

Eine entscheidungspsychologische Lesart von digitalen Varianten des Vorkassebetrugs

Von Till Neuhaus M.Ed., M.A., M.A., Bielefeld

1 Einleitung



Durch E-Mails initiiert, verursacht nach Schätzungen knapp 3 Mrd. US-Dollar Schaden jährlich². Gleichzeitig kann angenommen werden, dass eine Vielzahl an Taten – aufgrund von Scham seitens der viktimisierten Personen – gar nicht erst erfasst wird. Während ein Großteil der Publikationen im Feld Naivität auf Seiten des Opfers als zentrale Erklärung heranzieht, möchte dieser Beitrag exemplarisch einen idealtypischen Betrug³ darstellen und entscheidungspsychologisch rahmen, sodass die – seitens der Täter genutzten – Mechanismen in ihrer Wirkungsweise und Funktion anteilig erklärt werden können. Dabei fokussiert dieser Beitrag auf eine Variante des Vorkassebetrugs, genauer gesagt auf die narrative Ausgestaltung in Form des sog. *Nigerian Scam*. In dieser Variante des Vorkassebetrugs wird die Geschichte eines, häufig in Nigeria beheimateten, Adligen, Priesters oder Geschäftsmannes präsentiert, der sich in einer misslichen Notsituation befindet und lediglich etwas Geld benötigt, um erneut auf sein – im Moment nicht verfügbares – Vermögen zugreifen zu können. Dabei verspricht der Sender der Nachricht, seinen Helfer großzügig zu entlohnen, sobald er erneut auf seinen Reichtum zugreifen kann. Aufgrund der Vielzahl an betrügerischen Mails existieren zahllose Variationen dieses Betrugs, ebenso sind alternative narrative Ausgestaltung möglich. Nichtsdestotrotz kann festgehalten werden, dass Vorkassebetrug in seiner basalsten Form auf eine 400-jährige Geschichte zurückblickt und im zeitlichen Verlauf in verschiedenen Kommunikationsformaten und -medien durchgeführt worden ist⁴. Daher kann angenommen werden, dass die Betrugsmechanismen Grunddynamiken menschlichen Denkens und Handelns adressieren, die dieser Aufsatz anteilig skizzieren möchte. Damit kann dieser Beitrag sowohl aus der Perspektive des durch E-Mails initiierten Betrugs gelesen werden, ebenso werden sich Teile der Ausführung auch in anderen Betrugsformaten wiederfinden und so für die Prävention nutzbar gemacht werden können.

Um die Feinheiten des *Nigerian Scam* angemessen rahmen zu können, verwendet dieser Beitrag die Theorieschule des *Nudging*⁵. Das Konzept des Nudging geht davon aus, dass Menschen im Prozess der Entscheidungsfindung eine Entscheidungsarchitektur – alle als relevant ausgemachten sowie verfügbaren Impulse – konsultieren. Darüber hinaus basiert Nudging auf der Annahme, dass Menschen zwei, für unterschiedliche Arten von Entscheidungen notwendige, Entscheidungssysteme besitzen: Ein langsames, analytisch und reflektiertes System sowie ein intuitives, schnelles und unbewusst agierendes System. Die Kunst des Nudging besteht nun darin, die Entscheidungsarchitektur durch bewusste Umgestaltung so zu verändern, dass das intuitive Entscheidungssystem primär agiert und damit bestimmte Entscheidungen wahrscheinlicher werden als andere. Die Umgestaltung von Entscheidungsarchitekturen kann bspw. durch die Präsentation von Daten geschehen – medizinische Laien, aber auch ExpertInnen entscheiden in einer Behandlungssituation unterschiedlich, je nachdem ob eine Überlebens- oder eine Sterbewahrscheinlichkeit ausgewiesen wird, selbst bei numerisch gleichen Werten⁶ – oder aber durch das bewusste Setzen sozialpsychologischer Impulse. Im Folgenden wird dieser Aufsatz den Nigerian Scam zeitlich phasieren und jede Phase hinsichtlich genutzter Nudges befragen. Die Phasierung orientiert sich an der im anglophonen Raum üblichen Abfolge zur Beschreibung von Betrugsmaschinen: bait, hook, line und sinker⁷. Jede Phase wird eingangs idealtypisch skizziert – was macht bzw. schreibt ein Scammer? –, anschließend werden jene Tätigkeiten durch die Perspektive des Nudging reflektiert, sodass einerseits die Komplexität und psychologische Vielschichtigkeit des Vorkassebetrugs ersichtlich und andererseits die Perspektive des Opfers auf Seiten der Strafverfolgung verständlicher wird. Denn erst durch die Berücksichtigung beider Perspektiven kann Prävention effektiv und zielgerichtet vorangetrieben werden.

2 Das Auswerfen des Köders - die Bait-Phase

Die Initiatoren des Betrugs versenden ihre Mails an Adressen, die sie entweder erworben, erbeutet oder die ihnen auf andere Arten und Weisen verfügbar gemacht worden sind. Wichtig hierbei ist, dass in dieser Phase des Betrugs keine Vorauswahl hinsichtlich der Adressaten getroffen werden kann und aufgrund der Kommunikationsmodalitäten – E-Mails sind günstig, weltweit verfügbar, skalierbar und direkt – getroffen werden muss. In postalischen Varianten von Vorkassebetrug wurden aktiv Mitglieder von Kirchen, Wohltätigkeitsorganisationen oder Selbsthilfegruppen adressiert, da sich Betrüger bei diesen Gruppen – aufgrund von ausgeprägterem Mitgefühl bzw. vermutetem Geldmangel – höhere Erfolgswahrscheinlichkeiten ausrechneten⁸. Während in der postalischen Variante die Kosten (in Form von Papier und Porto) relativ am Anfang des Betrugs stehen, verschiebt sich dieses Gefüge in der digitalen Variante des Vorhabens. Hier entstehen (Personal-)Kosten im Verlauf durch das kontinuierliche Schreiben von Mails, wohingegen die Kommunikation selbst quasi kostenfrei ist⁹. Da allerdings auf Basis der verfügbaren E-Mailadressen keine Sortierung vorgenommen werden kann, nutzen die Betrüger den Mechanismus der Selbstselektion, um den Betrug für sich monetär attraktiv zu gestalten. Anstatt Szenarien zu konstruieren, die von vielen Internetnutzern beantwortet werden würden, verfassen die Initiatoren des Betrugs Geschichten, die – für wohlinformierte Internetnutzer – nach Betrug klingen. Dazu gehört bspw. die Nennung des Standortes Nigeria, der in Internetkreisen mit Betrug gleichgesetzt ist. Dieses Vorgehen hat zur Folge, dass von ca. 12,5 Millionen ausgesendeten Betrugsemails lediglich eine beantwortet wird¹⁰; allerdings können die Initiatoren des Betrugs bei dem/der Antwortenden davon ausgehen, dass sich diese Person nicht besonders gut im Internet auskennt, vermutlich fortgeschrittenen Alters ist und wahrscheinlich sozial isoliert lebt – optimale Bedingungen für den geplanten Vorkassebetrug. Durch diese selbstgesteuerte Vorauswahl modifizieren die Betrüger das Kosten-Nutzen-Verhältnis zu ihren Gunsten, da jene, die ihnen antworten (und für die Zeit und Personal aufgebracht werden müssen) zu einer höheren Wahrscheinlichkeit Geld überweisen werden, wohingegen falsch-positive (Antwortende, die später kein Geld überweisen) minimiert werden. Die initiale Adressierung via E-Mail dient also, ökonomisch gesprochen, der Zielgruppenoptimierung¹¹.

3 Alles hat einen Haken - die Hook-Phase

Die Hook-Phase kann sozusagen als das Kernstück des Vorkassebetrugs betrachtet werden und beginnt, sobald ein potenzielles Opfer auf eine betrügerische E-Mail geantwortet hat. In der Folge werden typische Vorgehensweisen vorgestellt und analysiert; einige dieser Vorgehensweisen können bei ausgewählten Varianten des Vorkassebetrugs auch schon in der ersten Nachricht vorgefunden werden, der Zweck bzw. die Funktionsweise bleibt allerdings identisch. Das Ziel der Hook-Phase besteht darin, dass die adressierte Person dem/der BetrügerIn Geld überweist, wobei die initiale Summe zweitrangig ist. Die in dieser Phase seitens der Betrüger gesetzten sozialpsychologischen Impulse – Autorität, Knappheit, Reziprozität und Sympathie¹² – werden zusätzlich vom *Truth Default*¹³ begünstigt. Dabei handelt es sich um die menschliche Tendenz, davon auszugehen, dass man im Austausch mit Mitmenschen grundsätzlich mit Wahrheiten konfrontiert ist. Der *Truth Default* ist in verschiedenen Personen unterschiedlich stark ausgeprägt, aufgrund der vorangegangenen (Selbst-)Selektion handelt es sich in dieser Phase des Betrugs tendenziell um Personen mit stark ausgeprägtem *Truth Default*.

Der bekannteste Aspekt des hier skizzierten Vorkassebetrugs ist die Anmaßung einer Autoritätsposition, wie bspw. eines Regierungsvertreters, Monarchens, erfolgreichen Geschäftsmannes oder Priesters. Im Rahmen der Hook-Phase beutet dieser sozialpsychologische Impuls zweierlei – erlernte und gesellschaftlich tief verwurzelte – Heuristiken bzw. Denkabkürzungen aus: Autorität und Knappheit. Menschen organisieren sich seit jeher in Kompetenzhierarchien, in denen jene, die mehr bzw. passgenauere Fähigkeiten in einem Bereich aufweisen ebenso mehr Befugnisse haben. Dabei ist hervorzuheben, dass ein Großteil dieser Kompetenzhierarchien funktional und mit meritokratischen Gesellschaftsansprüchen vereinbar ist. Auf Basis ebenjener Kompetenzhierarchien etablierte sich im Verlauf der letzten 150 Jahre ein stark ausdifferenziertes Zertifizierungssystem für verschiedene gesellschaftliche Bereiche. Jene Zertifizierungen dienen ebenso als Denkabkürzung, da im Falle einer vorliegenden Zertifizierung (bspw. eines Diploms oder einer Approbation) von einer vertieften Kenntnis des Feldes sowie, damit einhergehend, Kompetenz ausgegangen werden kann¹⁴. Dies erleichtert (vor allem Laien) die Unterscheidung zwischen ExpertInnen und Nicht-ExpertInnen. Dabei ist die Wirkmächtigkeit von Autorität nicht zu unterschätzen, wie bspw. die Milgram Experimente¹⁵ oder Fälle von Amtsanmaßung/Betrug (bspw. im medizinischen Sektor) verdeutlichen. Aufgrund gesellschaftlicher Lern- und Sozialisationsprozesse sind Menschen tendenziell anfällig für Autoritätshörigkeit – ein Umstand, den die Nigerian Scammers durch das Vorspielen einer solchen Autoritätsposition versuchen auszunutzen. Dabei spielt es eine besondere Rolle, wie ein solcher Anspruch glaubwürdig kommuniziert werden kann. In der Urversion des Vorkassebetrugs, dem

sog. Spanischen Gefangenen, erhielten potenzielle Opfer im 17. Jahrhundert einen Brief auf feinem Papier. Da dies für die Zeit vergleichsweise untypisch war, konnten die Betrüger ihrer Geschichte durch die Wahl und Qualität des Mediums mehr Glaubwürdigkeit verleihen. Dies geschieht im 21. Jahrhundert nicht mehr, was ebenso für die Notwendigkeit der oben skizzierten Selbstselektion spricht.

Neben dem angesprochenen Autoritätsimpuls, dient die Anmaßung eines Titels bzw. einer hochrangigen Position noch einem zweiten Zweck: sie suggeriert Knappheit, denn wie viele Leute werden schon von Monarchen, wohlhabenden Geschäftsleuten oder Klerikern persönlich adressiert. Dabei funktioniert das Prinzip der Knappheit in zwei Richtungen. Einerseits bedient sie das menschliche Bedürfnis des Besonders-seins, denn – so wird es zumindest gesellschaftlich kommuniziert und erlernt –, was knapp ist, ist tendenziell besonders und damit wertvoll¹⁶. Andererseits modifiziert die Wahrnehmung eines Gegenstandes oder einer Möglichkeit als knapp (und damit wertvoll) auch die Beurteilung von Risiken, da nun die Bedauernsaversion (engl. *regret aversion*) zu wirken beginnt. Bei der Bedauernsaversion versucht der/die Betroffene eine Entscheidung zu treffen, aber statt diese auf Basis verfügbarer Merkmale zu treffen, imaginiert der/die EntscheiderIn stattdessen sich selbst bzw. seine/ihre emotionalen Zustände in der Zukunft unter Eintritt verschiedener Szenarien¹⁷. Die Originalfrage – sollte ich jemanden, den ich nicht kenne, Geld überweisen? – wird abgelöst durch die Frage *Wie würde ich mich fühlen, wenn ich diese Möglichkeit verpasse?* Statt also das rationale, besonnene und langsame Denksystem für diese Entscheidung heranzuziehen, konsultieren viktimisierte Personen vornehmlich das schnelle, intuitive und unbewusst agierende System. Dabei kann ihnen unter Umständen nicht auffallen, dass sie im Verlauf die zu beantworteten Frage (unbewusst) ausgetauscht haben. Für eine solche Interpretation der Denkprozesse spricht, dass Knappheits- und Autoritätsimpulse häufig mit Wörtern der Dringlichkeit bzw. des begrenzten temporalen Kontextes seitens der Betrüger kommuniziert werden¹⁸. Es scheint sich so darzustellen, dass die BetrügerInnen sich der verschiedenen Denkmodi (schnell/intuitiv vs. langsam/analytisch) bewusst sind und aktiv versuchen den schnellen und tendenziell fehlerbehafteteren zu adressieren – bspw. über Autoritäts- und Knappheitsimpulse.

Neben den eher direkten Autoritäts- und Knappheitsimpulsen nutzen viele Vorkassebetrüger noch Varianten der vermeintlich im Ungleichgewicht befindlichen Reziprozität. Hierbei handelt es sich um ein mentales Buchführungssystem, das Menschen vermittelt, ob sie – im Austausch mit ihrer Umwelt – tendenziell Schulden haben oder übermäßig gütig waren¹⁹. Die Existenz dieses menschlichen Mechanismus hat höchstwahrscheinlich evolutionäre Wurzeln, da langfristige Kooperation eine evolutionär-stabile Überlebensstrategie darstellt. Damit eine solche Kooperation allerdings langfristig und mit verschiedenen Akteuren funktioniert, muss sich das Individuum vor egoistischen Trittbrettfahrern schützen und andererseits schauen, dass er/sie selbst stets einigermaßen ausgewogen zur Umwelt steht. Mentale Buchführung ist kein punktgenaues System, sondern vermittelt, ob man sich eher im Ungleichgewicht befindet oder nicht. Betrachtet man versendete Betrugsmails unter diesem Gesichtspunkt, so fällt auf, dass eine Vielzahl der Nachrichten versucht, Vertrauensvorschuss zu leisten. Dies geschieht bspw. durch das Anhängen von – wahrscheinlich gefälschten – Ausweisdokumenten, die die Glaubwürdigkeit des Senders verifizieren sollen. Hinzu kommen Bekundungen, die die Gutmütigkeit des Empfängers ins Zentrum rücken. Beide Maßnahmen haben das Ziel das unbewusst agierende Reziprozitätssystem zu adressieren und – ohne die Verwendung von monetären/materiellen Ressourcen – ins Ungleichgewicht zu rücken²⁰. Dem potenziellen Opfer erscheint es zu diesem Zeitpunkt so, als ob er/sie Geld überweisen müsse, wobei sich dieser Drang (neben den oben skizzierten Impulsen) aus dem Gefühl speist, dass man sozusagen (immaterielle) Schulden bei der anderen Person habe – bei der finalen Konsultation der verfügbaren Entscheidungsarchitektur ist dies ein nicht zu unterschätzender Faktor.



Ergebnis eines Betruges.

Wie bereits hinsichtlich der Aspekte Autorität, Knappheit und Reziprozität ausgeführt, versuchen Betrüger alles, um die Frage, mit der sich das potenzielle Opfer auseinandersetzen soll auszutauschen bzw. anders zu rahmen. Dies geschieht insbesondere im letzten sozialpsychologischen Impuls der Hook-Phase, dem Versuch Sympathie zu erzeugen²¹. Durch die Schaffung von Sympathie soll angeleitet werden, dass das potenzielle Opfer sich nicht mehr primär die Frage stellt, ob er/sie Geld überweisen soll, sondern, ob er/sie den Betrüger tendenziell mag bzw. sympathisch findet. Dies versuchen Scammer in E-Mails auf vielfältige Arten und Weisen, wobei nur exemplarische Versuche skizziert werden können. Prominente Beispiele für den Versuch Sympathie zu erzeugen ist das fingieren von Unglücksgeschichten, seien es Krankheiten, Unfälle oder andere Schicksalsschläge.

