Wie Cyberkriminelle arglose Jobsucher rekrutieren

Internetbetrüger nutzen oft Konten von Strohleuten, um Geld aus Vorkasse-Überweisungen zu waschen. Wir erklären, wie die Täter mithilfe ahnungsloser Opfer solche Konten eröffnen, welche finanziellen und strafrechtlichen Folgen drohen und wie man sich dagegen schützt.

Von Markus Montz

kompakt

- Internet-Betrüger ködern Arbeitssuchende auf Jobportalen und verleiten sie dazu, bei angeblichen Produkttests „Testkonten“ bei Banken wie N26 zu eröffnen.
- In Wahrheit handelt es sich um echte Girokonten, die auf den Namen der Opfer laufen, während die Täter damit Geld aus Betrugsgeschäften waschen.
- Handeln die Opfer nicht, droht ihnen eine Anklage wegen Geldwäsche und sie haften zivilrechtlich für die Schäden, die Dritten dadurch entstehen.

Die Anzeigen auf einigen Jobportalen klingen verlockend: einfacher Nebenjob von zu Hause, keine Vorkenntnisse und schnelle Einarbeitung. Es reichen ein Computer, ein Smartphone und eine stabile Internetverbindung. Doch was nach leicht verdientem Geld aussieht, entpuppt sich als böse Falle, wenn die zukünftigen Opfer im Auftrag angeblicher Marktforschungsagenturen Konten bei N26 und anderen Banken eröffnen sollen. Während sie selbst nie Zugriff auf diese Konten haben, verschieben die Täter damit Geld aus krummen Geschäften auf eBay Kleinanzeigen oder in Fake-Shops [1, 2] – bis im schlimmsten Fall die Polizei auf der Matte steht.

Eine Leserin von c’t ist auf den Trick hereingefallen. Sie hat

aber nicht nur schnell und überlegt gehandelt und dadurch Schlimmeres verhindert, sondern uns den Fall auch minutiös geschildert. Anhand ihres Beispiels zeigen wir, wie raffiniert die Täter vorgehen, um ihre wahren Absichten zu verschleiern – und wie sie dabei die Unkenntnis selbst vorsichtiger Opfer ausnutzen. Wir erklären außerdem, an welchen Anzeichen man einen kriminellen Hintergrund erkennt und wie man Schaden abwendet, wenn man doch auf den Trick hereingefallen ist.

Unmoralische Angebote

Franziska E. suchte einen Minijob, den sie bequem von zu Hause erledigen konnte. Auf der Website der Jobbörse Indeed stieß sie auf ein passendes Angebot: Für die „Datenerhebung im Homeoffice“ bei Firma A. sollten Bewerber laut Stellenbeschreibung einfache Marktforschungstätigkeiten im Internet erledigen. Vorkenntnisse und eine lange Einweisung seien nicht erforderlich, man brauche lediglich einen Computer, ein Smartphone und eine Internetverbindung.

Mit Jobangeboten für einfache Tätigkeiten aus dem Homeoffice ködern die Täter die Opfer, die später die Bankkonten für sie eröffnen.

Zur Sicherheit googelte Franziska E. den Firmennamen und stieß auf ein norddeutsches Unternehmen, das mit SEO-Optimierung und Social-Media-Marketing warb. Das Impressum wirkte vollständig, die angegebene Adresse war auf Google Maps zu finden. Auf Franziska E. wirkte das seriös, also klickte sie auf „Schnellbewerbung“. Dabei füllen Nutzer auf Stellenbörsen wie Indeed einige Felder aus; die Börse leitet den Inhalt dann weiter.

