



Anti- Betrugs- Antleitung

Small World Financial Services Group
Mai 2013 - Version 1.0

Inhalt:

Einleitung
Betrügerischer Missbrauch von Geldtransfers
Betrugsbeispiele
Hilfreiche Tips für Kunden
Meldung von Betrugsfällen

Einleitung

Der Zweck dieser Anti-Betrugs-Anleitung ist die Sensibilisierung des Bewusstseins über die Modi Operandi von Betrügern gegenüber unser Geldtransfersystem. Diese Anleitung richtet sich an die Mitarbeiter und Agenten der Small World Financial Services Group ("Small World").

Der korrekte Umgang mit Betrugsfällen spielt eine Schlüsselrolle für Small World. In erster Linie gilt es die Verpflichtung einzuhalten, unser System vor betrügerischen Aktivitäten zu schützen und gleichzeitig zu verhindern, dass es als Instrument von solchen kriminellen Personen oder Organisationen genutzt wird. Darüber hinaus verpflichten wir uns auch selbstverständlich, unsere Kunden über solche Aktivitäten zu informieren. In zweiter Linie, will Small World seinen Ruf als vertrauenswürdiger, globaler Provider für Geldtransferdienstleistungen bewahren. Gegen jegliche Form von kriminellen Aktivitäten, wie z. B. Geldwäsche, Finanzierung von Terrorismus oder Betrug etc., wird unser Unternehmen die notwendigen Maßnahmen selbstverständlich ergreifen.

In der Anleitung stellen wir Ihnen einige Details zu potentiellen Betrugsfällen vor. Beispiele aus der Praxis, aus denen Sie die Handlungsweisen von Betrügern entnehmen können, werden ebenfalls vorgestellt. Abschließend werden wir Ihnen außerdem wichtige Tips geben, wie Sie sich selbst und Ihre Kunden davor schützen können, Betrugsoffer zu werden.

(Fußnote: Die Informationen in diesem Dokument sind geheimzuhalten. Es steht ausschließlich der adressierten Person zur Verfügung und darf von Fremden weder genutzt, noch kopiert werden.)

Betrügerischer Missbrauch von Geldtransfers

Betrug in Verbindung mit Geldtransfers richtet sich i. d. R. gegen zwei verschiedene Opfertypen:

1. Unser Kunde, der das Geld an einen betrügerischen Begünstigten sendet
2. Angestellte oder Agenten, die für Small World arbeiten.

Der erste Opfertyp, unser Kunde, ist das am häufigsten anvisierte Opfer. Kunden können das Opfer verschiedenster Betrugspläne werden, in denen versucht wird, sich auf illegale Art und Weise das Geld vom Kunden anzueignen oder indem versucht wird, durch den Kunden an das Geld anderer Personen zu gelangen. Aber auch Sie, als eine für das Small-World-System operierende Person, die die Aufträge unserer Kunden entgegennimmt, können das Opfer von Betrügern werden. In diesem Falle versuchen die Betrüger einen Zugang zum Geldtransfersystem zu bekommen, indem sie Ihr Passwort missbrauchen. Im nächsten Kapitel dieser Anleitung können Sie einige Fallbeispiele entnehmen, die die verschiedenen Betrugspläne beschreiben.

Kundenfokussierter Geldtransfer-Betrug:

Betrüger versuchen ihre Opfer durch eine glaubhafte Geschichte zu beeinflussen, damit diese eine bestimmte Summe an einen unbekannten und unzuverlässigen Begünstigten senden.

Agentenfokussierter Geldtransfer-Betrug:

Durch die Erlangung eines unautorisierten Zugriffs auf das OMNEX Geldtransfersystem, initiieren Betrüger Aufträge, die zu finanziellen Aufwendungen des zum Opfer gewordenen Agenten werden.

Betrugsbeispiele

In diesem Kapitel werden wir die Charakteristika der Geldtransferbetrüge diskutieren. Allgemeine Betrugsbeispiele sind:

1. Internet- oder Auktionserwerb
2. Steuern oder andere Gebühren die in Verbindung mit einen Lotteriegewinn stehen
3. Anzahlungen oder Gebühren für Darlehen
4. Investitionsmöglichkeiten
5. Notfallsituationen bezüglich Personen, die sie im Internet kennengelernt haben
6. Arbeitsmöglichkeiten, die Sie von zu Hause aus erledigen können, für die aber eine Gebühr anfällt, welche für die Vorbereitung (Ausbildung) zu zahlen ist.

Abgesehen von diesen hier aufgeführten Beispielen, gibt es selbstverständlich auch weitere Arten des Geldtransfer-Betrugs und es tauchen regelmäßig auch weitere Formen auf. Aber in der Regel weisen sie ähnliche Charakteristika auf, die sich wiedererkennen lassen. Weiter unten werden wir einige Betrugstypen im Detail vorstellen, um Ihnen einen Überblick über die Eigenschaften zu vermitteln, auf die sie besonders aufpassen sollten.

Darlehensbetrug

Kriminelle suchen kontinuierlich nach neuen Wegen um an das Geld von unschuldigen Opfern zu gelangen. Häufig erreichen sie dies durch die Überzeugung Ihres Kunden (im weiteren Verlauf als "Opfer" bezeichnet), der ihnen Geld durch die Nutzung unseres Geldtransfersystems senden soll. Kriminelle nutzen ausgeklügelte Techniken um die Opfer zu täuschen. Die Kriminellen visieren meistens diejenigen an, die z. Z. eine Pechsträhne durchlaufen, solche, die gerade ihren Job verloren haben oder aber diejenigen, die sich bemühen ihren finanziellen Verpflichtungen in Zeiten der schwierigen Wirtschaftslage nachzukommen. Im folgenden Beispiel stellen sich die Kriminellen als Kreditberater (im weiteren Verlauf als "Krimineller" bezeichnet) einer Bank oder eines anderen Finanzinstitutes vor und visieren solche Personen an, die dringend einen Kredit benötigen. Diese Kriminellen kontaktieren die Opfer per Telefon, E-Mail oder schriftlich per Post und erklären ihm, dass es eine Möglichkeit gibt, ein Darlehen in Höhe von 5.000 € zu gewähren. Er bietet dem Opfer einen sehr niedrigen und vorteilhaften Zins an, geringe monatliche Rückzahlungen und außerdem den Verzicht auf eine Überprüfung der Kreditfähigkeit. Auch wenn das Opfer am Anfang etwas skeptisch auf dieses Angebot reagiert, versichert ihm der Kriminelle, dass er die Kreditsumme bereits innerhalb einer Woche zur Verfügung stellen kann. Und als Zeichen des guten Glaubens erklärt er dem Opfer außerdem, dass es die ersten fünf Monatsraten über unser Geldtransfersystem tilgen kann. Bei solchen Bedingungen kann es vorkommen, dass das Opfer zustimmt und sich bereit erklärt, die ersten fünf Monatsraten im Voraus zu überweisen (5 Raten, jeweils 200 € pro Monat = insgesamt 1.000 €). Am Ende der Woche bemerkt das Opfer schließlich, dass der erhoffte Kredit, leider nicht auf sein Konto überwiesen wurde und daraufhin versucht es den Anbieter telefonisch zu erreichen und stellt dabei fest, dass unter der angegebenen Telefonnummer keiner mehr antwortet oder dass die Nummer nicht mehr existiert. Darüber hinaus stellt es ebenso fest, dass auch die versendeten Email-Anfragen unbeantwortet bleiben. Als letzte Option versucht es schließlich die Transaktion wieder rückgängig zu machen um den vollen Betrag zurückzuerhalten. Da der versendete Betrag aber bereits abgeboben wurden, ist das Opfer für die Streichung der Transaktion nicht mehr berechtigt.

