Löse dein Problem mit einem Augenzwinkern

Der Mann von der Bank kennt meinen Namen und hat viel zu viel Zeit

Wie du einen gefälschten Bankanruf erkennst und die Identität des Anrufers selbst überprüfst



Max Paradox

Der Mann von der Bank kennt meinen Namen und hat viel zu viel Zeit

Wie du einen gefälschten Bankanruf erkennst und die Identität des Anrufers selbst überprüfst

Max Paradox

Rozwiąż swój problem z przymrużeniem oka

ISBN: 9788384905715

ALL-IN Rafał Płonkowski



INHALTSVERZEICHNIS

INTRO 5

Kapitel 1 - Guten Tag, ich rufe von der Bank an. Zumindest behaupte ich das 12

Kapitel 2 - Woher weiß er das alles? Die Anatomie des Vertrauens auf Kredit 22

Kapitel 3 - In fünf Minuten ist dein Geld weg: Wie der Betrüger dir zuerst die Zeit stiehlt, bevor er dir irgendetwas anderes nimmt 33

Kapitel 4 - Drei magische Worte: „Ich kenne mich aus." Warum vermeintliche Sicherheitsmaßnahmen versagen 43

Kapitel 5 - Entschuldigung, dass ich mich nicht betrügen lasse. Die Falle übertriebener Höflichkeit 55

Kapitel 6 - Bitte klicken Sie hier. Die Technik, die helfen sollte und plötzlich Befehle erteilt 66

Kapitel 7 - Nur noch ein letzter Schritt. Warum es so schwer ist, ein begonnenes Verfahren abzubrechen..... 77

Kapitel 8 - Wenn der Betrüger die Uniform der Autorität anzieht. Warum ein Amtstitel keinen Beweis ersetzt..... 87

Kapitel 9 - Leg auf, aber mit Köpfchen. Die Kunst, die Kontrolle über dein Telefon zurückzugewinnen..... 97

Kapitel 10 - Überprüfe die Bank, nicht die Geschichte. Wie du einen Anrufer wirklich verifizierst.....107

Kapitel 11 - Der Code ist angekommen, also ist alles in Ordnung? Wie du Bankmitteilungen liest, bevor es zu spät ist 117

Kapitel 12 - Ich habe den Code schon weitergegeben. Was jetzt? Erste Hilfe für dein Konto ohne Panik und Selbstvorwürfe 128

Kapitel 13 - Der Bankanruf unter der Lupe. Wie du eine verdächtige Geschichte überprüfst, ohne Detektiv zu werden.....140

Kapitel 14 - Das häusliche Sicherheitszentrum. Bereite dich vor, bevor der Herr zur Rettung deiner Ersparnisse anruft 151

Kapitel 15 - Die Bank geht nicht ran, das Telefon spielt verrückt und der Betrüger ist bestens gelaunt. Was tun, wenn der perfekte Plan zusammenbricht?.....162

Kapitel 16 - Das Geld ist weg und der Herr von der Bank verschwunden. Wie du nach einem Betrug wieder Ordnung in die Sache bringst 173

Kapitel 17 - Es ist nicht mein Konto, aber mein Problem. Wie du einem Angehörigen hilfst, der mit einem Betrüger telefoniert.....184

Kapitel 18 - Sichere Gewohnheiten statt täglichem Misstrauen. Wie du aufmerksam bleibst, ohne ständig in Alarmbereitschaft zu leben.....195

Kapitel 19 - Sie rufen schon wieder an. Wie du eine wiederkehrende Bedrohung erkennst, bevor sie erneut deine Aufmerksamkeit gewinnt..... 205

Kapitel 20 - Der Herr von der Bank kann warten. Dein Geld, deine Regeln.....216

INTRO

Um 14:37 Uhr klingelt das Telefon. Die Nummer kommt dir bekannt vor, vielleicht ähnelt sie sogar der Nummer auf der offiziellen Website deiner Bank. Du gehst ran, schließlich bist du ein verantwortungsbewusster Mensch. Am anderen Ende meldet sich ein höflicher Mann, stellt sich als Mitarbeiter der Sicherheitsabteilung vor, nennt deinen Vor- und Nachnamen und erklärt anschließend, dass gerade ein verdächtiger Überweisungsversuch von deinem Konto festgestellt worden sei. Das klingt ernst. Sehr ernst sogar. Vor allem, weil der Herr ruhig, professionell und mit einer Selbstsicherheit spricht, als hätte er gerade persönlich das weltweite Finanzsystem gerettet und nun noch fünf Minuten gefunden, um sich um deine Ersparnisse zu kümmern.

Das Problem ist nur, dass du keine Ahnung hast, wer er wirklich ist.

Der Mann kennt deinen Namen. Er weiß, bei welcher Bank du ein Konto hast. Er kann den Namen des Ortes nennen, in dem du wohnst, und manchmal sogar einen Teil deiner Kontonummer. Alles stimmt, also beginnt dein Gehirn mit einer ziemlich riskanten Operation: Es verwandelt die Kenntnis einiger Informationen in einen Beweis für die Glaubwürdigkeit des Gesprächspartners. Dabei sind Vorname, Nachname und Telefonnummer keine geheimnisvollen Zauberformeln, die ausschließlich Bankangestellten zur Verfügung stehen. Solche Daten können auf unterschiedlichen Wegen in die falschen Hände geraten sein. Und die angezeigte Telefonnummer? Leider sagt auch sie nicht immer die Wahrheit. Eine Technik namens Spoofing ermöglicht es, auf deinem Bildschirm eine

andere Nummer erscheinen zu lassen, als es der tatsächlichen Herkunft des Anrufs entspricht.

Und genau deshalb gibt es dieses Buch. Nicht, damit du ab morgen jeden Anruf mit den Worten entgegennimmst: „Bitte nennen Sie mir den Geburtsnamen der Mutter des Bankvorstandsvorsitzenden und die dritte Ziffer der Schuhgröße des Filialleiters." Obwohl ich zugeben muss, dass das eine interessante Methode wäre, um Telefonverkäufer abzuschrecken. Es geht um etwas wesentlich Praktischeres: zu lernen, Situationen zu erkennen, in denen jemand versucht, dein Vertrauen auszunutzen, und die Identität eines Gesprächspartners zu überprüfen, ohne dabei den Anweisungen genau des Menschen zu folgen, dessen Identität du gerade überprüfen möchtest.

Denn darin liegt die größte Absurdität der ganzen Situation. Ein Fremder ruft an, behauptet, Bankmitarbeiter zu sein, und wenn du um eine Bestätigung bittest, schlägt er vor, dass du ihm einfach glaubst. Wahlweise kann er dich auch mit seinem Vorgesetzten verbinden. Diesen Vorgesetzten gibt es selbstverständlich, zumindest innerhalb dieses Telefongesprächs. Vielleicht sitzt er auf dem Stuhl daneben, besitzt dasselbe Telefon und wurde gerade zum Leiter der Sicherheitsabteilung befördert, weil er seine Stimmlage so beeindruckend verändern kann.

Telefonbetrug beginnt nicht immer mit einer plumpen Lüge. Häufig wirkt er wie ein professionell vorbereitetes Verfahren. Dein Gesprächspartner kann die richtigen Fachbegriffe verwenden, grundlegende Bankabläufe kennen und genau wissen, welche Mitteilungen du von einem Finanzinstitut erwartest. Er kann dich sogar vor Betrügern warnen, was besonders dreist ist, ihm aber leider durchaus

nützen kann. Wenn jemand behauptet, dich vor Kriminellen zu schützen, möchtest du ihn natürlich als jemanden betrachten, der auf der richtigen Seite steht. Nur ist die Behauptung, Schutz zu bieten, noch lange kein Schutz. Ein Feuerwehrmann mit einem Plastikhelm kann ebenfalls „Feuer!“ rufen. Bevor du ihm allerdings deine Wohnungsschlüssel überlässt, solltest du überprüfen, ob er tatsächlich mit einem Feuerwehrfahrzeug gekommen ist.

Das wichtigste Werkzeug eines Betrügers ist manchmal nicht die Technik, sondern der Druck, den er aufbaut. Du hörst, dass dein Geld gleich verschwinden wird, dass du sofort handeln musst, dass du das Gespräch auf keinen Fall unterbrechen darfst und dass jede Rücksprache mit anderen Personen die Sicherheit deines Kontos gefährden könnte. Mit jedem weiteren Satz wird der Raum für ruhiges Nachdenken kleiner. Du musst keineswegs leichtgläubig sein, um dabei Anspannung zu verspüren. Es genügt, dass du Ersparnisse besitzt, Rechnungen bezahlen musst und die Vorstellung nicht besonders reizvoll findest, dass jemand auf deine Kosten einen neuen Fernseher kauft. Der Betrüger muss dich nicht von allem gleichzeitig überzeugen. Es reicht, wenn du einem ersten, scheinbar harmlosen Schritt zustimmst. Anschließend nutzt er aus, dass du bereits in das Gespräch verwickelt bist.

Vielleicht denkst du jetzt, dass du niemals auf so etwas hereinfallen würdest. Das ist eine ausgesprochen angenehme Überzeugung. Leider führt ein Betrüger keinen Intelligenztest durch. Er sucht nach einem Moment, in dem du beschäftigt, müde, verängstigt oder schlicht davon überzeugt bist, mit der richtigen Person zu sprechen. Jemand kann die Sicherheitsregeln hervorragend kennen und trotzdem einen Fehler machen, wenn am anderen Ende

der Leitung eine dramatische Warnung über das eigene Geld ausgesprochen wird. Deshalb ist es sinnvoller, sich eine einfache Vorgehensweise anzugewöhnen, als ein Gefühl der Unbesiegbarkeit zu entwickeln. Eine Vorgehensweise, die auch dann funktioniert, wenn deine Konzentration beschlossen hat, eine Mittagspause einzulegen.

In diesem Buch lernst du, zwischen Informationen zu unterscheiden, die glaubwürdig klingen, und solchen, die tatsächlich etwas bestätigen. Du wirst sehen, woran du typische Versuche erkennst, Druck auszuüben, warum eine vertraute Nummer auf dem Display keine Sicherheitsgarantie bietet und welche Bedeutung Aufforderungen haben, Codes oder Passwörter preiszugeben, Anwendungen zu installieren oder Überweisungen auszuführen. Vor allem aber wirst du ein Prinzip kennenlernen, mit dem du die Kontrolle über das Gespräch zurückgewinnen kannst: Du entscheidest selbst, über welchen unabhängigen Kontaktweg du deine Bank erreichst, anstatt in dem Kommunikationskanal zu bleiben, den ein Fremder für dich ausgewählt hat.

Stell dir vor, jemand berichtet dir am Telefon von einer verdächtigen Transaktion. Statt dich auf eine Diskussion einzulassen, beendest du das Gespräch. Anschließend öffnest du selbstständig die offizielle App deiner Bank oder verwendest eine Telefonnummer, die du auf ihrer echten Website oder auf deiner Bankkarte findest. Du kontaktierst die Bank unabhängig vom vorherigen Anrufer und fragst nach, ob tatsächlich ein Problem vorliegt, das ein Eingreifen erfordert. Du wählst keine Nummer, die dir der Anrufer diktiert hat, klickst nicht auf einen zugesandten Link und betrachtest einen erneuten Anruf derselben Person nicht als Identitätsbestätigung. Das ist keine spektakuläre Geheimdiensttechnik. Du brauchst weder einen Knopf im

Ohr noch eine dunkle Sonnenbrille oder den Decknamen „Operation Festgeld“. Du brauchst lediglich eine Regel, die sich auch unter Druck anwenden lässt.

Natürlich sind echte Situationen manchmal komplizierter als ein schön übersichtliches Beispiel. Was machst du, wenn der Anrufer Einzelheiten über dein Konto kennt? Wenn er behauptet, dass du dein Geld verlierst, sobald du auflegst? Wenn er dich auffordert, einen Vorgang in der Banking-App zu bestätigen, obwohl er gerade noch versichert hat, genau diesen Vorgang verhindern zu wollen? Und was passiert, wenn du bereits einige Informationen preisgegeben oder eine Anweisung befolgt hast und erst jetzt bemerkst, dass etwas nicht stimmt? In solchen Momenten brauchst du keine Selbstvorwürfe, sondern eine verständliche Reihenfolge konkreter Maßnahmen. Nicht jeder Fehler bedeutet automatisch, dass Geld verloren geht. Manche Fehler erfordern jedoch einen sofortigen Kontakt mit der Bank und die Absicherung deiner Zugänge. Aus Angst vor einer peinlichen Situation zu zögern, kann am Ende teurer werden als der ursprüngliche Fehler.

Wir werden auch nicht so tun, als wäre jeder Anruf einer Bank automatisch ein Betrugsversuch. Banken nehmen tatsächlich Kontakt zu ihren Kunden auf, auch in Sicherheitsangelegenheiten. Das Ziel besteht also nicht darin, gesunde Vorsicht in grenzenloses Misstrauen gegenüber jedem Menschen mit einem Telefonhörer zu verwandeln. Es geht darum, zwei Dinge voneinander zu unterscheiden: eine Information anzuhören und eine Anweisung auszuführen. Du kannst eine Warnung ernst nehmen, ohne automatisch die Identität der Person anzuerkennen, die sie übermittelt. Du kannst höflich bleiben, ohne persönliche Daten preiszugeben. Du kannst ein

Gespräch beenden, ohne um Erlaubnis zu bitten. Und vor allem kannst du die Situation eigenständig überprüfen, selbst wenn dein Gesprächspartner dir erklärt, dass dies absolut unmöglich sei.

Gerade das ist manchmal besonders komisch. Ein Institut, dem du dein Geld anvertraut hast, soll dir angeblich verbieten, es über seine offiziellen Kontaktwege zu erreichen. Das klingt ungefähr so, als würde ein Restaurant davor warnen, dass die Überprüfung seiner Adresse auf der eigenen Website eine Explosion in der Küche auslösen könnte. Wenn jemand dich hartnäckig daran hindert, eine unabhängige Überprüfung vorzunehmen, musst du nicht erst beweisen, dass er ein Betrüger ist, bevor du aufhörst, seinen Anweisungen zu folgen. Es genügt, dass du keine Bestätigung dafür hast, mit wem du tatsächlich sprichst.