Kurz darauf meldete sich ein angeblicher Vertreter von Firma A. per Mail und wollte unter anderem wissen, ob Franziska E. Facebook, Twitter, Instagram und N26 kenne. Die ersten drei Fragen bejahte sie, bei der Digitalbank N26 musste sie passen. Für die Firma schien das aber kein Problem zu sein: Franziska E. bekam umgehend einen ersten Probeauftrag, der bereits mit 50 Euro vergütet werden sollte. Der Arbeitsvertrag würde nach den ersten Einsätzen folgen. Anschließend einigte man sich auf einen ersten Arbeitstermin. Die Firma A. schickte Franziska E. einen Link zu einem Livechat auf der Firmenhomepage, bei dem sie sich zum vereinbarten Zeitpunkt melden sollte. Franziska E. stutzte zwar kurz, weil der Link zu einer anderen Homepage als der gegoogelten führte, hielt diese dann aber für eine Mitarbeiterseite.

Warnsignale

Die Masche ist in diesem frühen Stadium schwer zu erkennen. Ein Indiz ist aber das Schema der Stellenausschreibungen: Es handelt sich stets um „einfache“ Tätigkeiten, die keine Vorerfahrung erfordern und vollständig digital im Homeoffice stattfinden sollen. Bei Franziska E. hieß das Ganze „Homeoffice/Datenerhebung“, andere Beispiele sind „Kundendienstmitarbeiter/in“ oder „Financial Controller“. Meist geht es um Mini- oder Teilzeitjobs. Stutzig machen sollte außerdem, wenn das Unternehmen beim Arbeitnehmer ein Smartphone oder Tablet sowie eine funktionierende und stabile Internetverbindung voraussetzt.

Prüfen Sie daher stets die angegebene Homepage, so wie es auch Franziska E. tat. Beginnen Sie mit dem Impressum: Gewerbliche Internetauftritte müssen ihre Anschrift, Umsatzsteuer-ID und, je nach Unternehmensform, Handelsregisternummer vermerken. Letztere und die Anschrift gleichen Sie auf handelsregister.de ab (ct.de/y6cu). Betrüger setzen allerdings häufig Links zu seriösen Unternehmen oder kopieren Namen und Adressen von anderen Homepages. Auch eine professionell aussehende Fake-Homepage inklusive Livechat kann man mit Baukästen in wenigen Stunden zusammenklicken.

Googeln Sie zusätzlich den Unternehmensnamen und schauen Sie, ob es weitere Unternehmen mit ähnlichen Namen gibt: Betrüger arbeiten gerne mit leicht angepassten Bezeichnungen und URLs, die seriösen Angeboten ähneln. Manchmal ahmen sie sogar das Design der Homepage nach. Auch die Homepage selbst liefert mögliche Hinweise: Wollen die Unternehmensbeschreibung und die angebotene Tätigkeit nicht recht zueinander passen, seien Sie skeptisch.

Erkundigen Sie sich noch vor der Bewerbung beim Unternehmen nach Inhalten der Tätigkeit – mit einer Bewerbung fließen ja bereits Ihre persönlichen Daten. Fragen Sie bei allgemeinen Angaben wie „Marktforschung“, um welche Branchen es geht und

ob das Unternehmen Referenzen besitzt. Ein seriöses Unternehmen antwortet sachlich und konkret, andernfalls brechen Sie den Kontakt ab.

Haben Sie einen vollständig online durchgeführten Bewerbungsprozess begonnen, sollten Sie alle unklaren Namen und Begriffe recherchieren. Geht es darum, Marktforschung oder Produkttests zu Finanzinstituten oder Identifikationsverfahren durchzuführen, brechen Sie ab. Abbrechen sollten Sie auch, wenn man im Bewerbungsverlauf eine Ausweiskopie von Ihnen haben will: So etwas ist auf keinen Fall seriös und kann Ihnen weitere Schwierigkeiten bringen [1].