Dabei wird versucht, eine – aufgrund von geteilten Eigenschaften – *in-group* Mentalität entstehen zu lassen²². Und auch wenn der Empfänger selbst nicht von einem Schicksalsschlag gebeutelt ist, so besteht immer noch die vergleichsweise große Chance im näheren Umfeld des Opfers auf Kranke oder Verunfallte zu stoßen und so Nähe (und damit Sympathie) suggerieren zu können. Dieses Vorgehen lässt sich empirisch anteilig damit belegen, dass in betrügerischen E-Mails aktuelle Ereignisse – dies konnte für 9/11 und den Afghanistankrieg nachgewiesen werden – aufgegriffen werden, in der Hoffnung jemanden zu adressieren, der von ebendiesen Ereignissen betroffen ist. Aber nicht nur über die artifizielle Konstruktion einer *in-group* wird versucht Sympathie seitens der potenziellen Opfer zu erzeugen, denn es spielt noch ein zweiter, menschlicher Mechanismus eine zentrale Rolle: Das menschliche Selbstbild. Die meisten Personen möchten gute Menschen sein. Eine Weisheit aus der Werbepsychologie besagt, dass Produkte nicht auf der Basis erworben werden, wer wir sind bzw. was wir brauchen, sondern wer wir gerne sein möchten. Unter ähnlichen Gesichtspunkten sollten Betrugsmails betrachtet werden, denn sie suggerieren, dass sie eine Chance darstellen zu beweisen, dass die adressierte Person ein guter Mensch ist. Zusammen mit der allgegenwärtigen Tendenz Mitleid – als zentraler Ausdruck des (Mit-)Menschseins²³ – zu zeigen, können diese Impulse das Gefühl kreieren, dass man den Absender der Nachricht tendenziell sympathisch findet und in der Folge gerne unterstützen möchte.

Wie hoffentlich gezeigt werden konnte, verwenden Nigerian Scammer in der Hook-Phase des Betrugs vielfältige Mechanismen, die die Entscheidungsarchitektur des potenziellen Opfers bewusst und im Sinne der BetrügerInnen verändern sollen. Dabei beuten sie sowohl evolutionäre wie auch gesellschaftlich perpetuierte Verhaltensmuster aus und tun dies beinahe ausschließlich über sprachliche und narrative Werkzeuge. Diese Werkzeuge konnten anteilig über die Fokussierung auf die Impulskategorien Autorität, Knappheit, Reziprozität und Sympathie erschlossen werden. Die Hook-Phase endet sobald das Opfer dem Betrüger Geld hat zukommen lassen, wobei die initiale Summe von nachrangiger Bedeutung ist. Von dort an beginnt die Line-Phase, die sich durch möglichst lange Aufrechterhaltung sowie kostenmäßig Eskalation des Geldtransfers kennzeichnet, quasi ein „*please hold the line*“ in einer äußerst teuren Warteschleife.

4 Das Opfer auf Spur halten – die Line-Phase

In der Line-Phase fingiert der Betrüger stetig neue Hindernisse, die ihn daran hindern auf sein Vermögen zuzugreifen. In den

narrativen Ausgestaltungen können dies verschiedene Arten von Gebühren oder Kosten sein, die natürlich nur mit Hilfe des gütigen Gebers beglichen werden können. Ebenso selbstverständlich versichert der – nun von zahllosen Gebühren heimgesuchte – Versender der betrügerischen Mails, dass auch diese Überweisungen um ein Vielfaches zurückgezahlt werden, sobald er auf seinen vermeintlichen Reichtum zugreifen kann. Während seitens des Betrügers eine stetige Kosteneskalation forciert wird, ist das Opfer dreierlei Effekten ausgesetzt, die sich anteilig gegenseitig bedingen bzw. verstärken. Diese Effekte sind im Feld der Kognitions- und Sozialpsychologie verortet, werden in der Folge kurz dargestellt und können anteilig erklären, wieso das Betrugsopfer – trotz eskalierenden Kosten – diesem irrationalen Handeln die Treue hält.