Ich verspreche dir nicht, dass dich nach der Lektüre dieses Buches nie wieder ein Krimineller überraschen wird. Betrugsmethoden verändern sich, und selbst vernünftige Menschen können Fehler machen. Du kannst jedoch lernen, so zu reagieren, dass dir ein einzelner Telefonanruf nicht die Möglichkeit nimmt, eigenständige Entscheidungen zu treffen. Anstatt zu versuchen, dir jedes denkbare Betrugsszenario einzuprägen, entwickelst du die Gewohnheit, Informationsquellen zu überprüfen, Manipulationsversuche zu erkennen und Handlungen zu stoppen, deren Konsequenzen du nicht verstehst.

Und wenn das nächste Mal der Herr von der Bank anruft, der deinen Vor- und Nachnamen kennt und offenbar unbegrenzt Zeit besitzt, um dein Vermögen zu retten, musst du nicht mehr erraten, ob er ein Held ist oder ein Mensch mit einer außergewöhnlich flexiblen Einstellung zum Eigentum anderer Leute. Du bedankst dich für die Information,

beendest das Gespräch und überprüfst die Angelegenheit selbst an der richtigen Stelle.

Der Mann darf deinen Namen kennen. Das bedeutet noch lange nicht, dass er auch das letzte Wort haben muss.

Kapitel 1 - Guten Tag, ich rufe von der Bank an. Zumindest behaupte ich das

Das Beunruhigendste an einem Telefonbetrug ist, dass sein Anfang vollkommen unspektakulär sein kann. Kein finsteres Lachen, keine dramatische Musik und keine Stimme eines Menschen, der schon als Kind davon geträumt hat, eine kriminelle Karriere einzuschlagen. Nur ein gewöhnlicher Anruf, eine höfliche Begrüßung und ein Satz, ausgesprochen im Tonfall einer Person, die solche Probleme jeden Tag löst. Würde man einen Gesprächspartner ausschließlich nach seinen Umgangsformen beurteilen, bekäme so mancher Betrüger eine hervorragende Bewertung und gleich noch das Angebot, eine Schulung zum Thema Kundenservice zu leiten. Leider sind gute Manieren kein Zertifikat für Ehrlichkeit, und eine professionell klingende Stimme beweist noch lange nicht, dass jemand tatsächlich bei einer Bank beschäftigt ist.

Stell dir Marta vor, die gerade vom Einkaufen zurückgekommen ist. Sie versucht, ihre Einkaufstaschen auszupacken, Platz für Produkte zu finden, die sie ganz bestimmt nicht kaufen wollte, und gleichzeitig ihre Familie davon zu überzeugen, dass Joghurt in den Kühlschrank gehört und man darüber keine stundenlangen Verhandlungen führen muss. In diesem Moment klingelt das Telefon. Ein Mann stellt sich als Adam Kowalski von der Sicherheitsabteilung ihrer Bank vor und berichtet von einem Versuch, eine nicht autorisierte Transaktion durchzuführen. Er nennt den Namen der Bank, Martas Vornamen und die letzten Ziffern ihrer Telefonnummer. Anschließend fragt er, ob sie gerade versucht habe, eine Überweisung

auszuführen. Marta antwortet mit Nein. Der Gesprächspartner erklärt sofort, dass er genau das befürchtet habe. Seine Stimme wird ernster, bleibt aber höflich. Das Ganze klingt so glaubwürdig, dass Marta ihre Einkäufe stehen lässt und sogar das Speiseeis vergisst, das gerade seine unwiderrufliche Verwandlung in eine süße Suppe beginnt.

In dieser kurzen Szene ist etwas Wichtigeres passiert als die bloße Weitergabe einer Information. Der Anrufer hat die Kontrolle über Martas Aufmerksamkeit übernommen. Noch einen Augenblick zuvor entschied sie selbst, was sie mit ihrem Nachmittag anfangen wollte. Jetzt bestimmt ein Fremder ihre Prioritäten, beschreibt eine Bedrohung und vermittelt ihr den Eindruck, dass nur die Zusammenarbeit mit ihm einen finanziellen Schaden verhindern könne. Genau das ist einer der Gründe, warum gefälschte Bankanrufe manchmal erfolgreich sind. Der Betrüger muss nicht sofort nach Geld fragen. Zunächst braucht er einen Platz in deinem Kopf, vorzugsweise dort, wo du die wirklich dringenden Angelegenheiten unterbringst.

