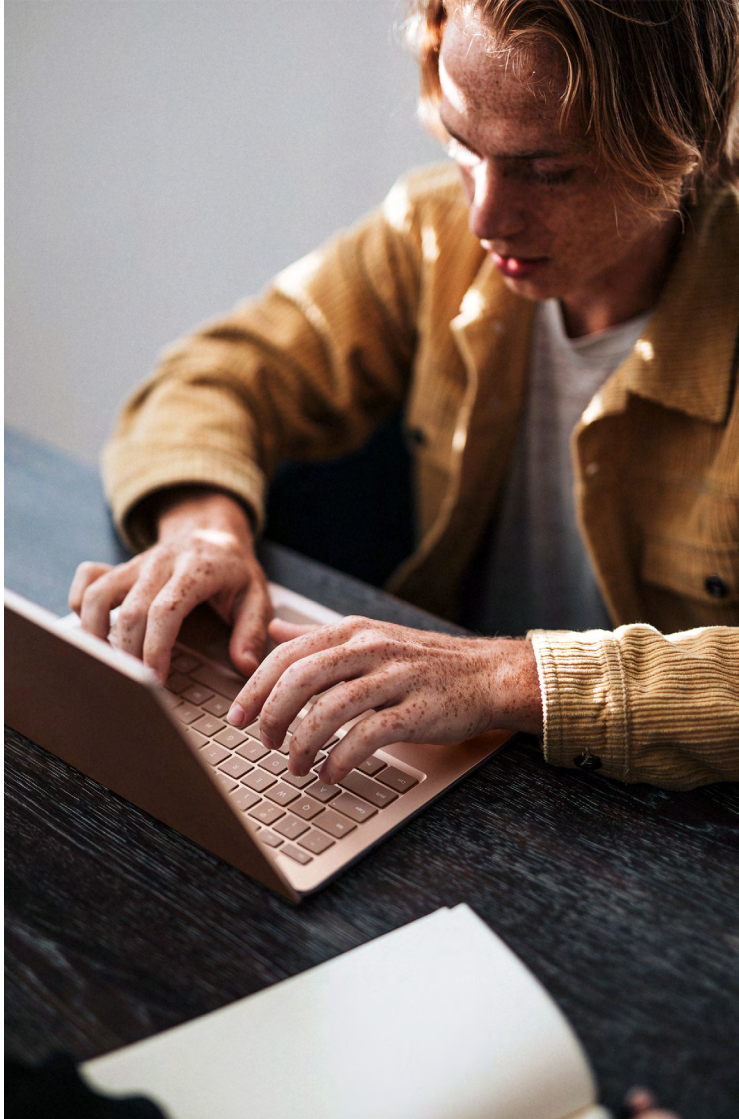
N26

Der N26 Ratgeber für sicheres Online-Banking



So schützt du dein Geld beim Online-Banking

COVID-19 hat dafür gesorgt, dass wir uns alle an eine neue Normalität gewöhnen müssen. Für viele Menschen weltweit bedeutet das auch, mit neuen Technologien und Innovationen Bekanntschaft zu machen. Kunden entscheiden sich zunehmend für digitale Lösungen: kontaktlose Zahlungen statt Bargeld und Online-Shopping statt Shopping Mall. Dementsprechend überrascht es auch wenig, dass viele Menschen auf digitales Banking setzen, um den Weg in die Filiale zu vermeiden. Tatsächlich rechnet man damit, dass bis 2021 knapp 39 % der Weltbevölkerung über das Internet auf Bankdienste zugreifen werden.

Jetzt fragst du dich vielleicht: „Wer schützt eigentlich mein Geld?"

Als deutsches Institut mit Vollbanklizenz unterliegt N26 denselben Vorschriften wie traditionelle Banken. Deshalb investieren wir massiv in die Sicherheit unserer Online-Banking-Plattform. Jenseits dessen, was hinter den Kulissen bei N26 vor sich geht, kannst du selbst Sicherheitsmaßnahmen ergreifen, um dich vor Cyberkriminalität zu schützen. In diesem Ratgeber haben wir unsere Empfehlungen und Tipps zusammengefasst.

Die Bedeutung von Sicherheit in der digitalen Welt

Alle Banken müssen sich mit Cyberkriminalität auseinandersetzen. Und da N26 sich seit einigen Jahren zunehmender Beliebtheit erfreut, bedeutet das auch für uns, dass wir häufiger ins Visier von Kriminellen geraten. Wie jede andere lizenzierte Bank ist N26 an strenge Vorgaben in den Bereichen Sicherheit, Rechtskonformität und Prävention von Wirtschaftskriminalität gebunden.

In einer digitalen Umgebung nimmt Sicherheit einen noch höheren Stellenwert ein. Betrüger sind stets auf der Suche nach neuen Möglichkeiten, ihre Masche weiterzuentwickeln und nichts ahnende Kunden genau dann zu treffen, wenn diese am wenigsten darauf vorbereitet sind. Sie gehen dabei schnell, innovativ und äußerst kreativ vor: So nahm etwa die Anzahl der Phishing-Attacken mit Coronavirus-Bezug im März 2020 – dem ersten Monat der COVID-19-Pandemie – weltweit um 667 % zu.[1]

Genau aus diesem Grund optimieren wir bei N26 kontinuierlich unsere Sicherheitsvorkehrungen. