäßige Strafzahlungen in Rechnung zu stellen, wenn Sie die Rechnung nicht sofort bezahlen. Sie können sich auch als ein Unternehmen wie Australia Post ausgeben und Ihnen mitteilen, dass ein Paket für Sie zur Abholung bereitliegt und Ihnen für jeden Tag, den Sie nicht dafür bezahlen, eine Gebühr berechnet

wird. Was auch immer der Fall ist, diese Betrüger versuchen, Sie zu beunruhigen und dazu zu bringen, sofort zu handeln, anstatt zuerst nachzudenken und zu prüfen, ob die Angaben wahr sind.

Wenn der Betrug per E-Mail versendet wird, ist es wahrscheinlich, dass diese einen Anhang oder einen Link zu einer gefälschten Website enthält, auf der Sie aufgefordert werden, den Nachweis der „Rechnung", „Geldstrafe" oder der „Lieferdaten" herunterzuladen. Wenn Sie den Anhang öffnen oder die Datei herunterladen, wird Ihr Computer mit Malware infiziert (siehe Seite 16).

So schützen Sie sich

- Lassen Sie sich nicht von einem Anrufer mit Drohungen unter Druck setzen. Halten Sie inne, denken Sie nach, und überprüfen Sie, ob die Behauptungen wahr sind.
- Eine Behörde oder ein vertrauenswürdiges Unternehmen würde Sie niemals auffordern, mit ungewöhnlichen Zahlungsmethoden wie Geschenkkarten, Bankanweisungen oder Bitcoins zu bezahlen.
- Überprüfen Sie die Identität des Anrufers, indem Sie die zuständige Organisation direkt anrufen oder ihn über eine unabhängige Quelle wie ein Telefonbuch, eine frühere Rechnung oder Online-Suche finden.
- Verwenden Sie nicht die Kontaktdaten, die Ihnen in E-Mails oder am Telefon gegeben wurden. Auch hier gilt: Finden Sie die Daten über eine unabhängige Quelle.

Betrug mit unerwartetem Geld

Seien Sie vorsichtig, wenn Sie aufgefordert werden, für den Erhalt von Waren oder Geld erst eine Zahlung zu leisten.

Wie der Betrug funktioniert

Diese Betrüger teilen Ihnen aus heiterem Himmel mit, dass Sie Anspruch auf Geld, Edelsteine, Gold oder wertvolle Aktien haben, aber Vorabzahlungen leisten müssen, um diese zu erhalten. Sie werden niemals das Versprochene erhalten, nur immer weitere Gründe dafür, warum Sie erst mehr bezahlen müssen. Wenn Sie diese Gebühren bezahlen, werden Sie Ihr Geld verlieren.

Rückzahlungs- oder Rückerstattungsbetrug wird von Betrügern ausgeführt, die Ihnen sagen, dass Ihnen Geld aus Quellen wie Steuerüberzahlung, Bankgebühren oder einer Entschädigung zusteht. Bevor Sie jedoch Ihr Geld erhalten können, werden Sie gebeten, eine kleine Verwaltungsgebühr zu zahlen.

Beim **Erbschaftsbetrug** geben sich Betrüger als Anwälte, Banker oder ausländische Beamte aus und sagen Ihnen, dass Sie Anspruch auf eine große Erbschaft haben, oder sie bieten Ihnen einen Anteil an einem Fond an, weil Sie den gleichen Namen haben wie jemand, der gestorben ist. Diese Betrüger verwenden oft offiziell aussehende Dokumente und bitten Sie, Gebühren und Steuern zu zahlen, bevor Sie die Erbschaft erhalten können. Sie fordern möglicherweise auch Ihre persönlichen Daten an, um „offizielle Papiere“ auszufüllen. Das bedeutet, dass Ihnen neben Ihrem Geld auch Ihre Identität gestohlen wird.

Die allgemein als **nigerianischer Betrug** bekannte Betrügerei hat womöglich ihren Ursprung in Westafrika, kann aber aus der ganzen Welt kommen. Diese Betrüger teilen Ihnen mit, dass sie Ihre Hilfe brauchen, um

ein großes Vermögen zu sichern, das sie verzweifelt versuchen, aus ihrem Land zu schaffen. Sie behaupten zum Beispiel, dass das Vermögen ein versteckter Vorrat an Geld, Gold oder Vermögenswerten ist, der von einer korrupten Regierung oder einem korrupten Beamten zurückgelassen wurde, und wenn Sie zustimmen, ihn in Empfang zu nehmen, erhalten Sie einen großen Anteil davon, sobald es sicher ist. Wie bei allen dieser Betrügereien wird der Betrüger Ihnen sagen, dass Sie zuerst Steuern, Bankgebühren oder Gebühren für die Terrorismusbekämpfung oder für Geldwäscheprüfungen zahlen müssen, bevor er das Geld an Sie versenden kann.

Diese Betrügereien kommen in der Regel aus dem Ausland und fordern Zahlungen per Bankanweisung oder Banküberweisungen oder andere Zahlungsmethoden.

Wenn Sie auf diesen Betrug hereinfallen, werden Sie nie etwas von dem Betrüger erhalten und jegliches Geld, das Sie überwiesen haben, verlieren.

So schützen Sie sich

- Denken Sie daran, dass es keine Zauberformel zum schnellen Reichtum gibt. Wenn etwas zu gut klingt, um wahr zu sein, dann ist es das wahrscheinlich auch.
- Vermeiden Sie Vereinbarungen mit einem Fremden, der eine Vorauszahlung per Zahlungsanweisung, Banküberweisung, internationaler Überweisung, mit Kredit aufgeladener Karte oder elektronischer Währung verlangt. Geld, das auf diese Weise versendet wurde, kann kaum je wieder zurückerlangt werden.
- Wenn eine E-Mail verdächtig aussieht, löschen Sie sie. Klicken Sie auf keine Links.
- Regierungsbehörden, Banken oder Versorgungsunternehmen kontaktieren Sie niemals, um eine Vorauszahlung zu verlangen, damit sie Ihnen eine Gebühr oder eine Zahlung zurückzuerstatten können.
- Wenn Sie sich nicht sicher sind, überprüfen Sie die Identität des Kontakts. Verwenden Sie dazu nicht die Kontaktdaten aus der an Sie gesendeten Nachricht – recherchieren Sie die Kontaktdaten über eine unabhängige Quelle wie ein Telefonbuch oder eine Online-Suche.
- Führen Sie eine Online-Suche mit dem genauen Wortlaut des Angebots durch – viele Betrügereien können so erkannt werden.

Preisausschreiben- und Lotteriebetrug

Lassen Sie sich nicht von einem Überraschungsgewinn verführen – der Betrüger ist der Einzige, der den Gewinn mit nach Hause nimmt.

Wie der Betrug funktioniert

Diese Betrügereien versuchen, Sie dazu zu bringen, eine Vorauszahlung zu leisten oder Ihre persönlichen Daten preiszugeben, um einen Preis aus einer Lotterie, einem Gewinnspiel oder einem Preisausschreiben zu erhalten, an dem Sie nie teilgenommen haben. Betrüger behaupten, dass Sie Gebühren oder Steuern zahlen müssen, bevor Ihr „Gewinn" oder Preis freigegeben werden kann.

Möglicherweise müssen Sie auch eine Telefonnummer mit hohem Tarif anrufen oder eine SMS schicken, um Ihren Gewinn zu erhalten. Beim **Rubbelkarten-Betrug** erhalten Sie Hochglanzbroschüren mit einer Reihe von Rubbelkarten in der Post, von denen eine einen Gewinn verspricht. Damit es glaubwürdiger erscheint, ist der Preis oft nur der zweite oder dritte Preis. Wenn Sie dann anrufen, um Ihren Preis einzulösen, verlangen die Betrüger, dass Sie Gebühren oder Steuern bezahlen, bevor Sie Ihren Gewinn erhalten.

Lotteriebetrüger verwenden möglicherweise die Namen tatsächlicher ausländischer Lotterien und behaupten, dass Sie Bargeld gewonnen haben, obwohl Sie nie an der Lotterie teilgenommen haben. Betrüger verlangen in der Regel Gebühren oder Steuern, um die Gelder freizugeben. Die Betrüger behaupten

außerdem, dass sie Ihre persönlichen Daten benötigen, um nachzuweisen, dass Sie der rechtmäßige Gewinner sind, und verwenden dann diese Informationen, um Ihre Identität oder Ihr Geld von Ihrem Bankkonto zu stehlen.

Betrüger können Ihnen **unechte Gutscheine und Geschenkgutscheine** per E-Mail oder SMS, oder über Nachrichten in sozialen Medien senden. Die Nachricht behauptet, Sie hätten einen Geschenkgutschein für einen bekannten Einzelhändler gewonnen, aber Sie müssen einige Details angeben, bevor Sie ihn in Anspruch nehmen können. Dies ist ein Versuch, personenbezogene Daten zu erhalten, die bei Identitätsdiebstahl verwendet werden können, oder um einen anderen Betrug an Ihnen zu versuchen. Angebote wie diese sind auch dafür bekannt, dass sie Ransomware auf Ihrem Gerät installieren (siehe Seite 17).

Beim **Reisepreisbetrug** behaupten die Betrüger, Sie hätten einen kostenlosen Urlaub oder eine Flugreise gewonnen. Was Sie tatsächlich gewonnen haben, ist die Möglichkeit, Unterkunft oder Fluggutscheine zu kaufen. Diese Reisegutscheine haben oft versteckte Gebühren und Bedingungen oder sie sind gefälscht und wertlos. Manche Betrüger bieten Ihnen erstaunlich vergünstigte Urlaubspakete an, die es gar nicht gibt.

So schützen Sie sich

- Denken Sie daran: Sie können keine Lotterie und kein Preisausschreiben gewinnen, an dem Sie nicht teilgenommen haben.
- Verlosungen und Lotterien verlangen keine Gebühren, um einen Gewinn einzulösen. Suchen Sie den genauen Text des Angebots im Internet. Auf diese Weise kann oft herausgefunden werden, ob es sich um einen Betrug handelt.
- Seien Sie vorsichtig, bevor Sie eine Telefonnummer anrufen oder eine SMS an eine Telefonnummer schicken, die mit „19“ anfängt – diese Nummern haben einen hohen Tarif.

Online-Shopping, Kleinanzeigen und Auktionsbetrug

Betrüger lieben auch die Einfachheit des Online-Shoppings.

Wie der Betrug funktioniert

Verbraucher und Unternehmen kaufen und verkaufen zunehmend online. Leider suchen auch Betrüger gerne online nach Opfern.

Betrüger können sehr überzeugende **fiktive Einzelhändler-Websites** erstellen, die echt aussehen, auch in sozialen Medien wie Facebook. Der wichtigste Hinweis dafür, dass eine Einzelhandels-Website betrügerisch ist, ist die Zahlungsmethode – seien Sie vorsichtig, wenn Sie aufgefordert werden, per Banküberweisung oder anderen ungewöhnlichen Methoden zu bezahlen.

Beim **Online-Auktionsbetrug** behaupten Betrüger, dass Sie eine zweite Chance haben, einen Gegenstand zu kaufen, auf den Sie ein Gebot abgegeben haben, da der Gewinner sein Angebot zurückgezogen hat. Der Betrüger wird Sie bitten, außerhalb der sicheren Zahlungsmöglichkeit der Auktionsplattform zu bezahlen; wenn Sie dies tun, geht Ihr Geld verloren, Sie erhalten die Ware nicht, für die Sie bezahlt haben, und die Auktionsplattform wird Ihnen nicht helfen können.

Betrug mit Online-Kleinanzeigen ist ein weitverbreiteter Betrug, der sowohl auf Käufer als auch Verkäufer abzielt. Käufer sollten sich vor Betrügern hüten, die gefälschte Anzeigen auf legitimen Kleinanzeigen-Websites veröffentlichen. Die Anzeigen können für alles Mögliche sein, von Mietwohnungen bis hin zu Haustieren, Gebrauchtwagen

oder Kameras, und sind oft sehr preiswert. Wenn Sie Interesse an dem Artikel zeigen, behauptet der Betrüger dann, dass er auf Reisen ist oder ins Ausland gezogen ist und dass ein Agent die Ware nach Zahlungseingang liefern wird. Nach der Zahlung erhalten Sie die Ware nicht und können sich auch nicht mehr an den Verkäufer wenden.

Verkäufer erhalten ein großzügiges Angebot auf ihre Anzeige von einem Kleinanzeigen-Betrüger. Wenn Sie es akzeptieren, zahlt der Betrüger per Scheck oder Zahlungsanweisung. Der Betrag, den Sie erhalten, ist jedoch höher als der vereinbarte Preis. Bei diesem **Überzahlungsbetrug** sagt Ihnen der „Käufer" dann, dass dies ein Fehler war und bittet Sie, den Überschussbetrag per Überweisung zurückzuerstatten. Der Betrüger hofft, dass Sie das Geld überweisen, bevor Sie feststellen, dass der Scheck nicht gedeckt ist bzw. die Zahlungsanweisung ungültig ist. Sie verlieren sowohl das Geld als auch die Ware, die Sie verkauft haben, wenn Sie diese bereits geschickt haben.

So schützen Sie sich

- Vergewissern Sie sich, mit wem Sie es zu tun haben. Wenn es sich um einen australischen Einzelhändler handelt, sind Sie wesentlich besser in der Lage, etwas zu tun, wenn etwas schief geht.
- Überprüfen Sie, ob der Verkäufer seriös ist, eine Erstattungsrichtlinie hat und ein Verfahren zur Reklamationsbearbeitung anbietet.
- Vermeiden Sie alle Vereinbarungen, die eine Vorauszahlung per Zahlungsanweisung, Banküberweisung, internationaler Überweisung, mit Kredit aufgeladener Karte oder elektronischer Währung erfordern. Geld, das auf diese Weise gesendet wurde, kann kaum je zurückerlangt werden. Senden Sie niemals Geld und geben Sie keine Kreditkarten- oder Online-Kontoinformationen an jemanden weiter, den Sie nicht kennen oder dem Sie nicht vertrauen, und niemals per E-Mail.
- Bezahlen Sie nur über die sichere Zahlungsmethode der Website – suchen Sie nach einer Webadresse, die mit „https" beginnt und ein geschlossenes Schloss-Symbol aufweist.
- Akzeptieren Sie niemals einen Scheck oder eine Zahlungsanweisung über einen Betrag, der höher ist als der, den Sie vereinbart haben. Leiten Sie kein Geld für jemand anderen weiter.

Computer- und Mobilgerät-Betrug

Denken Sie daran: Alles, was eine Internetverbindung hat, ist anfällig für Betrug.

Wie der Betrug funktioniert

Ein **Computerbetrüger** ruft Sie am Telefon an und behauptet, dass Ihr Computer mit Viren infiziert ist. Wenn Sie seine Anweisungen befolgen, verleihen Sie ihm Fernzugriff auf und Kontrolle über Ihren Computer. Er kann dann Informationen stehlen oder Malware installieren. Er versucht möglicherweise auch, Sie dazu zu überreden, „Antivirensoftware“ zu kaufen, die sich in der Regel als überteuert oder als im Internet frei verfügbar herausstellt.

Malware ist ein Begriff für jede bösartige Software, die auf Ihrem Computer oder anderen Geräten installiert werden kann, darunter Viren, Spyware, Ransomware, Trojaner und Tastatureingabeprotokollierung.

Tasteneingabeprotokollierung und Spyware ermöglichen es Betrügern, das aufzuzeichnen, was Sie auf Ihrer Tastatur eingeben. Damit finden sie Passwörter und Bankverbindungen heraus und können auf Ihre persönlichen Informationen zugreifen und diese überall hin versenden. Einmal installiert, können Betrüger Ihre E-Mail- und Benutzerkonten in sozialen Medien kontrollieren und alle Informationen auf Ihrem Gerät abrufen, einschließlich Passwörter.

Sie können auch Ihre Benutzerkonten verwenden, um andere Betrugsfallen an Ihre Freunde und Familie zu senden.

Ransomware ist eine Art von Malware, die Ihr Gerät verschlüsselt oder sperrt. Sie werden erpresst, einen Betrag zu zahlen, um es wieder zu entsperren. Die Bezahlung zu leisten garantiert nicht, dass Ihr Gerät entsperrt wird oder frei von versteckten Viren ist. Diese können sich dann auf andere Computer oder Geräte in Ihrem Netzwerk ausbreiten und diese infizieren.

Malware wird häufig per E-Mail verbreitet und kommt oft aus scheinbar legitimen Quellen, wie z.B. Ihrem Versorgungsunternehmen, einer Regierungsbehörde oder sogar der Polizei, die vorgibt, eine Geldstrafe verhängt zu haben. Klicken Sie auf keine Links und öffnen Sie keine Anhänge, bei denen Sie sich nicht absolut sicher sind. Sie könnten auf diese Weise bösartige Software herunterladen. Diese Betrügereien richten sich sowohl an Einzelpersonen als auch an Unternehmen.

So schützen Sie sich

- Seien Sie vorsichtig mit kostenlosen Downloads von Musik, Spielen, Filmen und Zugang zu Pornographie-Webseiten. Diese könnten ohne Ihr Wissen schädliche Programme auf Ihrem Computer installieren.
- Schützen Sie Ihre Büronetzwerke, Computer und mobilen Geräte. Aktualisieren Sie Ihre Antivirenprogramme, ändern Sie Passwörter regelmäßig und sichern Sie Ihre Daten. Speichern Sie Ihre Backups an einem anderen Ort und offline. Informationen dazu, wie Sie Ihre Daten und Ihre mobilen Geräte sichern können, finden Sie unter www.staysmartonline.gov.au.
- Öffnen Sie keine Anhänge und klicken Sie auf keine Links in E-Mails oder sozialen Medien-Nachrichten, die Sie von Fremden erhalten haben – klicken Sie auf Löschen.

Identitätsdiebstahl

Jeder Betrug hat das Potenzial für Identitätsdiebstahl. Sich vor Betrügereien zu schützen bedeutet auch, Ihre persönlichen Daten zu schützen.

Jeder Betrug kann Identitätsdiebstahl beinhalten

Die meisten Menschen verbinden Betrügereien mit Versuchen, an Ihr Geld zu kommen. Aber Ihre persönlichen Daten sind für Betrüger ebenso wertvoll. Betrüger stehlen diese für betrügerische Aktivitäten wie unbefugte Einkäufe mit Ihrer Kreditkarte, oder sie verwenden Ihre Identität zur Eröffnung von Bank- und Telefonkonten. Sie können Kredite aufnehmen oder andere illegale Geschäfte in Ihrem Namen tätigen. Sie können Ihre Daten sogar an andere Betrüger weitergeben, die diese dann zur weiteren illegalen Verwendung verkaufen.

Der Diebstahl Ihrer Identität kann sowohl finanziell als auch emotional verheerend sein. Es kann Monate dauern, bis Sie Ihre Identität wiedererlangen, und die Auswirkungen des Diebstahls können jahrelang anhalten.

Phishing – ein Betrüger kontaktiert Sie aus heiterem Himmel per E-Mail, Telefon, Facebook oder SMS, und gibt vor, von einem legitimen Unternehmen wie einer Bank, einem Telefon- oder Internetdienstanbieter zu sein. Er leitet Sie zu einer gefälschten Version der Website des Unternehmens und fragt nach Ihren persönlichen Daten, um Kundendaten aufgrund eines technischen Fehlers zu überprüfen. Oder er behauptet, ein Luxusgüterhändler zu sein, der Sie anruft, weil jemand angeblich versucht, Ihre Kreditkarte zu benutzen. Er rät Ihnen, Ihre Bank zu kontaktieren, legt aber nicht auf und hält die Leitung offen. Wenn Sie dann versuchen, Ihre Bank anzurufen, sprechen Sie immer noch mit dem Betrüger. Er simuliert ein echtes Telefongespräch, imitiert

Bankmitarbeiter und fragt nach Ihren Konto- und Sicherheitsdaten. In beiden Fällen sammelt der Betrüger alle Informationen, die Sie ihm geben, und verwendet sie dann, um auf Ihre Konten zuzugreifen.

Fingierte Umfragen – Diese Betrüger versprechen Preise und Prämien wie zum Beispiel Geschenkgutscheine für namhafte Einzelhändler als Gegenleistung für das Ausfüllen einer Online-Umfrage. Die Umfrage erfordert, dass Sie eine Reihe von Fragen beantworten, einschließlich Fragen zur Offenlegung wichtiger Identifikations- und Bankdaten.

Bestandteil eines anderen Betrugs – Betrüger fragen oft im Zuge eines Betrugs nach persönlichen Daten. In einem Lotteriebetrug zum Beispiel fragen Betrüger oft nach Ihrem Führerschein oder Reisepass, um „Ihre Identität zu bestätigen, bevor sie das Preisgeld freigeben können". Beim Dating- und Beziehungsbetrug fragen Betrüger möglicherweise nach Informationen, um ihren Visumsantrag „zu sponsern, damit sie Sie in Australien besuchen können".

Denken Sie daran: Die Weitergabe persönlicher Daten an einen Betrüger kann genauso schlimm sein wie die Weitergabe von Geld. Geben Sie Ihre persönlichen Daten nicht weiter und bewahren Sie sie sicher auf.

So schützen Sie sich

- **Seien Sie vorsichtig damit, was Sie in einer Online-Umgebung sagen oder tun**

  Seien Sie vorsichtig beim Austausch von Informationen über sich selbst online, einschließlich in sozialen Medien, Blogs und anderen Online-Foren. Halten Sie inne und denken Sie nach, bevor Sie Umfragen ausfüllen, an Wettbewerben teilnehmen, auf Links oder Anhänge klicken oder auch bevor Sie jemanden „befreunden", „liken" oder etwas online „teilen".

- **Seien Sie wachsam, wenn Ihre Daten oder Geld verlangt werden**

  Betrüger versuchen, Sie zur Übergabe Ihrer Daten zu verleiten, indem sie die Namen bekannter Unternehmen oder Regierungsstellen verwenden. Wenn Sie denken, dass es sich um einen Betrug handelt, reagieren Sie nicht. Überprüfen Sie die Kontaktdaten der Organisation mittels des Telefonbuchs oder einer Online-Suche. Verwenden Sie niemals die in der ursprünglichen Anfrage angegebenen Kontaktdaten.

Wenn Sie Betrügern personenbezogene Daten gegeben haben, rufen Sie IDCARE unter der Nummer 1300 432 273 an.

Job und Beschäftigungsbetrug

Großes Einkommen garantiert?
Unwahrscheinlich!

Wie der Betrug funktioniert

Job- und Beschäftigungsbetrug beinhaltet Angebote, von zu Hause aus zu arbeiten oder in eine „Geschäftsmöglichkeit" zu investieren. Betrüger versprechen einen Job, ein hohes Gehalt bzw. eine hohe Investitionsrendite nach ersten Vorauszahlungen. Diese Zahlungen sind zum Beispiel für einen „Business-Plan", Schulungskurs, Software, Uniformen, Sicherheitsüberprüfung, Steuern oder Gebühren. Wenn Sie die Gebühr bezahlen, erhalten Sie möglicherweise gar nichts oder nicht das, was Sie erwartet haben oder Ihnen versprochen wurde.

Einige Stellenangebote können eine Verkleidung für **illegale Geldwäsche** sein. Sie werden gebeten, als „Kundenbetreuer" oder „persönlicher Assistent" zu fungieren, Zahlungen auf Ihr Bankkonto für eine Provision zu erhalten, und das Geld dann an eine ausländische Firma weiter zu überweisen.

Solche Jobbetrügereien werden oft über Spam-Mails, in bekannten Kleinanzeigen oder in Jobbörsen angeboten – manchmal sogar auf staatlichen Websites für Stellenangebote.

Eine große Gefahr bei diesen Jobbetrügereien besteht darin, dass Sie womöglich nach vielen persönlichen Daten gefragt werden, die Sie nicht angeben sollten, zum Beispiel Ihre Steuernummer und Kopien

Ihres Reisepasses oder Führerscheins. Diese Informationen können später zum Identitätsdiebstahl verwendet werden.

So schützen Sie sich

- Hüten Sie sich vor Jobangeboten oder Geschäftsplänen, die ein garantiertes Einkommen versprechen oder eine Vorauszahlung verlangen.
- Willigen Sie niemals ein, Geld für jemand anderen zu überweisen – das ist Geldwäsche und illegal.
- Geben Sie weder Ihre Steuernummer noch Ihren Führerschein oder Reisepass heraus, wenn Sie sich um einen Job bewerben. Es kann sein, dass Sie diese Informationen später angeben müssen, wenn Sie mit der Arbeit beginnen.

Geldwäsche ist eine Straftat: Willigen Sie niemals ein, für einen Fremden Geld zu überweisen.

Wohltätigkeits- und medizinischer Betrug

Betrüger sind herzlos und nutzen Notlagen, um Opfer zu auszunutzen.

Wie der Betrug funktioniert

Betrüger nutzen Menschen aus, die für einen guten Zweck spenden möchten oder eine Lösung für ein Gesundheitsproblem finden wollen.

Beim **Wohltätigkeitsbetrug** sammeln Betrüger Geld, indem sie vorgeben, für eine legitime Spendenaktion oder Wohltätigkeitsorganisation zu arbeiten, oder auch für eine fiktive, die sie selbst erfunden haben. Diese Betrüger nutzen oft eine Naturkatastrophe oder Krise, über die in den Nachrichten berichtet wurde.

Diese Betrügereien nehmen dringend benötigte Spenden von legitimen Wohltätigkeitsorganisationen weg. Wohltätigkeitsorganisationen müssen bei der Regierung registriert sein. Damit Ihre Spende an die richtige Stelle gelangt, überprüfen Sie zuerst die Registrierung.

Der Betrug mit **Wunderheilmitteln** bietet eine Reihe von Produkten und Dienstleistungen, die als legitime alternative Medikamente erscheinen und in der Regel die schnelle und wirksame Heilung schwerer Krankheiten versprechen. Die Behandlungen werden oft

durch falsche Aussagen von Menschen untermauert, die erfolgreich „geheilt“ wurden.

Der **Gewichtsabnahmebetrug** verspricht eine drastische Gewichtsabnahme mit nur geringer oder ohne jegliche Anstrengung. Diese Art von Betrug wird zum Beispiel in Form einer ungewöhnlichen Diät, einer revolutionären körperlichen Betätigung, eines „fettabbauenden“ Geräts, oder als Tabletten, Pflaster oder Cremes angeboten. Möglicherweise müssen Sie eine große Anzahlung leisten oder einen langfristigen Vertrag abschließen, um laufende Lieferungen zu erhalten.

Falsche Online-Apotheken bieten Imitat-Medikamente zu sehr günstigen Preisen an und stellen diese manchmal ohne ärztliches Rezept zur Verfügung. Diese Medikamente enthalten unter Umständen nur eingeschränkte oder gar keine Wirkstoffe, was tödliche Folgen für Anwender haben kann.

So schützen Sie sich

- Wenn Sie auf der Straße von einem Mitarbeiter einer Wohltätigkeitsorganisation um eine Spende gebeten werden, fragen Sie nach seinem Ausweis. Wenn Sie Zweifel an der Authentizität der Person haben, spenden Sie nichts.
- Prüfen Sie die Liste der registrierten Wohltätigkeitsorganisationen der Vereinigung gemeinnütziger australischer Wohltätigkeitsorganisationen (Australian Charities Not for Profit Association).
- Sprechen Sie mit Ihrem Arzt, wenn Sie ein Angebot eines „Wundermittels“ oder einer „Sofortheilung“ durch ein Medikament, Nahrungsergänzungsmittel oder eine alternative Behandlung erwägen.
- Fragen Sie sich selbst: Wenn dies wirklich ein Wundermittel ist, hätte Ihnen Ihr Arzt nicht davon erzählt?

Unternehmensbetrug

Betrüger nutzen den Zeitmangel vieler Unternehmen, um sie zu betrügen.

Wie der Betrug funktioniert

Betrügereien, die auf Unternehmen abzielen, existieren in allen möglichen Formen und werden gerne zu Zeiten durchgeführt, an denen sehr viel los ist, wie zum Beispiel am Ende des Geschäftsjahres.

Betrug mit fingierten Rechnungen ist der häufigste Trick, der von Betrügern gegen Unternehmen angewendet wird. Betrüger stellen fingierte Rechnungen für nicht angeforderte bzw. nicht autorisierte Anzeigen, Werbungen, Produkte oder Dienstleistungen aus. Der Branchenverzeichnis-Betrug ist ein bekanntes Beispiel. Sie erhalten eine Rechnung für die Aufnahme in ein vermeintlich bekanntes Branchenverzeichnis. Die Betrüger verleiten Sie zum Abonnement, indem sie das Angebot als ausstehende Rechnung oder kostenlose Anzeige tarnen, die jedoch mit einem im Kleingedruckten versteckten Abonnementvertrag verbunden ist.

Der **Domainnamenbetrug** ist ein weiterer Trick, der von Betrügern angewendet wird. Sie werden verleitet, sich für eine unerbetene Internet-Domain zu registrieren, die Ihrer eigenen sehr ähnlich ist. Oder Sie erhalten einen gefälschten Verlängerungsbescheid für Ihren tatsächlichen Domainnamen und bezahlen ihn, ohne es zu merken.

Bei einem **Bürobedarfsbetrug** werden Ihnen Produkte geschickt und in Rechnung gestellt, die Sie nicht bestellt haben. Diese Betrügereien beinhalten oft Produkte oder Dienstleistungen, die Sie regelmäßig bestellen, wie Schreibwaren und Reinigungsmittel. Betrüger rufen Ihr

Unternehmen an und geben vor, dass die Dienstleistung oder die Waren bereits bestellt wurden.

Beim **Zahlungsumleitungsbetrug** verwenden Betrüger Informationen, die sie durch einen Hackerangriff auf Ihr Computersystem erhalten haben. Sie geben sich als einer Ihrer Stammlieferanten aus und sagen Ihnen, dass sich ihre Bankverbindung geändert hat, da sie vor kurzem die Bank gewechselt hätten. Die Betrüger verwenden unter Umständen kopierte Briefköpfe und Markenzeichen, um Sie davon zu überzeugen, dass die Angaben legitim sind. Sie erhalten eine neue Kontonummer und werden gebeten, alle zukünftigen Zahlungen entsprechend der neuen Bankverbindung abzuwickeln.

Dieser Betrug wird oft erst dann aufgedeckt, wenn Ihr regulärer Lieferant nachfragt, warum seine Rechnungen nicht bezahlt wurden.

Ransomware kann für ein Unternehmen extrem schädlich sein. Die beste Verteidigung ist, Ihre Daten regelmäßig zu sichern und Ihre Backups an einem anderen Ort und offline zu speichern. Weitere Informationen finden Sie auf Seite 17.

So schützen Sie sich

- Stimmen Sie Angeboten oder Geschäften nicht sofort zu – fordern Sie immer ein schriftliches Angebot ein und lassen Sie sich von unabhängiger Seite beraten, wenn es sich um ein Angebot handelt, das Geld, Zeit oder eine langfristige Verpflichtung erfordert.
- Geben Sie die Bank-, Finanz- und Buchhaltungsdaten Ihres Unternehmens niemals an jemanden weiter, der Sie unerwartet kontaktiert und den Sie nicht kennen oder dem Sie nicht vertrauen.
- Effektive Managementverfahren können einen großen Beitrag zur Verhinderung von Betrug leisten - richten Sie klar definierte Prozesse zur Überprüfung und Bezahlung von Rechnungen ein und prüfen Sie Anträge auf Änderung von Bankdaten sehr sorgfältig.
- Schulen Sie Ihre Mitarbeiter, Betrügereien zu erkennen.
- Sichern Sie Ihre Geschäftsdaten an einem anderen Ort und offline.
- Seien Sie achtsam bei E-Mails, die eine Änderung von Bankdaten verlangen. Bestätigen Sie Änderungen von Zahlungsdaten immer direkt mit dem Unternehmen oder der Person.

Wie Betrügereien funktionieren—die Anatomie eines Betrugs

Die meisten Betrügereien folgen dem gleichen Muster, und sobald Sie dieses Muster verstehen, sind die Tricks von Betrügern leichter zu erkennen.

Wenn Sie sich die verschiedenen Arten von Betrug in diesem Buch genau ansehen, werden Sie feststellen, dass die meisten drei Phasen durchlaufen: (1) Kontaktaufnahme, (2) Kommunikation und (3) Zahlung.

Wenn Sie die grundlegenden Bestandteile von Betrügereien verstehen, können Sie die aktuellen Betrugsmethoden vermeiden und sich vor neuen Betrügereien schützen, die in der Zukunft auftauchen.

1. Kontaktaufnahme: Annäherungsmethode

Wenn Betrüger Sie kontaktieren, werden sie Ihnen immer eine Geschichte präsentieren, die Sie dazu verleiten soll, einer Lüge zu glauben. Der Betrüger gibt vor, jemand zu sein, der er nicht ist, zum Beispiel ein Regierungsbeamter, ein erfahrener Investor, ein Lotteriemitarbeiter oder sogar ein Bewunderer.

Um Ihnen diese Lügen zu vermitteln, verwenden Betrüger eine Reihe von Kommunikationsmethoden.

Online

Betrüger lauern in der anonymen Umgebung des Internets.

E-Mail ist eine beliebte Methode der Kontaktaufnahme, da sie eine kostengünstige und einfache Möglichkeit bietet, in großem Umfang zu kommunizieren. Phishing-E-Mails, die nach Ihren persönlichen Daten fragen, sind die häufigste Art von E-Mail-Betrug.

Soziale Netzwerke, Dating-Sites und Online-Foren ermöglichen es Betrügern, sich mit Ihnen „anzufreunden" und in Ihr persönliches Leben einzutreten, um auf Ihre persönlichen Daten zuzugreifen, die dann gegen Sie oder Ihre Familie und Freunde verwendet werden können.