Kommt ohne echtes Auswahlverfahren bereits eine Zusage, ist das ebenfalls kein gutes Zeichen. Manchmal versuchen die Betrüger, zusätzlich durch einen Arbeitsvertrag Vertrauen zu schaffen. Doch auch der kann gefälscht sein. Probeaufträge, bei denen der Arbeitsvertrag lediglich in Aussicht steht, sind noch verdächtiger. Ansonsten gilt dasselbe wie vor der Bewerbung: Gibt es Ungereimtheiten, Verdachtsmomente oder kommt Ihr Gegenüber erst nach der Zusage mit der eigentlichen Jobbeschreibung heraus, brechen Sie ab. Das gilt auch für Jobs, bei denen man Sie lediglich über Mail, Livechats oder Messenger wie WhatsApp begleiten will, aber ein telefonisch erreichbarer Ansprechpartner fehlt. Melden Sie solche Anzeigen bei der Jobbörse, damit sie diesen nachgeht.

Ein unseriöser Job

Wie vereinbart meldete sich Franziska E. pünktlich im Livechat an. Der Operator erklärte ihr nun erstmals ihre Aufgabe: Man teste „in erster Linie den Live-Support und Identifikationsservice von Banken“ in deren Auftrag. Dazu müsse sie sich mit den Zugangsdaten, die er ihr übermitteln würde, in der App einer Bank registrieren und „eine Videoverifikation durchführen“. Sie würde aber lediglich ein Testkonto eröffnen, das anschließend wieder gelöscht werde, log der Operator weiter.

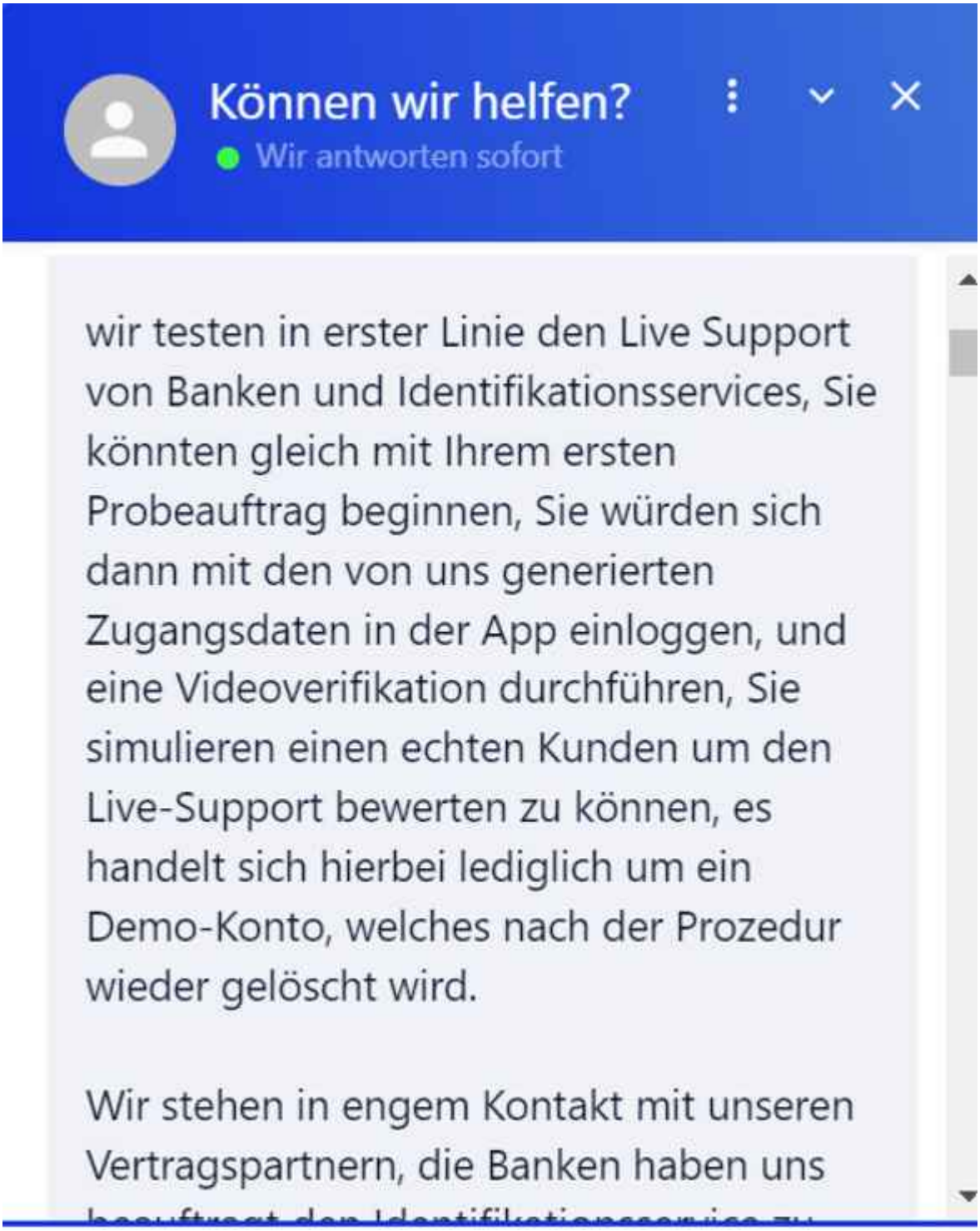
Anschließend bat er Franziska E., die Daten aus der Bewerbung abzugleichen und eventuelle Zweitnamen entsprechend ihrem Personalausweis anzugeben. Den solle sie überdies bereithalten. Der Auftrag sei „bei der N26 Bank“, sie solle aber nichts von einem Job oder einer Marktforschung erwähnen, „da der Mitarbeiter sich so verhalten soll, als wären Sie ein echter Kunde“. Frage man sie nach dem Grund der Verifizierung, solle sie sagen, dass es sich um „ein Girokonto bei der N26 Bank“ handele. Während des Probeauftrags müsse sie im Livechat bleiben, wo man ihr wichtige Daten und Links zusenden würde. Außerdem solle sie sich Notizen zum Mitarbeiter, dem Ablauf und der Nutzerführung in der App machen.