Der erste Effekt, der in dieser Phase des Betrugs zum Tragen kommt, ist der Wunsch des Opfers nach Konsistenz im Handeln. So konnte bereits Leon Festinger²⁴ und Carl Rogers²⁵ unabhängig voneinander in den 1950er Jahren zeigen, dass Konsistenz – in diesen Fällen zwischen Wertvorstellungen und Handlungen – ein menschliches Grundbedürfnis darstellt, dessen Nichtbefriedigung zu (nur schwierig auszuhaltenden) kognitiven Dissonanzen führen kann. Festinger argumentiert in seiner Studie, dass Probanden die Tendenz aufweisen (können), die objektiv wahrnehmbare Welt umzuinterpretieren bzw. anders wahrzunehmen anstatt ihre Glaubensgrundsätze anzupassen. Auf den Nigerian Scam angewendet bedeutet dies, dass die viktimisierte Person ebenso eher Tendenzen zeigt dem Betrüger zu glauben, anstatt die Alternative ins Auge zu fassen. Die Betrachtung von Alternativen gestaltet sich im Rahmen des Nigerian Scams als besonders schwierig, da die Grundannahme – ich bin eine wohlthätige, gutmütige Person, die jemandem in Not hilft – wesentlich angenehmer zu empfinden ist als die zu betrachtende Alternative, die das Opfer als naiv und ausgebeutet charakterisiert²⁶.

Der zweite Effekt, der die Kosteneskalation begünstigt, hat etwas mit modifizierter Risikowahrnehmung in Abhängigkeit zu wahrgenommenen Verlusten zu tun. Im Normalfall sind Menschen risikoavers, da – evolutionär gesprochen – Verluste das Überleben stärker gefährden als Gewinne es potenziell begünstigen. Dies manifestiert sich bspw. in wohldokumentierten Effekten wie der Verlustaversion²⁷. Diese Daumenregel besagt, dass Verluste von Menschen ca. doppelt so stark wahrgenommen werden wie Gewinne des gleichen Betrags: Ein verlorener Euro schmerzt so sehr wie ein Gewinn von zwei Euro Freude bereitet. Diese tendenziell risikoaverse Grundausrichtung verändert sich allerdings, wenn die betroffene Person – nach Konsultation ihres mentalen Buchführungssystems – das Gefühl hat sich in der Verlustzone zu befinden. Dann nämlich sind Menschen tendenziell bereit größere Risiken einzugehen, um sozusagen die gemachten Verluste zu kompensieren – ein hochgradig irrationales und unter Umständen gefährliches Verhalten²⁸. Das Betrugsopfer hat zu diesem Zeitpunkt mindestens eine (vielleicht sogar mehrere) Überweisung getätigt, befindet sich also in der Verlustzone und ist somit bereit, höhere (monetäre) Risiken zur Kompensierung des bisherigen Verlustes einzugehen. Diese *sunken-cost-fallacy* – der Fakt, dass man bereits verlorene Ressourcen mit höheren Einsätzen wiedergutmachen möchte – begünstigt die Absichten des Betrügers, der graduell höhere Summen einfordert, immer mit dem Versprechen den Geber zeitnah zu entschädigen bzw. reich zu entlohnen.

Letztlich profitieren die Betrüger noch von einem dritten Effekt in der Line-Phase: Der graduellen Migration von Entscheidungsprozessen. Während die Initialentscheidung Geld zu versenden mit viel Mühe und Aufwand seitens der Betrüger modifiziert worden ist, automatisieren sich diese Entscheidungsprozesse bei Wiederholung derselben Entscheidung zusehends; dies gilt, selbst wenn die Geldsumme sich ändert/erhöht. Während also anfangs lediglich eine kleine Summe versandt wurde, begünstigt diese Handlung die Wiederholung einer vergleichbaren Handlung in der Zukunft. Die hier skizzierte Migration von Entscheidungsprozessen – vom bewusst und analytisch entscheidenden System hin zum unbewussten und automatisch agierenden – wird sicherlich noch von dem bereits diskutierten Wunsch nach Konsistenz begünstigt und hilft Betrügern ihre Opfer längerfristig zu viktimisieren.