Online-Shopping, Kleinanzeigen und Auktionsseiten werden von Betrügern genutzt, um Käufer und Verkäufer zu kontaktieren, wobei der erste Kontakt sowohl über seriöse und vertrauenswürdige Seiten als auch über gefälschte Webseiten erfolgen kann, die wie die echte Website aussehen. Suchen Sie nach sicheren Zahlungsmöglichkeiten und hüten Sie sich vor ungewöhnlichen Zahlungsmethoden wie Banküberweisung, Bitcoins oder mit Kredit aufgeladenen Geldkarten. Kreditkarten bieten in der Regel einen gewissen Schutz.

Am Telefon

Betrüger rufen auch an oder schicken SMS-Nachrichten.

Telefonanrufe an Haushalte und Unternehmen werden von Betrügern in einer Reihe von Betrügereien verwendet. Diese rangieren von Steuerbetrug bis hin zu Angeboten von Preisen und „Hilfe“ bei Computerviren. Dank günstiger Telefonverbindungen mit Sprachübertragung über das Internet (VOIP) können Call-Centers im Ausland mit Telefonnummern anrufen, die wie lokale Nummern aussehen. Die Identität des Anrufers kann so leicht verschleiert werden und ist einer der vielen Tricks, mit denen Betrüger Sie täuschen.

Eine Reihe von Betrügereien werden über **SMS-Textnachrichten** versendet, darunter Verlosungen und Preisausschreiben. Wenn Sie antworten, werden Ihnen hohe Telefontarife berechnet oder Sie werden bei einem Abonnement-Service angemeldet. Es ist sicherer, nicht zu antworten und nicht auf Links in SMS-Nachrichten zu klicken, es sei denn, Sie wissen, von wem sie stammen. Die Textnachrichten können auch Anhänge und Links zu bösartiger Software in Form von Fotos, Songs, Spielen oder Anwendungen enthalten.

An Ihrer Haustür

Passen Sie auf – Manche Betrüger versuchen, Sie an der Haustür zu betrügen.

Betrug mit Haustürgeschäften beinhaltet in der Regel Betrüger, die Waren oder Dienstleistungen anbieten, die dann nicht geliefert werden oder von sehr schlechter Qualität sind. Möglicherweise werden Ihnen sogar Arbeiten in Rechnung gestellt, die Sie nicht wollten oder denen Sie nicht zugestimmt haben. Ein häufiger Betrug an der Haustür wird von zweifelhaften Handwerkern vorgenommen, die von Ort zu Ort ziehen, schäbige Reparaturen ausführen oder einfach nur Ihr Geld nehmen und verschwinden.

Legitime Unternehmen dürfen an der Haustür verkaufen, müssen sich aber eindeutig identifizieren und eine Reihe anderer Regeln befolgen. Sie haben spezifische Rechte in Bezug auf Haustürgeschäfte, einschließlich das Recht auf Widerruf – erfahren Sie mehr unter www.accc.gov.au/doortodoor.

Betrüger können sich als **unechte Wohltätigkeitsmitarbeiter** ausgeben, um Spenden zu sammeln. Sie nutzen gerne die jüngsten Ereignisse wie Überschwemmungen und Buschbrände. Bevor Sie spenden, bitten Sie um einen Ausweis und sehen Sie sich das offizielle Quittungsbuch an.

Postversand wird verwendet, um **Lotterie- und Verlosungsbetrug, Investitionsmöglichkeiten, nigerianische Betrügereien** und **gefälschte Erbschaftsbriefe** zu versenden. Eine Hochglanzbroschüre ist keine Garantie dafür, dass ein Angebot legitim ist.

Unabhängig von der Art der Kontaktaufnahme, die ein Betrüger verwendet, ist seine Geschichte immer nur der Köder. Wenn Sie anbeißen, wird der Betrüger versuchen, auf die nächste Stufe fortzuschreiten.

2. Kommunikation und Anbahnung

Wenn Sie dem Betrüger die Chance geben, mit Ihnen zu reden, wird er anfangen, seine Tricks anzuwenden, um Sie dazu zu verleiten, Ihr Geld auszuhändigen.

Diese Tricks beinhalten unter anderem die folgenden Methoden:

- Betrüger erfinden aufwendige, aber überzeugende Geschichten, um das zu bekommen, was sie wollen.
- Betrüger verwenden Ihre persönlichen Daten, damit Sie glauben, dass Sie in der Vergangenheit bereits mit ihnen zu tun hatten und um den Betrug legitim erscheinen zu lassen.
- Betrüger kontaktieren Sie regelmäßig, um Vertrauen aufzubauen und Sie davon zu überzeugen, dass er Ihr Freund, Partner oder Liebesinteresse ist.
- Sie nutzen Ihre Gefühle aus, zum Beispiel die Freude über einen großen Gewinn, Hoffnung auf ewige Liebe, Mitleid für einen tragischen Unfall, Schuldgefühle über mangelnde Unterstützung, oder Angst vor Verhaftung oder einer Geldstrafe.
- Betrüger erschaffen gerne den Eindruck von Dringlichkeit, damit Sie keine Zeit haben, die Sache zu durchdenken und aufgrund von Emotionen anstatt logischer Überlegung handeln.
- Betrüger verwenden Verkaufstaktiken, die Sie unter Druck setzen, wie die Behauptung, dass ein Angebot begrenzt ist, Preise steigen werden, oder dass sich der Markt ändert und die Gelegenheit verschwinden wird.
- Ein Betrug kann alle Anzeichen eines echten Unternehmens besitzen und Hochglanzbroschüren mit Branchenjargon verwenden, unterstützt durch Bürofronten, Call-Centers und professionelle Websites.
- Mithilfe des Internets und cleverer Software ist es für Betrüger einfach, gefälschte und offiziell aussehende Dokumente zu erstellen. Ein Dokument, das von der Regierung genehmigt zu sein scheint oder mit juristischem Fachjargon gefüllt ist, kann einem Betrug einen Anschein der Autorität verleihen.

Die Tricks der Betrügers sind so konzipiert, Ihre Achtsamkeit abzubauen, Sie dazu zu bringen, einer Geschichte zu glauben, und dann schnell und irrational zu handeln und zur Endphase überzugehen – der Aushändigung Ihres Geldes.

3. Aushändigung von Geld

Der größte Hinweis dafür, dass Sie es mit einem Betrug zu tun haben, ist die verlangte Zahlungsweise.

Die Forderung nach Geld kann innerhalb weniger Minuten nach dem Betrug oder nach Monaten der sorgfältigen Anbahnung erfolgen. Betrüger haben ihre bevorzugten Zahlungsmethoden.

Betrüger leiten bekannterweise Opfer zu ihrer nächstgelegenen **Geldüberweisungsstelle** (Postamt, Überweisungsdienst oder sogar zur Bank), damit sie Geld senden. Es wurde berichtet, dass sie am Telefon bleiben, spezifische Anweisungen geben und möglicherweise sogar ein Taxi schicken, um mit der Geldsendung zu helfen. Betrüger akzeptieren Geld in allen Formen, einschließlich **direkter Überweisungen, mit Kredit aufgeladener Debitkarten, Geschenkgutscheine, Google Play, Steam oder iTunes-Karten** oder virtuelle Währungen wie Bitcoin. Jede Zahlungsaufforderung mit einer ungewöhnlichen Methode ist ein eindeutiger Hinweis darauf, dass es sich um einen Betrug handelt.