Wenn das Gespräch genauso abläuft, wie es sollte

Viele Menschen stellen sich einen Betrüger als jemanden vor, der nervös spricht, die Namen von Institutionen verwechselt und in jedem zweiten Satz eine Überweisung auf das Konto seines Cousins vorschlägt. Solche Gesprächspartner mag es ebenfalls geben, aber die eigene Sicherheit darauf aufzubauen, dass ein Betrüger schon offensichtliche Fehler machen wird, ist riskant. Ein gut vorbereiteter Krimineller kann die Gesprächsführung echter Bankberater nachahmen. Er verwendet förmliche Wendungen, nennt seine Position, kann eine Mitarbeiternummer angeben und spricht in der Sprache

betrieblicher Abläufe. Manchmal hört man im Hintergrund andere Gespräche, die an die Arbeit eines großen Callcenters erinnern. Der Eindruck einer gut organisierten Arbeitsumgebung beweist jedoch nicht, dass der Anruf tatsächlich von einer Bank kommt.

Es lohnt sich, den Unterschied zwischen einer Information, die dein Gesprächspartner nennt, und einer Information, die unabhängig bestätigt wurde, zu verstehen. Wenn jemand sagt: „Mein Name ist Adam Kowalski, ich bin leitender Spezialist für Sicherheitsfragen“, erfährst du zunächst nur, wie diese Person sich vorstellen möchte. Wenn er anschließend seine dienstliche Kennnummer nennt, stammt auch diese Information weiterhin aus derselben Quelle. Natürlich kannst du seinen Namen und die Kennnummer notieren. Du solltest sie aber nicht als Eintrittskarte zu deinem Vertrauen betrachten. Sonst würde es genügen, einen eleganten Notizblock zu kaufen, einige Bankbegriffe auswendig zu lernen und anschließend die eigene Beförderung zum Sicherheitsdirektor der gesamten Galaxie bekannt zu geben.

Ein echter Bankberater kann Kundendaten kennen, weil er Zugriff auf die Systeme der Bank hat. Ein Betrüger kann allerdings ebenfalls über einen Teil dieser Informationen verfügen, den er sich auf unterschiedliche Weise beschafft hat. Deshalb reichen ein übereinstimmender Nachname, eine richtige Adresse oder einige zutreffende Einzelheiten nicht aus. Viel wichtiger ist, was der Gesprächspartner von dir erwartet und ob er dich daran hindert, die Situation über einen unabhängigen, offiziellen Kontaktweg zu überprüfen. Besonders beunruhigend sind Aufforderungen, Passwörter, Autorisierungscodes oder PINs preiszugeben, unbekannte Software zu installieren oder Vorgänge zu bestätigen, die du

selbst nicht veranlasst hast. Bei solchen Anweisungen solltest du sofort innehalten, ganz gleich, wie überzeugend die angebliche Gefahr geschildert wird.

Eine echte Bank kann dich wegen eines Sicherheitsproblems anrufen. Daraus folgt jedoch nicht, dass du jedes Gespräch so lange fortsetzen musst, bis der Anrufer es für beendet erklärt. Du darfst sagen, dass du selbst Kontakt mit der Bank aufnehmen wirst. Du musst deinen Gesprächspartner weder von deiner Entscheidung überzeugen noch ausführlich erklären, warum du ihm nicht vertraust. Ein Telefonat ist keine Gerichtsverhandlung, und du bist nicht verpflichtet, vor dem Auflegen Beweismaterial vorzulegen.

Die erste Falle: Höflichkeit mit Verpflichtung verwechseln

Kehren wir zu Marta zurück. Der falsche Bankberater stellt ihr weitere Fragen. Zunächst sind es einfache Fragen, auf die sie problemlos antworten kann. Hat sie ein Konto bei dieser Bank? Nutzt sie die mobile Banking-App? Hat sie kürzlich eine Überweisung an einen unbekannten Empfänger vorgenommen? Mit jeder Antwort wirkt das Gespräch natürlicher. Marta hat zunehmend das Gefühl, an einem gewöhnlichen Sicherheitsverfahren teilzunehmen. Gleichzeitig entwickelt sie ein unterschwelliges Gefühl der Verpflichtung zur Zusammenarbeit. Schließlich nimmt sich da jemand Zeit, um ihr in einer gefährlichen Situation zu helfen.

So funktioniert der Mechanismus einer schrittweisen Einbindung. Der Anrufer muss nicht mit einer Bitte beginnen, die sofort Widerstand auslöst. Er kann zunächst eine Reihe von Antworten erhalten und erst danach zu immer anspruchsvolleren Anweisungen übergehen. Wenn du einige harmlose Fragen beantwortet hast, bedeutet das

selbstverständlich nicht, dass du später nicht mehr Nein sagen darfst. Das Problem entsteht, wenn jemand seine bisherige Bereitschaft zur Zusammenarbeit als Verpflichtung betrachtet, auch weiterhin mitzumachen. Weil er bereits so viel erzählt hat, erscheint ihm das Beenden des Gesprächs plötzlich unhöflich oder unvernünftig.