Die Line-Phase kann unterschiedlich lange andauern und endet erst, wenn das Opfer entweder anfängt den Betrug zu hinterfragen, von Externen instruiert wird oder der Betrüger aus anderen Gründen den Kontakt abbricht. Da die Zahlungen freiwillig geleistet worden sind und meist über Geldvermittlerdienste ins Ausland versandt worden sind, ist die Wiederbeschaffung des Geldes meist unmöglich. Hinzu kommt der Umstand, dass die Täter unter falschen Namen agieren, was die Strafverfolgung extrem erschwert. Der Abbruch des Kontaktes ist ebenso gleichbedeutend der Eintritt in die Sinker-Phase, in der das Opfer finanziell und bzgl. seines/ihrer Selbstbildes geschädigt zurückbleibt.

5 Transfer und Ausblick

Wie dieser Beitrag zeigen konnte, handelt es sich bei dem Nigerian Scam um einen psychologisch sowie kommunikationstheoretisch hochgradig ausgeklügelten und durchdachten Betrug, der lediglich sinnbildlich für andere Betrugsformate im digitalen Raum steht. Denn auch wenn der Nigerian Scam tendenziell rückläufig erscheint, erhöht sich die Anzahl digital verübter Straftaten stetig, wobei angenommen werden kann, dass die skizzierten Prozesse und Mechanismen auf andere Arten betrügerischer E-Mails transferierbar sind. Darüber hinaus deutet dieser Beitrag das Potenzial sozial- und kognitionspsychologischer Einsichten für die Rahmung, Strukturierung und Erklärung solch gearteter Betrugsmaschinen an. Auch

diesbezüglich kann die Vermutung geäußert werden, dass zentrale Bausteine ebendieser entscheidungspsychologischen Forschung für die vertiefte Auseinandersetzung mit digitalen (aber ebenso analogen) Betrugsvorhaben genutzt werden können.

Bildrechte: ProPK (www.polizeiberatung.de).

