Löse dein Problem mit einem Augenzwinkern

Ich habe das perfekte Jobangebot gefunden. Offenbar hat es mich zuerst gefunden.

Wie du gefälschte Stellenanzeigen erkennst und deine persönlichen Daten bei der Jobsuche schützt



Max Paradox

Ich habe das perfekte Jobangebot gefunden. Offenbar hat es mich zuerst gefunden.

Wie du gefälschte Stellenanzeigen erkennst und deine persönlichen Daten bei der Jobsuche schützt

Max Paradox

Rozwiąż swój problem z przymrużeniem oka

ISBN: 9788384906620

ALL-IN Rafał Płonkowski



INHALTSVERZEICHNIS

INTRO 5

Kapitel 1 - Das perfekte Angebot oder warum der Betrüger deine beruflichen Träume kennt 11

Kapitel 2 - Der Recruiter aus dem Nichts oder wie geliehenes Vertrauen funktioniert 21

Kapitel 3 - Die teuerste kostenlose Bewerbung oder wenn der Bewerber plötzlich zahlen soll 33

Kapitel 4 - Das Formular will alles oder wie du nicht dein ganzes Privatleben der Personalabteilung überlässt 43

Kapitel 5 - Überall bewerben, nichts überprüfen oder wie die Erschöpfung bei der Jobsuche Betrügern hilft 56

Kapitel 6 - Vorstellungsgespräch oder Theateraufführung? Wie du nicht in ein gefälschtes Bewerbungsverfahren hineingezogen wirst 68

Kapitel 7 - Alle verdienen schon Geld, nur du überlegst noch. Die Falle des sozialen Beweises 82

Kapitel 8 - Dein Lebenslauf reist um die Welt oder wie du bei der Jobsuche unnötige digitale Spuren reduzierst 94

Kapitel 9 - Fünfzehn Minuten, die deine Daten retten können. So überprüfst du ein Stellenangebot vor der Bewerbung 107

Kapitel 10 - Sicher bewerben, Schritt für Schritt. Was du verschicken solltest, was nicht und wann du Stopp sagen musst 119

Kapitel 11 - Ich habe auch ein paar Fragen. Wie du mit einem Recruiter sprichst, ohne zu einem leichten Ziel zu werden 131

Kapitel 12 - Herzlichen Glückwunsch, du bist eingestellt. Jetzt überprüfe, was du eigentlich unterschreibst.....143

Kapitel 13 - Geklickt, verschickt, bestätigt. Was tun, wenn eine verdächtige Bewerbung schon zu weit gegangen ist? 155

Kapitel 14 - Melde es, bevor die Spuren verschwinden. Wie du aus einem Betrugsverdacht konkrete Maßnahmen machst 168

Kapitel 15 - Das Unternehmen ist echt, der Recruiter ist echt und der Betrug auch. Was tun, wenn alles authentisch aussieht? 181

Kapitel 16 - Wenn du wirklich dringend Arbeit brauchst. Sicherheit unter finanziellem und zeitlichem Druck 193

Kapitel 17 - Ich bin darauf hereingefallen. Wie du Ruhe, Vertrauen und den Mut zur weiteren Jobsuche zurückgewinnst 205

Kapitel 18 - Sicher nach Arbeit suchen, ohne täglich Detektiv zu spielen. Gewohnheiten, die langfristig bleiben 216

Kapitel 19 - Schon wieder hat mich jemand gefunden. Wie du eine wiederkehrende Bedrohung erkennst, bevor sie ernst wird 229

Kapitel 20 - Den perfekten Job gibt es. Aber er muss nicht nach deinem Passwort fragen. Wie du selbstständig sichere Entscheidungen triffst 241

INTRO

Stell dir vor, es ist Dienstag, 21:47 Uhr. Du scrollst gerade durch die nächste Stellenanzeige. Die vorherigen zwölf verlangten fünf Jahre Berufserfahrung, Kenntnisse in sieben verschiedenen Systemen und die Fähigkeit, unter Druck zu arbeiten. Letzteres bedeutet vermutlich, dass dich jemand über den Firmenmessenger anschreien wird. Die dreizehnte Anzeige sieht anders aus. Attraktives Gehalt, flexible Arbeitszeiten, Homeoffice, schnelle Einarbeitung und keine absurden Anforderungen. Das Unternehmen wächst angeblich dynamisch, erwartet diesmal aber nicht, dass du dich gemeinsam mit ihm kostenlos weiterentwickelst.

Du schickst deine Bewerbung ab. Acht Minuten später kommt die Antwort. Der Recruiter ist von deinem Profil begeistert, obwohl er in dieser Zeit wahrscheinlich nicht einmal die Bedienungsanleitung einer Kaffeemaschine hätte lesen können. Er lädt dich zur nächsten Runde ein. Du musst nur noch ein Formular ausfüllen, ein Foto deines Ausweises hochladen und deine Bankdaten bestätigen. Eine kleine Formalität. Schließlich muss ein seriöses Unternehmen wissen, mit wem es zusammenarbeitet.

Und genau hier beginnt eine Geschichte, die möglicherweise nicht mit einem neuen Job endet, sondern mit einer sehr langen Bekanntschaft mit der Hotline deiner Bank.

Gefälschte Bewerbungsverfahren gehören zu den besonders unangenehmen Betrugsmaschen, weil sie etwas vollkommen Normales ausnutzen: den Wunsch, eine bessere Arbeit zu finden. Du musst weder naiv noch unvorsichtig oder besonders leicht zu manipulieren sein. Es reicht, wenn

du von der Jobsuche erschöpft bist, dringend Geld brauchst oder einfach auf ein Angebot stößt, das so perfekt zu deinen Vorstellungen passt, dass du für einen Moment an die Existenz eines Unternehmens glauben möchtest, das ein hohes Gehalt, völlige Freiheit und einen Vorgesetzten bietet, der sich ausschließlich dann meldet, wenn er tatsächlich etwas zu sagen hat.

Ein Betrüger muss dich nicht von etwas überzeugen, das du gar nicht willst. Viel einfacher ist es, dir genau das zu versprechen, wonach du suchst.

Wenn der Traum einen Link zum Formular bekommt

Noch vor einiger Zeit konnte man eine verdächtige Stellenanzeige manchmal an ihrer Sprache erkennen. Da versprach jemand „viel großes Geld für wenig Arbeiten“, die Nachricht klang wie eine Übersetzung aus dem Inneren eines Kühlschranks, und die Absenderadresse bestand aus zufälligen Buchstaben sowie einem Firmennamen mit drei Schreibfehlern. Solche Hinweise können auch heute noch nützlich sein, aber sie reichen nicht mehr aus. Eine gefälschte Anzeige kann sprachlich einwandfrei, professionell gestaltet und mit einem überzeugenden Logo versehen sein. Dein Gesprächspartner kann Fachbegriffe verwenden, Unterlagen verschicken, die echten Bewerbungsformularen zum Verwechseln ähnlich sehen, und sogar ein Vorstellungsgespräch führen.

Gerade Letzteres ist besonders dreist. Da bereitet sich jemand sorgfältig auf die Frage nach seinen größten Schwächen vor, erklärt eine Lücke im Lebenslauf, berichtet ausführlich über seine Berufserfahrung, und auf der anderen Seite interessiert sich jemand vor allem dafür, ob sich der Kandidat zur Preisgabe vertraulicher Informationen bewegen lässt. Würden Betrüger genauso viel Mühe in eine ehrliche

Geschäftstätigkeit stecken, bräuchten sie vielleicht irgendwann selbst eine Personalabteilung.

Das Problem besteht darin, dass es bei der Jobsuche völlig normal ist, Informationen weiterzugeben. Ein Lebenslauf enthält Kontaktdaten, den beruflichen Werdegang und Angaben zur Ausbildung. Ein Recruiter kann nach deiner Verfügbarkeit, deinen Gehaltsvorstellungen oder deiner Erfahrung fragen. Als Bewerber gewöhnst du dich deshalb daran, Fragen zu beantworten und Unterlagen einzureichen. Genau diese Gewohnheit versucht ein Betrüger auszunutzen, indem er die Grenze zwischen einer berechtigten Bitte und einer Forderung verschiebt, die mit der jeweiligen Phase des Bewerbungsprozesses nichts Sinnvolles mehr zu tun hat.

Nicht jede Bitte um zusätzliche Informationen ist ein Versuch, Daten zu stehlen. Nicht jedes ungewöhnliche Gespräch ist Betrug, genauso wenig wie jede unbeholfen formulierte Nachricht automatisch von einem Kriminellen stammt. Auch echte Unternehmen machen Fehler, arbeiten mit externen Personalagenturen und organisieren Bewerbungsverfahren, deren Logik manchmal sogar den eigenen Recruitern verborgen bleibt. Deshalb werden wir nicht lernen, grundsätzlich jeden und alles zu verdächtigen. Wir werden lernen, zwischen Situationen zu unterscheiden, in denen normale Aufmerksamkeit genügt, und solchen, in denen du innehalten und überprüfen solltest, wer dir tatsächlich schreibt.

Deine Daten sind keine Eintrittskarte zum Vorstellungsgespräch

Viele Menschen stellen sich Datendiebstahl als spektakulären Hackerangriff vor. Tatsächlich beginnt manchmal alles mit einer höflichen Mitteilung: „Um den

Bewerbungsprozess fortzusetzen, bitten wir Sie, Ihre Angaben zu vervollständigen.“ Je nach Vorgehensweise kann ein Betrüger versuchen, an ein Foto deines Personalausweises, Zugangsdaten, Bestätigungscodes oder finanzielle Informationen zu gelangen. Vielleicht versucht er auch, dich zu einer Überweisung zu bewegen. Ebenso kann er dich auf eine gefälschte Website lotsen, dir einen verdächtigen Anhang schicken oder eine Anwendung zur Installation anbieten, die angeblich für das Vorstellungsgespräch unbedingt erforderlich ist.

Nicht alle diese Handlungen verursachen denselben Schaden. Allein deine E-Mail-Adresse verschafft niemandem automatisch Zugriff auf dein Bankkonto. Und wenn du deinen Lebenslauf verschickst, bedeutet das nicht, dass du am nächsten Morgen mit einem Kredit für eine Yacht aufwachst. Das Risiko hängt davon ab, welche Informationen offengelegt wurden, unter welchen Umständen das geschah und was der Täter anschließend damit unternimmt. Gerade deshalb lohnt es sich, diese Unterschiede zu verstehen, statt bei jeder Nachricht von einer unbekannten Nummer in Panik zu geraten.