Nachdem Franziska E. die N26-App installiert hatte, bekam sie vom Operator Zugangsdaten in Form einer Mailadresse, einer Handynummer und eines Passworts zugesandt, mit denen sie sich registrieren sollte. Diese Daten solle sie auf Nachfrage auch dem Mitarbeiter im Videochat mitteilen, so der Operator. Alle anderen Felder füllte Franziska E. mit ihren persönlichen Daten aus. Zum Abschluss sandte ihr der Operator den Link, mit dem sie die Mailadresse bestätigen sollte – wie von N26 vorgegeben auf demselben Gerät, auf dem sie sich registriert hatte.

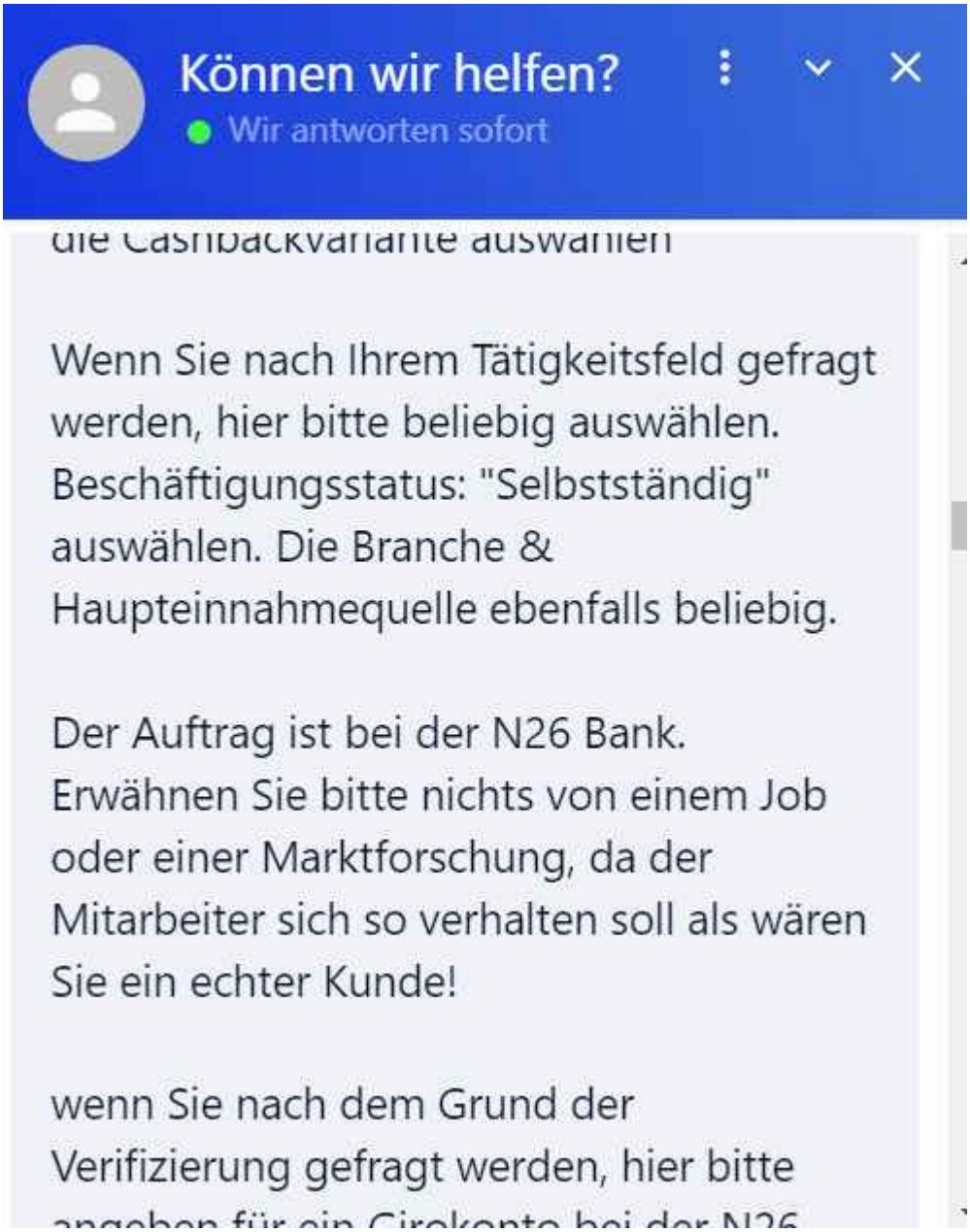
Es folgte die eigentliche Kontoeröffnung: Als Kontotyp gab der Operator das kostenlose Business-Modell „Standard“ mit virtueller Karte vor, das nur auf Kundenwunsch eine Plastikkarte umfasst. Für den erneuten Login schickte der Operator Franziska E. über den Chat den erforderlichen „SMS Code“, der zuvor auf seinem Handy landete. Danach absolvierte sie das Video-Ident-Verfahren. Die per Mail versandte sechsstellige Bestätigungs-TAN zum Abschluss des Video-Idents bekam sie gleichfalls vom Operator des Livechats – außerdem gab er ihr den vierstelligen „Bestätigungscode“ vor, mit dem man Änderungen im Konto bestätigt.

Zum Abschluss sollte Franziska E. ihre Bewertung abgeben, anschließend informierte man sie über ihre Einstellung – und

schlug gleich einen nächsten Termin für den Folgetag vor. Das Konto werde man im Übrigen nach spätestens 72 Stunden schließen. Nun wurde Franziska E. misstrauisch und bat um die Zugangsdaten, um selbst Hand anlegen zu können. Außerdem forderte sie den Operator auf, ihre persönlichen Daten zu löschen.