Anmerkungen

1. Der Autor ist Wissenschaftlicher Mitarbeiter an der Universität Bielefeld. An der Fakultät für Erziehungswissenschaften forscht und lehrt er zu pädagogischen Entscheidungsprozessen und beschäftigt sich darüber hinaus mit entscheidungspsychologischer Forschung in anderen Kontexten.
2. Vgl. Park, Y., Jones, J., McCoy, D., Shi, E., & Jacobsson, M. (2014). Scambaiter: Understanding Targeted Nigerian Scams on Craigslist. *NDSS Internet Society*, 1-15.
3. Die idealtypischen Charakteristika des Nigerian Scam werden in folgenden Publikationen bei-nah vollumfänglich skizziert: Dyrud, M. A. (2005). „I Brought You A Good News”. An Analysis of Nigerian 419 Letters. *Proceedings of the 2005 Association for Business Communication (Annual Convention)*; Schaffer, D. (2012). The Language of Scam Spams: Linguistic Features of the “Nigerian Fraud” E-Mails. *Review of General Semantics*, 69(2), 157-179.
4. Vgl. Smith, A. (2009). Nigerian Scam E-Mails and the Charms of Capital. *Cultural Studies*, 23(1), 27-47.
5. Ausführungen zu den Grunddynamiken des Nudgings sowie der assoziierten Denksysteme, s. Thaler, R. H. & Sunstein, C. R. (2017). *Nudge - Wie man kluge Entscheidungen anstößt* (Vol. 7). Berlin: Ullstein/Econ Verlag; siehe ebenso Kahneman, D. (2012). *Schnelles Denken, langsames Denken* (Vol. 8). München: Penguin Verlag/Random House.
6. Vgl. McNeil, B., Pauker, S., Sox, H., Jr., Tversky, A. (1982). On the elicitation of preferences for alternative therapies. *New England Journal of Medicine*, 306, 1259-1262.
7. Vgl. Konnikova, M. (2016). *The Confidence Game - Why we fall for it...every time*. Penguin/Random House. New York.
8. Cgl. Kich, M. (2005). A Rhetorical Analysis of fund-raiser-scam solicitations. *Circles*, 14, 129-142.
9. Zur ökonomischen Struktur des Nigerian Scam sowie dem Prinzip der Selbstselektion siehe Herley, C. (2012). Why do Nigerian Scammers Say They are from Nigeria? *Microsoft Research: One Microsoft Way*, 1-14. Retrieved from www.microsoft.com/en-us/research/wp-content/uploads/2016/02/WhyFromNigeria.pdf.
10. Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G. M., Paxson, V. & Savage, S. (2008). Spamalytics: An Empirical Analysis of Spam Marketing Conversion. *Proceedings of the 15th ACM Conference on Computer and Communications Security*, 1-12.
11. Vgl. Neuhaus, T. (2020). A (Nudge) Psychological Reading of the Nigerian Scam. *Brolly - Journal of Social Science* 3(3). 7-28.
12. Für die Wirkung von Autorität, Reziprozität, Sympathie, Knappheit sowie dem später diskutierten Wunsch nach Konsistenz, s. Cialdini, R. (2021). *Influence - The Psychology of Persuasion*. Harper Collins.
13. Levine, T. R. (2014). Truth-default theory (TDT) a theory of human deception and deception detection. *Journal of Language and Social Psychology*, 33(4), 378-392.
14. Vgl. Cialdini, R. B. (1987). Compliance Principle of Compliance Professionals. In: M. P. Zanna, J. M. Olson, & C. P. Herman (Eds.), *Social Influence: The Ontario Symposium* (Vol. 5, pp. 165-184). Psychology Press.
15. Milgram, S. (1965). Some Conditions of Obedience and Disobedience to Authority. *Human Relations*, 18(1), 57-76.
16. Vgl. Cialdini, R. B. (2003). The Power of Persuasion - Putting the Science of Influence to work in Fundraising. *Stanford Social Innovation Review*. 17-27.
17. Vgl. Loomes, G. & Sudgen, R. (1983). A Rationale for Preference Reversal. *American Economic Review*, 73, 428-43.
18. Vgl. Bergiel, B. J., Bergiel, E. B. & Balsmeier, P. W. (2008). Internet Cross Border Crime: A growing Problem. *Journal of Website Promotion*, 3(3/4), 133-142.
19. Zum Nutzen und Ablauf von Reziprozität, siehe Cox, J. C. (2004). How to identify trust and reciprocity. *Games and Economic Behavior*, 46, 260-281.
20. Vgl. Cialdini, R. B. (2003). The Power of Persuasion - Putting the Science of Influence to work in Fundraising. *Stanford Social Innovation Review*. 17-27.

21. Cialdini, R. B. & Goldstein, N. J. (2002). The Science and Practice of Persuasion. *Cornell Hotel and Restaurant Administration Quarterly*, 40-50.
22. Vgl. Sagarin, B. J./Mitnick, K. D. (2012). The Path of Least Resistance. In: D. T. Kenrick, N. J. Goldstein, & S. L. Braver (Eds.), *Six Degrees of Social Influence - Science, Application, and the Psychology of Robert Cialdini* (pp. 27-38). Oxford: Oxford University Press.
23. Hobson, R. P. (2012). Emotion as Personal Relatedness. *Emotion Review*, 4(2), 169-175.
24. Festinger, L. (1957). A theory of cognitive dissonance. Stanford, Calif: Stanford University Press.
25. Rogers, C. R. (1957). The necessary and sufficient conditions of therapeutic personality change. *Journal of Consulting Psychology*, 21, 95-103.
26. Neuhaus, T. (2021). A Nudge Psychology Perspective on Digital Marketing and Communication: Learning from the Nigerian Scam. In: María Dolores Olvera-Lobo, Juncal Gutiérrez-Artacho, Irene Rivera-Trigueros, Mar Díaz-Millón (Eds.). *Innovative Perspectives on Corporate Communication in the Global World* (S. 122-140). IGI Global Publishing. Hershey, Pennsylvania.
27. Tversky, A./Kahneman, D. (1991). Loss Aversion in Riskless Choice: A Reference- Dependent Model. *The Quarterly Journal of Economics*, 106 (4), 1039-1061.
28. Tversky, A./Kahneman, D. (1981). The Framing of Decisions and the Psychology of Choice. *Science*, 210, 453-458.