Wir werden auch über Zeitdruck sprechen. Betrüger mögen Situationen, in denen Bewerber sofort entscheiden sollen, weil „das Angebot in Kürze abläuft“, „nur noch ein Platz frei ist“ oder „die Personalabteilung das System in fünfzehn Minuten schließt“. Eine bemerkenswerte Arbeitsorganisation: Angeblich garantiert das Unternehmen flexible Arbeitszeiten, aber sein Bewerbungssystem verhält sich wie ein Kassierer, der den Laden vor einem langen Feiertagswochenende abschließen will.

Eile ist noch kein Beweis für Betrug. Sie kann es jedoch erschweren, Informationen in Ruhe zu überprüfen. Und

genau diese Überprüfung ist häufig das, was wir am dringendsten brauchen.

Vorsicht muss nicht gleich Paranoia bedeuten

Dieses Buch soll nicht dazu führen, dass du keine Bewerbungen mehr verschickst, jede Einladung zum Vorstellungsgespräch löschst und einen Anruf vom Recruiter behandelst, als versuche jemand, die Kontrolle über einen Satelliten zu übernehmen. Ziel ist es, ein vernünftiges Gleichgewicht zwischen Offenheit für berufliche Möglichkeiten und dem Schutz deiner persönlichen Daten zu finden.

Du wirst erfahren, wie du Stellenangebote, Unternehmen, Internetadressen und die Identität von Personen überprüfen kannst, die ein Bewerbungsverfahren durchführen. Du wirst sehen, welche Informationen du in den einzelnen Phasen normalerweise weitergeben kannst, wann es sinnvoll ist, zusätzliche Fragen zu stellen, und wann du den Kontakt besser beendest. Wir werden uns außerdem damit beschäftigen, was du tun kannst, wenn du bereits auf einen verdächtigen Link geklickt oder persönliche Daten weitergegeben hast. Denn das Bewusstsein für eine Gefahr wird manchmal gerade dann am wichtigsten, wenn etwas nicht nach Plan gelaufen ist.

Du bekommst keine magische Liste von Wörtern, bei denen jeder Betrugsversuch sofort einen roten Alarm auslöst. Stattdessen erhältst du etwas Praktischeres: eine Denkweise, mit der du Situationen auch dann einschätzen kannst, wenn eine Nachricht glaubwürdig aussieht und dein Gesprächspartner professionell klingt.

Merke dir zunächst eine Frage, auf die wir unter verschiedenen Umständen zurückkommen werden: Kann ich

unabhängig bestätigen, dass diese Person tatsächlich das Unternehmen vertritt, für das sie sich ausgibt? Nicht indem du auf den nächsten Link klickst, den dir dieselbe Person geschickt hat, sondern indem du die Angaben über einen unabhängigen und vertrauenswürdigen Kontaktweg überprüfst. Eine so kleine Gewohnheit kann den Verlauf eines ganzen Gesprächs verändern.

Die Jobsuche kann schon für sich genommen anstrengend genug sein. Du brauchst nicht auch noch einen Nebenjob als Privatdetektiv. Was du brauchst, sind einige gut ausgewählte Regeln, die du selbst dann anwenden kannst, wenn du einen schwierigen Tag hinter dir hast, fünf Bewerbungen abgelehnt wurden und deine Begeisterung für ein weiteres Gespräch darüber, wo du dich in fünf Jahren siehst, ungefähr auf dem Niveau eines leeren Druckertoners liegt.

Am besten siehst du dich in einem Job, den es tatsächlich gibt.

Und genau damit fangen wir an.

Kapitel 1 - Das perfekte Angebot oder warum der Betrüger deine beruflichen Träume kennt

Marta sucht seit sechs Wochen nach einer neuen Stelle. Sie hat Berufserfahrung, einen aktuellen Lebenslauf, ein sorgfältig ausgearbeitetes berufliches Profil und eine zunehmend persönliche Beziehung zu automatischen Nachrichten, die mit den Worten „Vielen Dank für Ihr Interesse“ beginnen. Sie hat sich auf siebenunddreißig Stellen beworben. Von sieben Unternehmen erhielt sie eine Absage, zwei luden sie zum Vorstellungsgespräch ein, und die übrigen haben ihren Bewerbungsprozess offenbar in eine andere Dimension verlegt, in der die Zeit anders vergeht und niemand seine E-Mails liest.

Eines Nachmittags erscheint eine Nachricht. Ein Unternehmen sucht eine Spezialistin für die Betreuung von Geschäftskunden. Das Gehalt liegt über ihren Erwartungen, die Arbeit erfolgt vollständig im Homeoffice, die Arbeitszeiten sind flexibel, und Martas Erfahrung passt perfekt zu den Anforderungen. Der Recruiter schreibt höflich, konkret und verzichtet auf die nervige Frage, ob sie belastbar sei. Außerdem schlägt er ein Vorstellungsgespräch noch am selben Tag vor.

Marta ist erleichtert. Endlich hat jemand ihre Fähigkeiten erkannt. Sie muss nicht schon wieder beweisen, dass sie mit Tabellenkalkulationen umgehen, mit Menschen kommunizieren und gleichzeitig darauf verzichten kann, das Büro in Brand zu setzen. Jemand hat ihr Profil gelesen und die richtigen Schlussfolgerungen gezogen.

Zumindest glaubt sie das.

Die Nachricht könnte von einem echten Recruiter stammen. Sie könnte aber auch der Anfang eines Betrugsversuchs sein, bei dem die Kenntnis von Martas Berufserfahrung lediglich Teil eines sorgfältig vorbereiteten Köders ist. Die wichtigste Frage lautet zunächst nicht, ob das Unternehmen seriös ist. Sie lautet: Warum hat gerade dieses Angebot so schnell ihr Vertrauen gewonnen?

Die Antwort ist wesentlich interessanter als die schlichte Feststellung, dass Menschen gut bezahlte Arbeit mögen.

Ein Angebot, das dich besser versteht als dein früherer Vorgesetzter

Gefälschte Bewerbungsverfahren nutzen häufig ganz gewöhnliche Bedürfnisse von Menschen aus, die eine neue Beschäftigung suchen. Für den einen ist Sicherheit das Wichtigste, für die andere die Möglichkeit, von zu Hause aus zu arbeiten, und für wieder jemand anderen ein schneller Verdienst, mit dem sich die nächste Miete bezahlen lässt. Ein Betrüger muss nicht die gesamte Lebensgeschichte eines Bewerbers kennen. Es genügt, ein Bedürfnis zu erkennen, um das sich ein glaubwürdiges Versprechen aufbauen lässt.

Wer vom täglichen Pendeln erschöpft ist, wird auf ein Homeoffice-Angebot aufmerksam. Jemand, der sich seit Monaten erfolglos auf Juniorpositionen bewirbt, interessiert sich besonders für eine Anzeige, die keine Berufserfahrung voraussetzt. Ein Bewerber, der gerade seinen Arbeitsplatz verloren hat, reagiert möglicherweise besonders stark auf die Aussicht, sofort anfangen zu können. All diese Reaktionen sind vollkommen natürlich. Problematisch wird es erst, wenn die Attraktivität eines Angebots die Prüfung seiner Glaubwürdigkeit ersetzt.

Dabei lässt sich ein gewisses Paradox beobachten. Je besser eine Stellenanzeige zu unseren Bedürfnissen passt, desto größer ist unsere Motivation, ihre Schwachstellen zu übersehen. Das geschieht nicht bewusst. Unser Verstand beginnt einfach damit, eine Entscheidung zu rechtfertigen, die wir emotional längst getroffen haben. Wenn das Angebot außergewöhnlich großzügig ist, verfügt das Unternehmen vielleicht über ein großes Budget. Wenn das Bewerbungsverfahren blitzschnell abläuft, braucht die Firma vermutlich dringend jemanden. Wenn keine Berufserfahrung verlangt wird, setzt man dort möglicherweise tatsächlich auf Potenzial.

Jede dieser Erklärungen kann stimmen. Schwierig wird es, wenn sie ausschließlich in unserem Kopf entstehen und nicht auf überprüfbaren Informationen beruhen.

Sehen wir uns eine Stellenanzeige an, die eine hohe Vergütung für wenige Stunden einfacher Tätigkeiten pro Tag verspricht. Es gibt keine Regel, nach der gut bezahlte Arbeit zwangsläufig schwierig oder unangenehm sein muss. Es gibt allerdings eine vernünftige Frage: Für welchen konkreten Nutzen möchte das Unternehmen bezahlen? Wenn sich die Antwort auf allgemeine Formulierungen über die Erledigung von Aufgaben, die Unterstützung des Teams und die Bedienung einer Plattform beschränkt, erhält der Bewerber nicht genügend Informationen, um das Angebot beurteilen zu können.

Auch bei echten Bewerbungsverfahren stößt man gelegentlich auf unklare Stellenbeschreibungen. Der Unterschied zeigt sich darin, was passiert, wenn man nachfragt. Ein seriöser Unternehmensvertreter sollte die Aufgaben erklären oder an jemanden verweisen können, der

die Antwort kennt. Ein Betrüger versucht möglicherweise, eine Erklärung durch das nächste Versprechen zu ersetzen.

„Alle Einzelheiten erfahren Sie nach der Registrierung. Die Verdienstmöglichkeiten sind wirklich hervorragend."

Diese Antwort verrät ausgesprochen viel über das Gehalt. Vorausgesetzt, wir betrachten die Begeisterung des Gesprächspartners als belastbare Information.

Drei Bestandteile eines verdächtig schönen Angebots

Ein attraktives Stellenangebot ist nicht automatisch gefälscht, nur weil es vorteilhaft klingt. Trotzdem lohnt es sich zu prüfen, ob drei charakteristische Merkmale zusammenkommen: ein außergewöhnlich großes Versprechen, auffallend wenige konkrete Informationen und die Erwartung, möglichst schnell zu handeln.

Das erste Merkmal zieht die Aufmerksamkeit auf sich. Das zweite erschwert die Beurteilung der tatsächlichen Tätigkeit. Das dritte verkürzt die Zeit, in der mögliche Probleme auffallen könnten. Besonders gefährlich wird die Situation durch das Zusammenspiel dieser drei Faktoren.

Stell dir folgende Anzeige vor: „Homeoffice, attraktives Gehalt, vollständige Flexibilität, sofortiger Arbeitsbeginn." Das klingt angenehm, aber eigentlich weißt du überhaupt nicht, was du tun sollst. Geht es um Kundenbetreuung, Vertrieb, Datenanalyse oder vielleicht darum, vor einem Computer zu sitzen und professionell beschäftigt auszusehen? Als du nach den Aufgaben fragst, erfährst du, dass dir alle Einzelheiten nach der Erstellung eines Kontos auf einer bestimmten Plattform mitgeteilt werden. Die Registrierung musst du innerhalb einer Stunde abschließen.

An diesem Punkt musst du noch kein endgültiges Urteil fällen. Es reicht festzustellen, dass dir grundlegende

Informationen fehlen, die du für eine Entscheidung brauchst, während bereits erwartet wird, dass du aktiv wirst.

Du kannst dann drei einfache Fragen stellen:

- Welche Tätigkeiten werde ich genau ausführen und unter welchen Bedingungen?
- Welches Unternehmen führt das Bewerbungsverfahren durch, und wo kann ich seine Beteiligung unabhängig bestätigen?
- Warum muss ich die verlangte Formalität erledigen, bevor ich grundlegende Informationen erhalte?

Es geht nicht darum, den Recruiter mit einer grellen Lampe im Gesicht zu verhören. Du kannst diese Fragen höflich und ohne Anschuldigungen stellen. Wichtiger als der Tonfall ist der Inhalt der Antwort. Konkrete Informationen ermöglichen eine weitere Beurteilung. Ausweichende Antworten, Druck oder die wiederholte Weiterleitung zu zusätzlichen Formularen rechtfertigen erhöhte Vorsicht.

Außerdem solltest du zwei Dinge voneinander trennen: Ist die Stelle für dich attraktiv, und ist die Person, die dich kontaktiert, tatsächlich berechtigt, sie anzubieten? Das sind zwei voneinander unabhängige Fragen. Selbst eine hervorragend beschriebene Position bestätigt nicht die Identität des Recruiters. Und die Existenz eines echten Unternehmens garantiert nicht, dass jeder, der seinen Namen verwendet, auch tatsächlich für dieses Unternehmen arbeitet.

Warum Personalisierung funktioniert

Kehren wir zu Marta zurück. Ihr berufliches Profil ist öffentlich zugänglich. Darin stehen Informationen über ihre Erfahrung in der Kundenbetreuung, ihre Kenntnisse bestimmter Programme und ihr Interesse an einer Tätigkeit

im Homeoffice. Wer eine gefälschte Nachricht vorbereitet, kann diese Angaben verwenden, um den Eindruck persönlichen Interesses zu erwecken.

„Ihre Erfahrung in der Betreuung von Geschäftskunden und Ihre Kenntnisse im Umgang mit CRM-Systemen haben unser Interesse geweckt."

Marta versteht diesen Satz als Beweis dafür, dass sich der Recruiter mit ihren Fähigkeiten beschäftigt hat. Tatsächlich bestätigt die Verwendung von Informationen aus einem öffentlichen Profil keineswegs die ehrlichen Absichten des Absenders. Die Personalisierung zeigt lediglich, dass jemand über bestimmte Angaben verfügt.

Das ist ein wichtiger Unterschied, denn moderne Werkzeuge ermöglichen es, zahlreiche scheinbar individuell formulierte Nachrichten zu erstellen, ohne die Bewerber tatsächlich genauer zu analysieren. Sorgfältig gewählte Worte, korrektes Deutsch und treffende Hinweise auf die Berufserfahrung erhöhen die Glaubwürdigkeit einer Kontaktaufnahme. Einen Beweis für ihre Echtheit liefern sie jedoch nicht.

Das bedeutet nicht, dass du deine berufliche Laufbahn aus dem Internet entfernen solltest. Ein berufliches Profil dient schließlich unter anderem dazu, von echten Arbeitgebern gefunden zu werden. Sinnvoll ist es allerdings, zu wissen, welche Informationen öffentlich sichtbar sind und wie sie verwendet werden können. Wenn eine fremde Person den Namen deines früheren Arbeitgebers kennt, braucht sie dafür weder besondere Befugnisse noch einen geheimnisvollen Zugang zur Personalakte. Möglicherweise hat sie einfach dein Profil gelesen.

Auch ein Kompliment ist keine Identitätsprüfung. Der Satz „Sie sind der ideale Kandidat“ kann die Stimmung deutlich verbessern, besonders nach einer Reihe von Absagen. Über die Ehrlichkeit des Absenders sagt er jedoch nichts aus. Ein echter Recruiter kann die Erfahrung eines Bewerbers aufrichtig schätzen. Ein Betrüger kann exakt dieselben Worte verwenden. Um den Unterschied zu erkennen, muss man mehr überprüfen als freundliche Bemerkungen.

Ein erster Filter, der dir keine Chancen nimmt

Bei der alltäglichen Jobsuche ist es unmöglich, zu jeder Anzeige stundenlange Ermittlungen anzustellen. Wenn jede Bewerbung einen Aufwand wie die Prüfung eines internationalen Konzerns erfordern würde, müsste der Kandidat einen Assistenten einstellen, um überhaupt nach Arbeit suchen zu können. Deshalb lohnt es sich, mit einem einfachen Filter zu beginnen.

Versuche vor dem Abschicken einer Bewerbung vier Fragen zu beantworten: Wer bietet die Stelle an? Was sollst du konkret machen? Unter welchen grundlegenden Bedingungen? Und wo kannst du überprüfen, ob dieses Bewerbungsverfahren tatsächlich existiert? Wenn die wesentlichen Informationen verfügbar sind, kannst du das Angebot weiter prüfen. Fehlen sie, solltest du zunächst um eine Erklärung bitten, bevor du sensiblere Daten weitergibst.

Angenommen, du findest ein Stellenangebot für eine Position in der Verwaltung. Der Name des Unternehmens, die Aufgaben, die Beschäftigungsform und die Kontaktmöglichkeiten sind angegeben. Du kannst die offizielle Website des Arbeitgebers selbst aufrufen und im Karrierebereich nachsehen. Wenn die Stelle dort nicht erscheint, beweist das noch keinen Betrug. Manche Unternehmen rekrutieren über Personalagenturen oder

externe Stellenportale. Du kannst dich jedoch über einen unabhängig gefundenen Kontaktweg an das Unternehmen wenden und nach dem Bewerbungsverfahren fragen.

Eine solche Überprüfung ist besonders wertvoll, wenn dich jemand von sich aus kontaktiert und du dich nicht daran erinnern kannst, eine Bewerbung abgeschickt zu haben. Viele echte Bewerbungsverfahren beginnen mit einer Nachricht an eine Person, die im Internet gefunden wurde. Eine unerwartete Kontaktaufnahme ist deshalb für sich genommen kein Alarmsignal. Sie ist allerdings ein guter Anlass, herauszufinden, wer dir eigentlich schreibt.

Wenn du ein großartiges Angebot siehst, dessen Herkunft du nicht überprüfen kannst, musst du es nicht sofort ablehnen. Du kannst die Weitergabe persönlicher Daten vorerst aussetzen, um eine eindeutige Identifizierung des Unternehmens bitten und die Angaben außerhalb des vom Gesprächspartner vorgeschlagenen Kommunikationswegs überprüfen. Genau darin liegt der Unterschied zwischen Vorsicht und dem Verzicht auf jede Gelegenheit.

Echtes Geld, künstliche Eile

Finanzieller Druck verändert die Art, wie wir Risiken beurteilen. Wenn du Ersparnisse und eine sichere Beschäftigung hast, wirkt das Angebot eines sofortigen Arbeitsbeginns möglicherweise einfach interessant. Wenn du vor Monatsende dringend Einkommen brauchst, bekommt dieselbe Nachricht eine völlig andere Bedeutung.

Es wäre sinnlos, so zu tun, als müsse man lediglich einen kühlen Kopf bewahren. Wer sich Sorgen um seine Rechnungen macht, wird nicht automatisch gelassener, nur weil er einen Ratgeber über digitale Sicherheit gelesen hat.

Er braucht eine Vorgehensweise, die auch unter Stress funktioniert.

Eine gute Lösung besteht darin, die Entscheidung, sich für ein Angebot zu interessieren, von der Entscheidung zu trennen, eine bestimmte Handlung auszuführen. Du kannst großes Interesse an einer Stelle haben und gleichzeitig ablehnen, eine Ausweiskopie zu verschicken, bevor die Identität des Unternehmens bestätigt wurde. Du kannst einem Vorstellungsgespräch zustimmen, ohne eine unbekannte Anwendung zu installieren, die umfangreiche Zugriffsrechte verlangt. Ebenso kannst du um Zeit bitten, um dich mit den Bedingungen vertraut zu machen.

Ein solches Verhalten ist keineswegs unprofessionell. Ein ordentliches Bewerbungsverfahren erfordert die Zusammenarbeit beider Seiten. Auch der Bewerber hat das Recht, Fragen zum Ablauf und zum Schutz seiner Daten zu stellen. Wenn dein Gesprächspartner behauptet, jeder Versuch einer Überprüfung würde deine Chancen automatisch zunichtemachen, erfährst du etwas Wichtiges über die Qualität dieses Kontakts.

Marta verschickt schließlich das Ausweisdokument nicht, um das sie bereits vor dem Vorstellungsgespräch gebeten wurde. Stattdessen versucht sie, die Rekrutierung über den offiziellen Kontaktweg des Unternehmens bestätigen zu lassen. In unserer beispielhaften Geschichte stellt sich heraus, dass das Unternehmen überhaupt keine solche Stelle besetzt. Wir wissen nicht, was passiert wäre, wenn Marta das Dokument verschickt hätte. Wir wissen aber, dass sie den Vorgang genau in dem Moment gestoppt hat, als das Risiko größer wurde.

Nicht jede Geschichte endet so eindeutig. Manchmal wird das Unternehmen die Rekrutierung bestätigen. In anderen

Fällen erhältst du keine Antwort, und das Angebot bleibt ungeprüft. Dann musst du mit begrenztem Wissen entscheiden und dir bewusst machen, dass die Aussicht auf einen Arbeitsplatz nicht jede Forderung rechtfertigt.

Die wichtigste Veränderung besteht darin, die Attraktivität eines Angebots nicht länger als Beleg für seine Echtheit zu betrachten. Ein hohes Gehalt ist eine Bedingung des Stellenangebots, kein Beweis für dessen Glaubwürdigkeit. Flexible Arbeitszeiten sind ein Vorteil, kein Sicherheitszertifikat. Die Begeisterung eines Recruiters kann aufrichtig sein, ersetzt aber keine Überprüfung seiner Identität.

Du darfst dich also weiterhin freuen, wenn du deine Traumstelle entdeckst. Du darfst dir sogar für einen Moment die erste Gehaltsüberweisung und deine neue E-Mail-Signatur vorstellen. Bevor du jedoch persönliche Daten weitergibst, solltest du einen einzigen, wenig romantischen Schritt unternehmen: Überprüfe, ob hinter dem Versprechen tatsächlich ein realer Arbeitgeber steht.

Ein perfektes Stellenangebot sollte ein paar vernünftige Fragen aushalten können. Wenn es bereits bei der ersten auseinanderfällt, bestand seine wichtigste Anforderung möglicherweise genau darin, dass du keine Fragen stellst.

Kapitel 2 - Der Recruiter aus dem Nichts oder wie geliehenes Vertrauen funktioniert

Während des Mittagessens vibriert dein Telefon. Auf dem Bildschirm erscheint eine Nachricht von jemandem, der sich als Vertreter eines großen Technologieunternehmens vorstellt. Der Absender schreibt, er habe dein Profil auf einem beruflichen Netzwerk entdeckt und würde dir gern ein Gespräch über eine interessante Position anbieten. Unter der Nachricht stehen sein Vor- und Nachname, die Abteilung sowie eine elegant aussehende Internetadresse. Alles wirkt wie eine professionelle Kontaktaufnahme.

Es gibt nur eine Kleinigkeit. Du hast keine Ahnung, wer dieser Mensch ist.

Daran wäre nichts Ungewöhnliches, wenn der Unternehmensvertreter nicht bereits nach zwei Nachrichten vorschlagen würde, auf einen privaten Messenger zu wechseln, um anschließend ein Verifizierungsformular auszufüllen. Er erklärt, das sei eine standardmäßige Sicherheitsmaßnahme. Einer Sicherheitsmaßnahme kann man nur schwer widersprechen, besonders wenn jemand sie in einem Ton präsentiert, als hätten fünf Juristen und elf Datenschutzexperten sie höchstpersönlich genehmigt.

Dabei lautet die eigentliche Frage: Woher weißt du, dass du tatsächlich mit der Person sprichst, für die sich der Absender ausgibt?

Im ersten Kapitel haben wir uns damit beschäftigt, wie ein attraktives Stellenangebot die Aufmerksamkeit eines Bewerbers gewinnt. Jetzt geht es um einen anderen

Mechanismus. Ein Betrüger kann versuchen, das Vertrauen auszunutzen, das du bereits einem bestimmten Unternehmen, einem bekannten Stellenportal oder dem professionellen Auftreten einer Person entgegenbringst. Er muss sich keinen eigenen guten Ruf aufbauen. Es genügt, sich überzeugend mit dem Ruf eines anderen zu schmücken.

Ein Logo ist kein Identitätsnachweis

Stell dir zwei Nachrichten vor. Die erste stammt von einer unbekannten Person, die dir die Teilnahme an einem nicht näher beschriebenen Projekt anbietet. Die zweite enthält den Namen eines bekannten Unternehmens, sein Logo, die Signatur eines Recruiters und die Information, dass du für ein erstes Gespräch ausgewählt wurdest. Selbst wenn sich die Texte beider Nachrichten ähneln, wird die zweite wahrscheinlich größeres Interesse wecken.

Das liegt daran, dass eine bekannte Marke bestimmte Vorstellungen hervorruft. Das Unternehmen hat eine Geschichte, eine Website, Produkte, Mitarbeiter und einen Ruf. Wenn du seinen Namen siehst, kann ein Teil dieses Vertrauens automatisch auf die Person übergehen, die angeblich in seinem Auftrag handelt.

Im Alltag ist das ein praktischer Mechanismus. Schließlich überprüfen wir nicht jedes Mal von Grund auf die Glaubwürdigkeit jeder Institution, mit der wir Kontakt haben. Das Problem besteht darin, dass man im Internet einen Unternehmensnamen ohne jede Berechtigung in eine Nachricht schreiben kann. Ein Logo lässt sich kopieren, und eine geschäftliche E-Mail-Signatur kann innerhalb weniger Minuten erstellt werden. Das Aussehen einer Nachricht bestätigt ihre Herkunft nicht.

Ein Betrüger kann sich als Recruiter eines bekannten Unternehmens, als Vertreter einer Personalagentur oder als Mitarbeiter einer Stellenplattform ausgeben. Er kann auch eine frei erfundene Firma erschaffen, die dank einer professionellen Website und sorgfältig vorbereiteter Unterlagen echt wirkt. In beiden Fällen verfolgt er dasselbe Ziel: Der Empfänger soll die behauptete Identität als überprüfte Tatsache akzeptieren.

Das bedeutet nicht, dass jede Nachricht mit einem Logo Verdacht erregen sollte. Das Erscheinungsbild eines Unternehmens gehört ganz normal zur beruflichen Kommunikation. Du solltest allerdings daran denken, dass die visuelle Gestaltung und die tatsächliche Identität des Absenders zwei verschiedene Dinge sind.

Wenn sich jemand als Recruiter einer bekannten Marke vorstellt, kannst du überprüfen, ob das Unternehmen tatsächlich für die genannte Position Personal sucht. Du kannst außerdem über einen offiziellen Kontaktweg nachfragen, ob die betreffende Person oder Agentur mit dem Unternehmen zusammenarbeitet. Wichtig ist, dass du deine gesamte Überprüfung nicht ausschließlich auf Informationen stützt, die dir die Person liefert, deren Identität du gerade feststellen möchtest.

Das wäre ungefähr so, als würdest du einen verdächtigen Verkäufer fragen, ob er wirklich kein Betrüger sei, und sein entschiedenes „Natürlich nicht!“ anschließend als ausreichenden Beweis betrachten. Die Höflichkeit deines Gesprächspartners ist durchaus erfreulich, besitzt aber nicht die Beweiskraft einer amtlichen Bescheinigung.

Eine Adresse, die vertraut aussieht

Ein häufiges Element beim Vortäuschen einer Unternehmensidentität ist die Verwendung einer ähnlich aussehenden Internetadresse. Wer eine gefälschte Nachricht vorbereitet, kann eine Domain verwenden, die an den echten Unternehmensnamen erinnert, oder einen Link einfügen, der zu einer Nachahmung der offiziellen Website führt.

Manche Unterschiede fallen sofort auf. Andere übersieht man leicht, besonders auf dem Smartphone, wenn eine lange Adresse nicht vollständig auf den Bildschirm passt. Ein zusätzliches Wort, ein vertauschter Buchstabe oder eine ungewöhnliche Domainendung beweisen noch keinen Betrug, sollten aber überprüft werden.

Eine Adresse, die den Namen eines Unternehmens enthält, muss beispielsweise nicht diesem Unternehmen gehören. Bei der Domain rekrutacja-przykladowafirma.example ist das Wort „przykladowafirma“ kein Beweis dafür, dass die Website tatsächlich dem betreffenden Arbeitgeber gehört. Ebenso kann ein Link, der mit dem Namen einer bekannten Marke beginnt, auf eine völlig andere Website führen, wenn sich die eigentliche Domain an einer anderen Stelle der Adresse befindet.

Du musst kein Spezialist für den Aufbau von Internetadressen werden, um das Risiko zu verringern. Die einfachste Regel lautet: Wenn eine Nachricht von dir eine wichtige Handlung verlangt, suche die offizielle Website des Unternehmens selbst, statt dich ausschließlich auf den zugesandten Link zu verlassen. Du kannst eine bereits bekannte Adresse, ein eigenes Lesezeichen oder eine vertrauenswürdige Quelle verwenden. Anschließend prüfst du, ob das Bewerbungsverfahren und der angegebene Kommunikationsweg bestätigt werden können.

Außerdem solltest du wissen, dass das Vorhängeschloss neben einer Internetadresse nichts über die Ehrlichkeit des Websitebetreibers aussagt. Es bedeutet vor allem, dass die Verbindung verschlüsselt ist und der Browser bestimmte Eigenschaften der Verbindung überprüfen kann. Auch eine gefälschte Website kann eine verschlüsselte Verbindung verwenden. Anders gesagt: Ein geschlossenes Vorhängeschloss bedeutet nicht, dass auf der anderen Seite ein Mensch mit offenem Herzen und makelloser beruflicher Vergangenheit sitzt.

Dieses Detail ist praktisch wichtig. Ein Bewerber sieht möglicherweise das Vorhängeschloss, ein professionell gestaltetes Formular und das Logo des Arbeitgebers und kommt zu dem Schluss, die Website sei sicher. Tatsächlich bestätigt keines dieser Merkmale für sich genommen, dass seine Dokumente beim richtigen Empfänger landen.

Ein echtes Konto, eine falsche Rolle

Wer sich als Recruiter ausgibt, muss dafür nicht immer eine vollständig erfundene Identität erschaffen. Ein Betrüger kann ein berufliches Profil mit einem realistisch wirkenden Werdegang, einem Foto und einer Kontaktliste anlegen. Er kann aber auch ein Konto verwenden, das einem tatsächlichen Nutzer gestohlen wurde. Im zweiten Fall sieht der Empfänger eine authentische Aktivitätsgeschichte, was das Erkennen der Gefahr zusätzlich erschwert.

Deshalb sollte die Überprüfung eines Profils nur ein Bestandteil der Beurteilung sein und nicht deren Abschluss. Eine lange Mitgliedschaft auf der Plattform, zahlreiche Kontakte und ein professionelles Foto können die Glaubwürdigkeit erhöhen. Sie garantieren jedoch weder, dass die aktuelle Nachricht tatsächlich vom Kontoinhaber

verschickt wurde, noch dass dieser berechtigt ist, das genannte Unternehmen zu vertreten.

Stell dir vor, eine Person schreibt dir, deren Profil mehrere Jahre Berufserfahrung in der Branche zeigt. In der Nachricht bietet sie dir eine Stelle bei einem bekannten Unternehmen an. Das Gespräch verläuft natürlich, und der Absender beantwortet Fragen zu den Aufgaben. Erst nach einiger Zeit bittet er darum, Dokumente über ein externes Formular hochzuladen.

In einer solchen Situation kann die bisherige Glaubwürdigkeit des Kontakts dazu führen, dass du spätere Aufforderungen nicht mehr überprüfst. Genau dann entfaltet geliehenes Vertrauen seine größte Wirkung. Man geht davon aus, dass auch der nächste Schritt sicher sein muss, weil mehrere vorherige Elemente korrekt erschienen sind.

Dabei kann jede neue Handlung ganz andere Konsequenzen haben. Ein Vorstellungsgespräch zu vereinbaren ist nicht dasselbe wie ein Ausweisdokument zu verschicken. Die Weitergabe einer Telefonnummer ist nicht mit der Übermittlung eines Autorisierungscodes gleichzusetzen. Die Teilnahme an einer Videokonferenz bedeutet nicht, dass du der Installation zusätzlicher Software zugestimmt hast.

Es lohnt sich deshalb, jede neue Bitte in dem Moment zu beurteilen, in dem sie gestellt wird, selbst wenn der bisherige Kontakt einwandfrei erschien. Vertrauen kann im Verlauf eines Bewerbungsverfahrens wachsen, sollte sich aber nicht automatisch auf jede Forderung erstrecken.

Wir wechseln den Kommunikationskanal, weil es einfacher ist