Geschickt briefen die Täter ihre Opfer im Chat oder Messenger. Die wiederum merken oft nichts von dem kriminellen Hintergrund.


Können wir helfen?
Wir antworten sofort
die Cashbackvariante auswählen
Wenn Sie nach Ihrem Tätigkeitsfeld gefragt werden, hier bitte beliebig auswählen. Beschäftigungsstatus: "Selbstständig" auswählen. Die Branche & Haupteinnahmequelle ebenfalls beliebig.
Der Auftrag ist bei der N26 Bank. Erwähnen Sie bitte nichts von einem Job oder einer Marktforschung, da der Mitarbeiter sich so verhalten soll als wären Sie ein echter Kunde!
wenn Sie nach dem Grund der Verifizierung gefragt werden, hier bitte

Straf- und zivilrechte Aspekte

Franziska E.s Bedenken waren berechtigt: Sie hatte den Tätern geholfen, ein echtes N26-Girokonto zu eröffnen. Obwohl es auf ihren Namen und ihre Identität lief, hatte sie keinen Zugriff auf das Konto – den besaßen nur die Täter, während sie nicht einmal die IBAN kannte. Geschickt hatten die Täter das Sicherheitsverfahren von N26 ausgetrickst, indem sie Franziska

E. überall dort vorschickten, wo N26 Identitäten prüft.

Unser Rat ist daher derselbe wie im Bewerbungsprozess: Brechen Sie spätestens dann den Kontakt ab, wenn Sie bei einer vollkommen unbekannten Agentur Marktforschung oder einen Produkttest für eine Bank durchführen sollen. Das gilt umso mehr, wenn Sie dabei ein Konto eröffnen; insbesondere, aber nicht nur bei N26. Wir haben bereits von ähnlichen Versuchen bei anderen Banken gehört, auch solchen im EU-Ausland.

Stoppen Sie als Betroffener den Prozess nicht, können Sie sowohl straf- als auch zivilrechtlich belangt werden. Die Täter nutzen die Konten in aller Regel, um darüber Geld aus Betrugsgeschäften zu waschen. Im einfachsten Fall eröffnen oder kapern sie Nutzerkonten auf eBay Kleinanzeigen, stellen dort Verkaufsangebote ein und verleiten Interessenten dazu, ihnen Geld auf das für die Betrüger eröffnete Konto zu überweisen.

Während diese Interessenten nie die Ware bekommen, überweisen die Täter das Geld auf Konten im Ausland weiter. Fliegt der Schwindel auf, wenden sich die Strafverfolgungsbehörden zunächst unter dem Verdacht der Geldwäsche an den Kontoinhaber. Damit nicht genug, können die Opfer zivilrechtliche Ansprüche gegen ihn geltend machen. Dabei geht es schnell um viele tausend Euro [1].

Schwachstelle N26

N26 ist im Vergleich zu anderen deutschen Banken – auch anderen Digital- sowie Direktbanken – relativ häufig von Identitätsmissbrauch betroffen. Aus Sicht vieler Experten haben die internen Strukturen der Bank zur Abwehr krimineller Aktivität nicht Schritt mit dem Kundenwachstum gehalten. Das Bundesamt für Finanzdienstleistungsaufsicht (Bafin) hat die Bank daher im Mai 2019 erstmals öffentlich wegen Mängeln in der Prävention von Geldwäsche und Terrorismusfinanzierung gerügt und mit einer Geldbuße belegt. Zwei Jahre später bekam

N26 zur Kontrolle zusätzlich einen Sonderbeauftragten der Bafin ins Haus geschickt, seit November 2021 darf die Bank maximal 50.000 Neukunden im Monat aufnehmen.

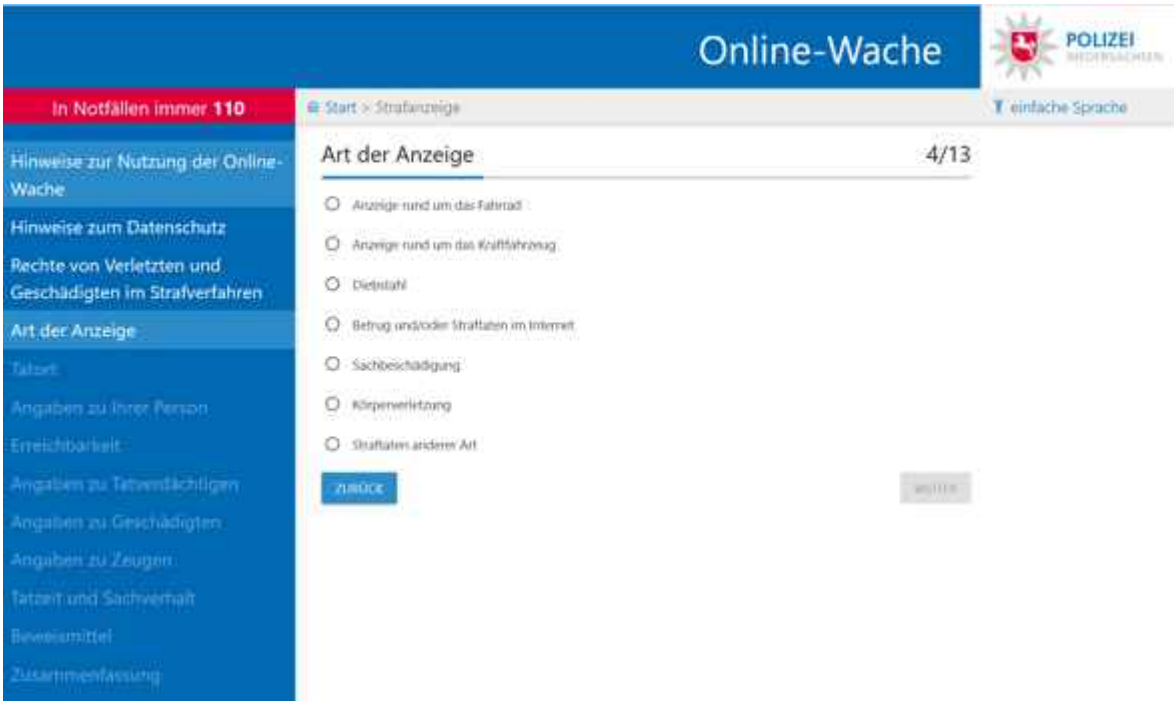
c’t hat N26 nach einer direkten Kontaktmöglichkeit für Opfer der Masche gefragt. N26 antwortete, dass man sich in solchen Fällen „grundsätzlich zunächst an die Strafverfolgungsbehörden wenden“ solle; N26 kooperiere dann mit diesen. Gleichzeitig nehme man Meldungen von potenziell betrügerischen Konten „außerordentlich ernst“ und folge dabei strengen regulatorischen Vorgaben. Außerdem überarbeite man „im Austausch mit den Behörden laufend [die] Prozesse zur Bearbeitung von Hinweisen Dritter“ und behandle Hinweise auf potenzielle Betrugsfälle „mit hoher Priorität“. Gemessen an den wenig hilfreichen und unstrukturiert wirkenden Reaktionen, die Franziska E. auf ihre Kontaktversuche erhielt, scheint N26 die Überarbeitung allerdings noch nicht gänzlich abgeschlossen zu haben.

Schadensbegrenzung

Franziska E. wandte sich direkt an N26, um Schlimmeres zu verhindern. Dort stand ihr aber lediglich ein Livechat zur Verfügung. Ob es bei N26 ein Konto auf ihren Namen und ihre Anschrift gebe, wollte sie dort wissen; sie sei Opfer eines Identitätsdiebstahls geworden. Mitarbeiter „S.“ riet ihr knapp, sich an die Polizei zu wenden. Erst als Franziska E. im zweiten Anlauf konkret darauf hinwies, dass mit ihrer Identität und einer fiktiven Mailadresse ein Girokonto eröffnet worden sei, bat Mitarbeiter „V.“ sie um eben jene Mailadresse. Weitere Auskünfte bekam sie nicht.

Bei der Polizei ihres Wohnortes ließ man Franziska E. auf Nachfrage zunächst wissen, dass man nichts machen könne, solange ihr kein Schaden entstanden sei. Daraufhin wandte sie sich an heise online und c’t. Auf unseren Rat hin fuhr Franziska E. unverzüglich zur nächsten Polizeiwache und erstattete wegen des Identitätsdiebstahls und -missbrauchs

Anzeige. Fünf Tage darauf beschwerten sich die Täter in einer letzten Mail, dass sie entgegen der „Richtlinien“ Kontakt zur Bank aufgenommen habe – und bestätigten damit indirekt, dass N26 das Konto geschlossen hatte.



Nutzen Sie am besten die Onlinewache, um Anzeige zu erstatten: Sie können Screenshots und Dateien hochladen und bekommen am Ende eine Vorgangsnummer, genau wie auf dem Revier.
Haben Sie festgestellt, dass Sie selbst oder jemand anderes Opfer dieser Masche geworden sein könnte, handeln Sie schnell. Andernfalls drohen besagte straf- und zivilrechtliche Konsequenzen. Sichern Sie alle Daten wie Telefonnummern und Mailadressen sowie alle Chatverläufe und Mails. Machen Sie Screenshots von Stellenanzeigen, Homepages und Livechats. Mit diesem Material bringen Sie den Identitätsdiebstahl zur Anzeige.

Sie haben das Recht auf eine Anzeige, und zwar auch dann, wenn ein materieller Schaden noch nicht eingetreten ist. Die Behörden veranlassen dann, dass die Bank das Konto schließt. Sie müssen nicht einmal eine Polizeidienststelle aufsuchen, sondern können die Onlinewache Ihres Bundeslandes nutzen; Ihre Rechte können Sie in der sogenannten „Opferfibel“ nachlesen (Links unter ct.de/y6cu). Ab dem Zeitpunkt der Anzeige sind

sie vor Ansprüchen dritter Geschädigter sowie Strafverfolgung weitgehend geschützt.

Geben Sie zu Protokoll, dass Sie über den Ausgang des Verfahrens informiert werden möchten, und stellen Sie außerdem Strafantrag. Normalerweise bietet die Polizei Ihnen beides an. Sie können dies aber noch bis zu drei Monate nach der Anzeige tun. Zum einen informieren Sie Polizei und Staatsanwaltschaft dann über den weiteren Verlauf und Abschluss des Verfahrens. Zum anderen kann ein Rechtsanwalt über den Strafantrag optional Akteneinsicht verlangen.

Zusätzlich sollten Sie Mailadressen beim Mailprovider (beispielsweise Hotmail) und die Stellenanzeige bei der Jobbörse melden. Sie können außerdem versuchen, über eine WhoIs-Abfrage (bei DE-Homepages über die Denic, ct.de/y6cu) den Nameserver/Provider einer Website herauszufinden und sie diesem anzuzeigen. Auch wenn die Täter wahrscheinlich schnell eine neue Homepage und Stellenanzeige online haben, kann man ihnen so zumindest ein paar Steine in den Weg legen. *(mon@ct.de)*

1. Literatur
2. Markus Montz, Perfektes Schauspiel, Wie Betrüger mit Fakt und Fiktion Gebrauchtkäufer abzocken, c’t 21/2022, S. 132
3. Nick Akinci, Niemals ausgeliefert, Fake-Shops erkennen und vermeiden, c’t 2/2023, S. 150

Handelsregister, Onlinewache, Opferfibel: ct.de/y6cu