Diese Täuschung solltest du möglichst früh durchschauen. Du darfst das Gespräch nach dem ersten Satz beenden, nach der fünften Frage oder nach zehn Minuten. Es gibt keine Regel, nach der die Zeit, die du einem Fremden gewidmet hast, dich dazu verpflichtet, ihm weitere Informationen zu liefern. Wenn du während des Gesprächs ein ungutes Gefühl bekommst, ist das bereits ein ausreichender Grund, innezuhalten. Du musst nicht warten, bis eine Forderung so verdächtig wird, dass ein Alarm ertönt und dein Telefon von selbst die Meldung „ACHTUNG, BETRÜGER!“ anzeigt.

In der Praxis hilft es, einen einzigen ruhigen Satz vorzubereiten: „Vielen Dank für die Information. Ich werde das Gespräch jetzt beenden und mich selbst über einen offiziellen Kontaktweg mit meiner Bank in Verbindung setzen.“ Dieser Satz enthält keine Anschuldigung, lädt nicht zu einer Diskussion ein und beschreibt eindeutig deinen nächsten Schritt. Wenn der Anrufer protestiert, kannst du deine Entscheidung wiederholen und anschließend auflegen. Du brauchst dafür nicht seine Zustimmung. Außerdem sollte jemand, dem die Sicherheit deines Geldes tatsächlich am Herzen liegt, nicht erwarten, dass du auf eine vernünftige Überprüfung verzichtest, nur um seine Gefühle nicht zu verletzen.

Die zweite Falle: Eine vertraute Nummer auf dem Display

Martas Telefon zeigt eine Nummer an, die der Telefonnummer ihrer Bank ähnelt. Das bestärkt sie zusätzlich in der Annahme, dass alles seine Richtigkeit hat. Schließlich fällt es schwer, ein Telefon der Lüge zu verdächtigen. Das Gerät hat mehrere Tausend Złoty gekostet, kann das Gesicht seines Besitzers erkennen und eine Route bis ans andere Ende Europas berechnen. Da sollte es doch wohl wissen, wer gerade anruft. Leider bedeuten die technischen Fähigkeiten eines Smartphones nicht, dass jede angezeigte Information über einen Anruf zuverlässig überprüft wurde.

Beim sogenannten Spoofing kann eine Telefonnummer so vorgetäuscht werden, dass auf dem Bildschirm des Empfängers eine andere Nummer erscheint als die des tatsächlichen Anrufers. Es gibt technische Maßnahmen, die solche Missbrauchsmöglichkeiten einschränken, doch du solltest nicht davon ausgehen, dass die angezeigte Nummer immer die Identität des Anrufers garantiert. Auch das Speichern der Banknummer in deinen Kontakten löst dieses Problem nicht. Dein Telefon kann einen vertrauten Kontaktnamen anzeigen, weil es die übermittelte Rufnummer wiedererkennt, und nicht, weil es persönlich die Beschäftigungsunterlagen des Menschen am anderen Ende der Leitung kontrolliert hätte.

Dabei solltest du zwischen einem eingehenden Anruf und einer selbst hergestellten Verbindung unterscheiden. Wenn jemand dich anruft, beginnt er die Kommunikation und behauptet, eine bestimmte Person zu sein. Wenn du hingegen selbst eine Telefonnummer wählst, die du aus einer vertrauenswürdigen, unabhängigen Quelle erhalten hast, bestimmst du wieder selbst, mit welcher Institution du Kontakt aufnehmen möchtest. Das ist keine magische

Garantie dafür, dass sämtliche Probleme gelöst werden, verändert die Situation aber erheblich. Du bist nicht länger ausschließlich auf die Behauptungen eines Fremden angewiesen.

Dabei darfst du allerdings weder eine Telefonnummer verwenden, die dir der verdächtige Anrufer per SMS geschickt hat, noch einen Link öffnen, den er dir gerade genannt hat. Das wäre ungefähr so, als würdest du die Ehrlichkeit eines Verkäufers verdächtiger Luxusuhren überprüfen, indem du seinen Freund anrufst, den er dir als unabhängigen Echtheitsexperten empfohlen hat. Die Kontaktinformationen müssen aus einer Quelle stammen, der du unabhängig von diesem Gespräch vertraust, beispielsweise aus der offiziellen Banking-App, von der echten Website, die du selbst aufgerufen hast, oder aus Unterlagen, die dir die Bank bereits zuvor zur Verfügung gestellt hat.

Die Gefahr zu erkennen beginnt mit der richtigen Frage

Du wirst nicht immer wissen, ob dein Gesprächspartner ein Betrüger ist. Und du musst es auch nicht sofort wissen. Eine angemessene Reaktion setzt nicht voraus, dass du innerhalb von dreißig Sekunden einen Kriminalfall löst. Es reicht zu erkennen, dass die Identität der Person am anderen Ende der Leitung nicht unabhängig bestätigt wurde und dass sie gleichzeitig versucht, Einfluss auf deine finanziellen Entscheidungen zu nehmen. Das allein ist bereits ein ausreichender Grund, ihre Anweisungen vorerst nicht auszuführen.