Verbrecherische Händler

Verbrecherische Händler (oder "falsche Anrufer") rufen unangekündigt bei Personen zu Hause an (oder erscheinen persönlich an der Tür der Opfer) und präsentieren sich als Vertreter eines legitimen Unternehmens. Es handelt sich hierbei meistens um Mitglieder von mobilen und gut organisierten kriminellen Gruppen, die das ganze Land durchreisen und sich auf der Suche nach Gebieten befinden, die eine hohe Population an älteren Menschen oder gemischter Gemeinschaften aufweisen. Sie sind bekannt dafür, Informationen über geeignete Gebiete mit anderen kriminellen Gruppen/Vereinigungen zu teilen. Sie berechnen bewusst einen zu hohen Betrag für eine unnötige Arbeit/einen unnötigen Service, beschädigen absichtlich das Eigentum der Opfer um einen Auftrag zu erhalten, lassen einen Auftrag unbeendet und benutzen aggressives und bedrohliches Verhalten um Geld zu erpressen. Verbrecherische Händler setzen benachteiligte Menschen unter Druck, um an ihr Geld heranzukommen und in einigen Fällen begleiten sie solche Personen sogar bis zu ihren Finanzinstituten um Geld von ihrem Konto abzuheben. Oftmals erpressen sie ihre Opfer sogar über einen längeren Zeitraum. Vor allem ältere Menschen, die aufgrund des Verlustes ihres Partners meistens isoliert leben, weisen z. B. durch die sichtbare Vernachlässigung ihrer Gärten vor ihren Häusern, ihre emotionale Lage auf und gerade solche Situationen machen sie leichter identifizierbar für Kriminelle.

Der "Sidi-Salem-Betrug"

Diese Art von Betrug kommt ursprünglich aus Tunesien, konnte sich jedoch im Laufe der Zeit auch in einigen europäischen Ländern ausbreiten, wie z. B. in Frankreich, Italien, Deutschland oder Belgien. Der Name "Sidi-Salem-Betrug" bezieht sich auf Weinverkäufer in Tunesien. Die selben Methode in abgeänderter Form nutzen auch nigerianische Kriminelle. In solchen Fällen wird behauptet, dass die betroffene Person einen Koffer voller Geld gewonnen hat und dass sie lediglich die entsprechenden Zoll- oder sonstigen gesetzlichen Gebühren zahlen muss, damit ihnen der Gewinn übermittelt werden kann. Die Betrüger versuchen dabei meistens per Telefon, möglichst viele potentielle Opfer zu erreichen. Im Weinbetrugsbeispiel wird dagegen behauptet, dass sie, im Vergleich zum europäischen Marktpreis, verschiedenen Weine von höchster Qualität zu günstigen Preisen verkaufen. Aufgrund der hohen Preise antworten die Opfer meistens, dass sie nicht interessiert sind. Daraufhin rufen die Betrüger mehrere Male an, manchmal sogar am selben Tag. Da es sich bei den Opfern häufig um ältere Menschen handelt, ziehen sie es oftmals vor, das Angebot letztendlich zu akzeptieren, damit die Belästigung ein Ende findet. Große Mengen an Geld sind in diesen Transaktionen involviert, manchmal sogar mehrere zehntausend Euro innerhalb weniger Monate. Zudem müssen die Opfer hinterher feststellen, dass es sich bei Ihrem Erwerb um einfachen Tafelwein handelt.

Vorauszahlungsbetrugsfälle

Bei Vorauszahlungsbetrugsfällen zahlen die Opfer eine bestimmte Summe im Voraus um hinterher etwas von größerem Wert zu erhalten. Beispiele hierfür sind Investitionsmöglichkeiten, verschiedene Arten von Verträgen, Darlehen etc. Schließlich erhalten sie im Gegenzug nur etwas von geringerem Wert oder häufig auch gar nichts. Solche Betrugspläne enthalten oftmals auch Strategien um bestimmte Produkte oder Dienstleistungen zu verkaufen, oder aber Reisen, Preise, Investitionsangebote oder Lotteriegewinne zu vergeben.