Kreditkarten bieten in der Regel einen gewissen Schutz. Suchen Sie auch nach sicheren Zahlungsoptionen, bei denen „https“ in der Webadresse steht und die Seite ein geschlossenes Schloss-Symbol aufweist.

Senden Sie niemals Geld an jemanden, den Sie nur online oder über das Telefon kennen - besonders wenn er sich im Ausland befindet.

Betrüger können auch Zahlungen in Form von wertvollen Waren und teuren Geschenken wie Schmuck oder Elektronik verlangen. Das Bezahlen von Geld an Betrüger ist nicht das Einzige, worüber Sie sich Sorgen machen sollten - wenn Sie für einen Fremden Geld überweisen, könnten Sie sich unwissentlich an **illegalen Geldwäscheaktivitäten** beteiligen.

Die goldenen Regeln, um sich selbst zu schützen

Denken Sie immer daran, dass es Betrüger gibt. Wenn Sie unaufgefordert von Personen oder Unternehmen kontaktiert werden, sei es am Telefon, per Post, E-Mail, persönlich oder auf einem sozialen Netzwerk, ziehen Sie immer die Möglichkeit in Betracht, dass es sich um eine Betrugsfalle handeln könnte. Wenn etwas zu gut scheint, um wahr zu sein, dann ist es das wahrscheinlich auch.

Finden Sie heraus, mit wem Sie es zu tun haben. Wenn Sie jemanden ausschließlich online getroffen haben oder sich nicht sicher sind, ob ein Unternehmen legitim ist, nehmen Sie sich die Zeit für weitere Recherchen. Führen Sie eine Google-Bildsuche nach Fotos durch oder suchen Sie im Internet nach anderen, die Erfahrungen mit dieser Person gemacht haben.

Öffnen Sie keine verdächtigen SMS-Nachrichten, Popup-Fenster oder E-Mails – löschen Sie sie. Wenn Sie sich nicht sicher sind, überprüfen Sie die Identität des Kontakts über eine unabhängige Quelle wie ein Telefonbuch oder eine Online-Suche. Verwenden Sie nicht die Kontaktdaten, die in der Ihnen zugesandten Nachricht angegeben werden.

Bewahren Sie Ihre persönlichen Daten sicher auf. Verschließen Sie Ihren Briefkasten und schreddern Sie Rechnungen und andere wichtige Dokumente, bevor Sie sie wegwerfen. Bewahren Sie Ihre Passwörter und PIN-Nummern an einem sicheren Ort auf. Seien Sie sehr vorsichtig damit, personenbezogene Daten auf Social Media-Websites weiterzugeben. Betrüger können Ihre Informationen und Bilder verwenden, um eine gefälschte Identität zu erstellen oder Sie zu betrügen.

Achten Sie auf ungewöhnliche Zahlungsmethoden. Betrüger bitten oft um Zahlung per Banküberweisung, mit Kredit aufgeladenen Karten und sogar Google Play, Steam oder iTunes-Karten und Bitcoin. Diese sind fast immer ein Zeichen dafür, dass es sich um einen Betrug handelt.

Schützen Sie Ihre mobilen Geräte und Computer. Verwenden Sie immer einen Passwortschutz, teilen Sie den Zugang mit niemanden (auch keinen Fernzugriff), aktualisieren Sie Ihre Sicherheitssoftware regelmäßig und sichern Sie Ihre Daten. Schützen Sie Ihr WLAN-Netzwerk mit einem Passwort und vermeiden Sie die Verwendung öffentlicher Computer oder WLAN-Hotspots, um auf Online-Banking zuzugreifen oder persönliche Daten einzugeben.

Wählen Sie Ihre Passwörter sorgfältig. Wählen Sie Passwörter, die für andere schwer zu erraten sind und aktualisieren Sie sie regelmäßig. Ein sicheres Passwort sollte eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Symbolen enthalten. Verwenden Sie nicht für jedes Benutzerkonto/Profil das gleiche Passwort und geben Sie Ihre Passwörter nicht an Dritte weiter.

Seien Sie achtsam bei allen Anfragen zu Ihren Daten und Geldforderungen. Senden Sie niemals Geld und geben Sie niemals Kreditkartennummern, Online-Kontoinformationen oder Kopien von persönlichen Dokumenten an jemanden weiter, den Sie nicht kennen oder dem Sie nicht vertrauen. Stimmen Sie nicht zu, Geld oder Waren für jemand anderen zu senden: Geldwäsche ist eine Straftat.

Seien Sie vorsichtig beim Online-Shopping. Hüten Sie sich vor Angeboten, die zu gut scheinen, um wahr zu sein, und nutzen Sie immer einen Online-Einkaufservice, den Sie kennen und dem Sie vertrauen. Überlegen Sie gut, bevor Sie virtuelle Währungen (wie Bitcoin) verwenden – diese bieten nicht den gleichen Schutz wie andere Transaktionsmethoden, was bedeutet, dass Sie Ihr Geld nicht zurückerlangen können, wenn Sie es einmal gesendet haben.

Wo Sie Hilfe und Unterstützung finden können

Wenn Sie Geld an einen Betrüger verloren haben oder Ihre persönlichen Daten an einen Betrüger weitergegeben haben, werden Sie Ihr Geld wahrscheinlich nicht zurückbekommen. Es gibt jedoch Maßnahmen, die Sie augenblicklich ergreifen können, um den Schaden zu begrenzen und sich vor weiteren Verlusten zu schützen.

Kontaktieren Sie Ihre Bank oder Ihr Kreditinstitut

Wenn Sie Geld oder persönliche Bankdaten an einen Betrüger weitergegeben haben, wenden Sie sich sofort an Ihre Bank oder Ihr Kreditinstitut. Diese können möglicherweise eine Geldüberweisung oder einen Scheck stoppen oder Ihr Konto schließen, wenn der Betrüger Ihre Kontodaten hat. Ihr Kreditkartenanbieter kann möglicherweise eine „Rückbelastung" (Stornierung der Transaktion) durchführen, wenn Ihre Kreditkarte unrechtmäßig belastet wurde.

Wiederherstellung Ihrer gestohlenen Identität

Wenn Sie vermuten, dass Sie ein Opfer von Identitätsdiebstahl geworden sind, ist es wichtig, dass Sie schnell handeln, um die Gefahr finanzieller Verluste oder anderer Schäden zu reduzieren.

Wenden Sie sich an **IDCARE** - ein kostenloser, von der Regierung finanzierter Service, der Opfer von Identitätsverbrechen unterstützt. IDCARE kann Ihnen bei der Entwicklung eines Aktionsplans helfen, die geeigneten Maßnahmen zu ergreifen, um die Schädigung Ihres Rufs, Ihrer Kreditwürdigkeit und Ihrer Identität zu beheben. Besuchen Sie die IDCARE-Website unter www.idcare.org oder rufen Sie 1300 432 273 an.