Viele Menschen konzentrieren sich auf die Frage: „Klingt dieser Mensch glaubwürdig?“ Wesentlich hilfreicher ist die Frage: „Was kann ich gefahrlos tun, ohne davon auszugehen, dass dieser Mensch die Wahrheit sagt?“ Die

erste Frage zwingt dich dazu, Stimme, Verhalten und Einzelheiten zu beurteilen, die möglicherweise sorgfältig vorbereitete Bestandteile eines Betrugsversuchs sind. Die zweite ermöglicht dir, eine Entscheidung unabhängig von diesen Eindrücken zu treffen. Du kannst dir die Information über die angebliche Transaktion notieren, das Gespräch beenden und die Angelegenheit selbst überprüfen. Dafür brauchst du weder die Gewissheit, dass dein Gesprächspartner lügt, noch einen Beweis dafür, dass er ehrlich ist.

Genau das tut Marta, als sie einen Augenblick Ruhe zurückgewinnt. Sie erklärt, dass sie selbst bei der Bank anrufen werde. Der Mann erwidert, dafür sei keine Zeit, und jede weitere Minute erhöhe das Risiko, Geld zu verlieren. Marta spürt die Anspannung, ändert ihre Entscheidung aber nicht. Sie beendet das Gespräch, öffnet ihre offizielle Banking-App und nutzt die dort angebotene Kontaktmöglichkeit. Sie schildert den Anruf und bittet darum, ihr Konto zu überprüfen. Erst die Informationen, die sie über diesen unabhängigen Kontakt erhält, bilden die Grundlage für ihre weiteren Entscheidungen.

In dieser Beispielgeschichte stellt sich heraus, dass die Bank den angeblichen Überweisungsversuch nicht bestätigen kann. Marta muss weder wissen, wer der Anrufer tatsächlich war, noch, woher er ihre Daten hatte. Sie hat das Notwendige getan: Sie hat keine vertraulichen Informationen preisgegeben, keinen Vorgang bestätigt und nicht zugelassen, dass ein Fremder bestimmt, wie sie seine Behauptungen überprüfen soll.

Und das Speiseeis? Leider gehört die Sicherung von Tiefkühlprodukten nicht zu den Aufgaben einer Bank. Jedes Verfahren hat seine Grenzen.

Warum gesunder Menschenverstand nicht immer ausreicht

Es ist leicht zu sagen, man müsse einfach seinen gesunden Menschenverstand benutzen. Schwieriger ist es zu erklären, was das genau bedeutet, wenn jemand behauptet, dass das über mehrere Jahre angesparte Geld in Gefahr sei. Gesunder Menschenverstand ist kein Knopf, den du drücken kannst, um deine Angst sofort auszuschalten. Er besteht eher aus einer Reihe vorher festgelegter Regeln, dank derer du nicht jede Entscheidung von Grund auf neu treffen musst.

Deshalb ist es sinnvoll, bereits vor einem verdächtigen Anruf zu wissen, wo du die offiziellen Kontaktinformationen deiner Bank findest und wie eine sichere Kommunikation mit ihren Mitarbeitern aussieht. Du kannst dich in der Banking-App über die verfügbaren Hilfekanäle informieren, die Sicherheitshinweise deiner Bank lesen und herausfinden, wie du bei nicht autorisierten Transaktionen reagieren solltest. Eine solche Vorbereitung ist keineswegs übertrieben. Genauso wenig, wie die Kenntnis eines Fluchtwegs bedeutet, dass du jeden Tag mit einem Brand rechnest, setzt die Kenntnis der Kontaktwege deiner Bank voraus, dass du glaubst, die ganze Welt wolle dein Konto übernehmen.

Wichtig ist außerdem, dass du deine eigene Sicherheit nicht ausschließlich anhand früherer Erfahrungen beurteilst. Die Tatsache, dass zehn Jahre lang kein verdächtiger Anruf zu einem Problem geführt hat, beweist nicht, dass der nächste ebenfalls harmlos sein wird. Andererseits bedeutet ein betrügerischer Anruf nicht automatisch, dass jemand bereits Zugriff auf dein Konto erlangt hat. Du musst zwischen einem Betrugsversuch und einer tatsächlichen

Verletzung deiner Kontosicherheit unterscheiden. Nach jedem unbekannten Anruf in Panik zu geraten, wäre genauso wenig praktikabel wie jedem Menschen bedingungslos zu vertrauen, der sich als Bankberater vorstellt.