Nigerianische Betrugsfälle

Die Anbieter versuchen zuerst eine große Menge an potentiellen Opfern durch das Internet oder per E-Mail zu kontaktieren. Die Opfer erhalten dabei ein lukratives Angebot; dies kann ein bestimmter Vertrag sein, ein Lotteriegewinn oder aber Erbschaftsansprüche beinhalten. In Betrugsfällen von "Internet-Dating" nutzen die Täter, sowohl Frauen als auch Männer, falsche Profile mit falschen Fotos auf den entsprechenden Datingseiten oder Foren. Falls das Opfer auf das erste Angebot positiv reagiert, werden anschließend weitere persönliche Informationen angefordert. Nach Erhalt werden dann gewisse Dokumente an das Opfer gesendet um das Angebot glaubhafter wirken zu lassen. Kurze Zeit danach wird der "Kunde" gebeten, eine Vorauszahlung zu tätigen, was hinterher meistens eine weitere Zahlung des beabsichtigten Gesamtbetrages mit sich zieht. Sollte das Opfer dazu nicht bereit sein, wird damit gedroht, dass das "Internet-Date" aufgrund von Geldnöten nicht mehr zustandekommen kann. Die Anfragen nach Geldüberweisungen setzen sich fort, bis die Opfer schließlich Verdacht spüren und mit den Zahlungen aufhören. Die Überweisungen für solche nigerianischen Betrugsfallbeispiele werden in der Regel aus Nord Amerika, West Europa oder der Arabischen Halbinsel an verschiedene Westafrikanische Länder - dazu zählen insbesondere Nigeria, die Elfenbeinküste, Senegal, Togo, Ghana und Benin - überwiesen. Wie dem auch sei, die Betrüger nutzen immer häufiger Mittelsmänner in West Europa um das Geld zu erhalten und hinterher weiter nach Westafrika zu senden. Dies ist als zusätzliche Barriere zwischen dem Opfer und dem Täter zu bewerten. Wenn es sich bei den Mittelsmännern um in Europa ansässige Komplizen handelt, kann es auch vorkommen, dass die Transaktionen in "Fonds" aufgesplittet werden, die auf der einen Seite von den Hauptakteuren aus anderen Westeuropäischen Ländern empfangen werden, und auf der anderen Seite an die Begünstigten in Westafrika weitergeleitet werden.

Lotteriebetrugsfälle

Bei Lotteriebetrugsfällen erhalten die potentiellen Opfer E-Mails oder Briefe in denen versprochen wird, dass sie den "großen Preis" gewonnen haben. Fast immer handelt es sich dabei um eine vermeintliche Lotteriegesellschaft aus dem Ausland, die behauptet, dass die "richtigen Zahlen" bei der Auslosung dem Opfer zugeteilt wurden. Das Opfer wird daraufhin aufgefordert, den Organisatoren die Verwaltungskosten zu überweisen, damit diese den Gewinn freigeben können (welcher selbstverständlich nicht existiert).

"Money-Mule-Fälle"

Das Phänomen "Money-Mule" kann wie folgt beschrieben werden:

Kriminellen Organisationen versuchen die Opfer anzulocken, indem sie ihnen Jobangebote über das Internet zukommen lassen. Vor allem Arbeitslose und junge Menschen stimmen den entsprechenden Bedingungen zu. Sie werden aufgefordert, dem Anbieter die Kontodaten zu geben, auf welches anschließend Geld (meistens aus dem Ausland) überwiesen werden soll. Der Kontoinhaber verpflichtet sich dann kurze Zeit später, den Betrag vom Konto abzuheben und in Bar über ein Geldtransferunternehmen ins Ausland zu überweisen. Das in diesem Geschäft verwickelte Individuum darf dabei eine Kommission von 10 % behalten. Die via E-Mail versendeten Arbeitsverträge sind häufig sehr professionell gestaltet und sorgen dafür, dass das Unternehmen als echt, bzw. seriös eingestuft wird und wecken somit das Interesse der Opfer für ein zusätzliches Einkommen. Es ist auffällig, dass in diesem Falle vor allem russische

Unternehmen als potentielle Arbeitgeber auftreten. Die auf das Konto des Opfers überwiesenen Beträge sind meistens das Ergebnis des sogenannten "Phishing-Betrugs", was eine der vielen Betrugsformen im Internet ist. Personen werden von einer falschen Bankwebsite angelockt und dazu überredet, dort ihre Kontodaten einzugeben. Auf diese Weise erhalten die Betrüger die notwendigen Kreditkartennummern um Geld vom Konto des Opfers abzuheben, ohne dass es etwas davon bemerkt. Für gewöhnlich handelt es sich hierbei um Deutsche, Belgische oder Dänische Bankkonten.

Aktienbetrugsfälle

Aktienverkaufsbetrüger (engl. "boiler room") nähern sich dem Opfer durch unaufgeforderte/unerwünschte Telefonate, durch den klassischen Schriftverkehr oder auch durch E-Mail Anfragen um ihnen Investitionsangebote zu unterbreiten. Dies ist typisch für im Ausland ansässige "Broker", welche die europäischen Aktionäre anvisieren, um ihnen Aktien anzubieten, die sich hinterher oftmals als wertlos entpuppen oder sich als hochriskante amerikanische oder britische Investmentobjekte herausstellen. Ein auffälliges Merkmal dieser "Broker" ist, dass sie große Überzeugungskünste besitzen und ziemlich hartnäckig verhandeln können.

Gebrauchtwagenangebote

Diese spezielle Betrugsstrategie beginnt häufig mit einer Werbeanzeige im Internet oder in einem Automobil-Magazin, in der ein englischer Verkäufer ein erstklassiges Auto zu einem sehr günstigen Preis anbietet. Der Verkäufer behauptet für gewöhnlich, dass er in Spanien oder Portugal lebt und aus bestimmten Gründen sein Auto schnellstmöglich verkaufen will/muss. Sie teilen den potentiellen Opfern ebenfalls mit, dass sie das Auto vorher leider nicht sehen können, da es sich z. Z. beim Transportunternehmen auf dem Schiffsweg befindet. In Wahrheit gibt es aber gar kein Auto und die Opfer bemerken es leider erst wenn es bereits zu spät ist und sie ihr Geld schon überwiesen haben.

Hilfreiche Tips für Kunden

In diesem abschließenden Kapitel werden wir Ihnen einige wichtige Tips zur Verfügung stellen, die zum Schutz vor Betrugsvorhaben hilfreich sein können. Die Berücksichtigung dieser Tips wird das Risiko, Betrugsoffer zu werden, deutlich senken.

Tips für Kunden, um Betrüger rechtzeitig zu stoppen:

- Senden Sie niemals Geld an Personen, die sie persönlich nicht kennen.
- Senden Sie niemals Geld im Voraus für ein Angebot (bspw. Darlehen, Jobs oder Lotteriegewinne etc.), das Ihnen im Gegenzug einen zukünftigen Gewinn verspricht.
- Glauben Sie niemals Personen, mit denen Sie keinerlei Verwandtschafts- oder Bekanntschaftsverhältnisse haben, die Ihnen versuchen ihre Notlage zu erklären und Sie dementsprechend um Ihre Hilfe bitten.
- Glauben Sie keinem Angebot, in dem behauptet wird, dass ein Geldtransfer die einzige Zahlungsmöglichkeit ist.
- Seien Sie besonders aufmerksam bei auffällig günstigen Angeboten, denn was "zu gut ist um wahr zu sein" ist auch in der Regel "zu gut um wahr zu sein".
- Es gibt keinen Schutz vor Verlusten, die aufgrund eines Geldtransferbetrugs hervorgerufen sind,

Betrugsfall melden

Wenn Sie glauben, dass Sie einen Betrugsversuch oder einen bereits erfolgten Betrugsfall entdeckt haben, teilen Sie es uns bitte unverzüglich an eine der unten stehenden Kontaktmöglichkeiten mit. International können Sie uns per Telefon, Fax oder per E-Mail unter den folgenden Daten erreichen:

Telefon (Vereinigtes Königreich): 0 800 019 5030

Telefon (International): +44 (0) 20 7378 1100

Fax: +44 (0) 20 7378 1220

Email: compliance.uk@smallworldfs.com