Beantragen Sie ein Opferzertifikat des Commonwealth (**Commonwealth Victims' Certificate**) – damit können Sie nachweisen, dass Sie Opfer eines Identitätsverbrechens geworden sind und Ihre Legitimation bei Behörden und Finanzinstituten wiederherstellen. Besuchen Sie die Website der Generalstaatsanwaltschaft unter www.ag.gov.au (oder rufen Sie 02 6141 6666 an), um mehr über den Schutz und die Wiederherstellung Ihrer Identität zu erfahren.

Wenden Sie sich an eine Beratungs- oder Unterstützungsstelle

Wenn Sie oder ein Bekannter betrogen wurden und an emotionalem Stress oder Depressionen leiden, wenden Sie sich an Ihren Hausarzt, einen örtlichen Gesundheitsdienst oder an jemanden, dem Sie vertrauen. Sie können auch Beratungs- und Unterstützungsdienste kontaktieren, darunter:

Lifeline—Wenn Sie in einer Krise Unterstützung benötigen, kontaktieren Sie Lifeline unter 13 11 14 (rund um die Uhr) oder besuchen Sie www.lifeline.org.au

Beyondblue—Informationen bei Depressionen oder Angstzuständen erhalten Sie von beyondblue unter der Nummer 1300 224 636 oder unter www.beyondblue.org.au

Kids helpline—Telefon- und Online-Beratungs- und Betreuungsdienst für junge Menschen im Alter zwischen 5 und 25 Jahren. Kontaktieren Sie die Kids Helpline unter 1800 551 800 oder besuchen Sie www.kidshelpline.com.au

Finanzberatung von Australien (Financial Counselling Australia)—wenn Sie in finanzieller Not sind, rufen Sie 1800 007 007 007 an, um mit einem kostenlosen Finanzberater zu sprechen oder besuchen Sie www.financialcounsellingaustralia.org.au.

Wo Sie einen Betrug melden können

Sie können anderen helfen, indem Sie einen Betrug an die zuständigen Behörden melden. Ihre Informationen werden diesen Organisationen helfen, sich ein besseres Bild von den neuesten Betrugsmethoden zu machen und andere Menschen darüber zu informieren, worauf sie achten müssen.

Bei den folgenden Organisationen können Sie verschiedene Arten von Betrug melden:

Scamwatch

Melden Sie Betrugsfälle an die ACCC über Scamwatch unter www.scamwatch.gov.au

Bleiben Sie Betrügern einen Schritt voraus

Bleiben Sie den Betrügern einen Schritt voraus - besuchen Sie die Scamwatch-Website, um mehr über Betrügereien zu erfahren, die auf australische Verbraucher und kleine Unternehmen abzielen. Erfahren Sie mehr über die Betrugsmethoden, wie Sie sich schützen können und was Sie tun können, wenn Sie betrogen wurden.

Melden Sie sich für das Scamwatch-Abonnement an, um kostenlose E-Mail-Benachrichtigungen über neue Betrugsfälle zu erhalten.

www.scamwatch.gov.au

Folgen Sie Scamwatch auf Twitter unter @scamwatch_gov oder http://twitter.com/Scamwatch_gov

Wenn Sie auf einen Betrug auf einer Website oder Social Media-Plattform stoßen, melden Sie ihn an die Website, damit er untersucht und entfernt werden kann. Wenn die Betrüger eine legitime Organisation wie eine Regierungsstelle oder eine Bank imitieren, teilen Sie es dieser mit, damit sie andere warnen kann.

Andere Behörden

Erwägen Sie auch, Ihren Betrug an andere Behörden zu melden, die sich speziell mit bestimmten Arten von Betrug befassen.

Art des Betrugs	Behörde
Cyberkriminalität	Das australisches Netzwerk zur Online-Meldung von Cyberkriminalität (Australian Cybercrime Online Reporting Network – ACORN)—besuchen Sie www.acorn.gov.au
Finanz- und Investitionsbetrug	Die australische Wertpapier- und Anlagekommission (Australian Securities and Investments Commission - ASIC) — besuchen Sie www.moneysmart.gov.au oder rufen Sie die ASIC-Infoline unter 1300 300 630 an
Betrug und Diebstahl	Ihre örtliche Polizei —rufen Sie 13 14 44 an
Spam-Mails und SMS-Nachrichten	Die australische Kommunikations- und Medienbehörde (Australian Communications and Media Authority - ACMA)—besuchen Sie www.acma.gov.au oder rufen Sie den ACMA-Kundendienst unter 1300 850 115 an
Steuerbetrug	Das australische Finanzamt (Australian Taxation Office - ATO)—um einen Steuerbetrug zu melden oder zu überprüfen, ob eine Person, die Sie vom ATO kontaktiert hat, legitim ist: • Rufen Sie 1800 008 540 an oder leiten Sie die E-Mail mit dem Steuerbetrug an ReportEmailFraud@ato.gov.au weiter
Bankgeschäfte	Ihre Bank oder Ihr Kreditinstitut

Kontaktieren Sie Ihre örtliche Verbraucherschutzbehörde

Die ACCC ist zwar die nationale Behörde für allgemeine Verbraucherschutzfragen, aber staatliche und territoriale Behörden können Ihnen womöglich auch weiterhelfen.

Amt für Regulierungsdienste des Australian Capital Territory (Australian Capital Territory Office of Regulatory Services)	www.accesscanberra.act.gov.au 13 2281
Verbraucherschutz von Victoria (Consumer Affairs Victoria)	www.consumer.vic.gov.au 1300 558 181
Fairer Handel New South Wales (New South Wales Fair Trading)	www.fairtrading.nsw.gov.au 13 3220
Verbraucherschutz des Northern Territory (Northern Territory Consumer Affairs)	www.consumeraffairs.nt.gov.au 1800 019 319
Amt für fairen Handel von Queensland (Queensland Office of Fair Trading)	www.fairtrading.qld.gov.au 13 7468
Verbraucher- und Unternehmensdienste von Südaustralien (South Australia Consumer and Business Services)	www.cbs.sa.gov.au/ 13 1882
Verbraucher-, Gebäude- und Beschäftigungsdienst von Tasmanien (Tasmania Consumer, Building and Occupational Services)	www.cbos.tas.gov.au/ 1300 654 499
Ministerium für Bergbau, Industrieregulierung und Sicherheit von Westaustralien (Western Australia Department of Mines, Industry Regulation and Safety)	www.consumerprotection.wa.gov.au/ 1300 304 054

Weitere Informationen

Die australische Regierung stellt einige sehr hilfreiche Ressourcen zur Verfügung, wie Sie online sicher bleiben und sich schützen können.

- Hilfsmittel und Tipps für die Online-Sicherheit—www.staysmartonline.gov.au
- CyberSmart website—www.cybersmart.gov.au
- Hinweise für die Online-Sicherheit—verfügbar unter www.staysmartonline.gov.au/get-involved/guides

www.scamwatch.gov.au