Ein gut vorbereiteter Gesprächspartner kann ausgesprochen überzeugend klingen, während ein echter Bankmitarbeiter vielleicht einen schlechten Tag hat, undeutlich spricht oder die elegante Begrüßung vergisst. Deshalb solltest du deine Entscheidungen nicht von einem Wettbewerb um die größte telefonische Ausstrahlung abhängig machen. Sicheres Verhalten muss unabhängig davon funktionieren, ob der Anrufer die samtweiche Stimme eines Radiomoderators besitzt oder klingt wie jemand, der gerade seinen dritten Kaffee getrunken hat und den Montag immer noch nicht begreift.

Letztlich geht es nicht darum, eine Diskussion mit einem Betrüger zu gewinnen. Du musst ihm nicht beweisen, dass du seine Absichten durchschaut hast, und du brauchst das Gespräch nicht so lange fortzusetzen, bis er seine Schuld eingesteht. Manchmal ist das vernünftigste Ende schlicht das Auflegen. Ohne dramatische Pointe, ohne große Rede und ohne ein befriedigendes Finale, das einem Actionfilm würdig wäre.

Dein Geld braucht keinen spektakulären Helden. Es braucht einen Besitzer, der weiß, wann er aufhören sollte, einem Fremden zuzuhören.

Kapitel 2 - Woher weiß er das alles? Die Anatomie des Vertrauens auf Kredit

Wenn ein Fremder deinen Vornamen nennt, ist das normalerweise nicht besonders beeindruckend. Dein Name steht auf Paketen, in Nachrichten, auf Dokumenten und in Internetprofilen. Wenn der Anrufer allerdings auch deinen Nachnamen, den Namen deiner Bank und einige Einzelheiten aus deinem Leben erwähnt, sieht die Situation plötzlich anders aus. Du bekommst das Gefühl, mit jemandem zu sprechen, der über einen besonderen Zugang verfügt. In deinem Kopf entsteht eine einfache Gleichung: Wenn er diese Details kennt, muss er derjenige sein, für den er sich ausgibt. Das Problem ist nur, dass diese Gleichung auf einer falschen Annahme beruht und gerade jemand versucht, dir ihre Anwendung in Rechnung zu stellen.

Stell dir Tomasz vor, der während seiner Arbeitspause einen Anruf entgegennimmt. Eine Frau stellt sich als Bankmitarbeiterin vor, nennt seinen vollständigen Namen und spricht anschließend von seiner Bankkarte und verdächtigen Aktivitäten auf seinem Konto. Tomasz fragt, woher sie diese Informationen habe. Die Frau antwortet ruhig, sie könne die Angaben im System sehen. Sie nennt sogar einige Ziffern, die ihn an seine Kontonummer erinnern. Tomasz stellt keine weiteren Fragen. Wenn die Mitarbeiterin Zugriff auf das System hat, muss schließlich alles offiziell sein. Ihm kommt nicht in den Sinn, dass man den Satz „Ich sehe das hier im System“ auch dann sagen kann, wenn das gesamte System lediglich aus einer geöffneten Tabelle mit Kundendaten besteht.

Das bedeutet nicht, dass jeder Anrufer über eine solche Datenbank verfügt oder dass jeder bekannt gewordene Vorname aus einem Datenleck stammen muss. Informationen können auf unterschiedlichen Wegen in fremde Hände geraten, und manche sind öffentlich zugänglich. Manchmal reichen einige wenige Fragmente aus, um den Eindruck zu erwecken, jemand kenne die gesamte Geschichte eines Kunden. Wenn du diesen Unterschied verstehst, verändert sich deine Art, Gesprächspartner zu beurteilen. Du fragst nicht mehr nur, wie viel jemand über dich weiß, sondern überlegst, ob die genannten Einzelheiten tatsächlich seine Berechtigung beweisen.

Informationen sind kein Identitätsnachweis

Stell dir einen Menschen vor, der auf der Straße auf dich zukommt und sagt: „Guten Tag, ich weiß, dass Sie Tomasz heißen, in Łódź wohnen und letzte Woche ein Paket bestellt haben." Vermutlich wärst du überrascht. Vielleicht sogar beunruhigt. Aber folgt allein aus der Tatsache, dass dieser Mensch solche Informationen besitzt, dass du ihm deine Geldbörse zur Kontrolle überlassen solltest? Natürlich nicht. Am Telefon erscheint dieselbe Situation jedoch wesentlich offizieller, insbesondere wenn dein Gesprächspartner den Namen einer Bank verwendet und davon spricht, dein Geld schützen zu wollen.

Persönliche Daten sind nicht dasselbe wie Befugnisse. Jemand kann deinen Nachnamen kennen, ohne irgendein Recht zu haben, Vorgänge auf deinem Konto auszuführen. Er kann wissen, wo du arbeitest, ohne selbst bei der Institution beschäftigt zu sein, die er angeblich vertritt. Er kann über echte Informationen verfügen und gleichzeitig eine vollkommen erfundene Geschichte erzählen. Das ist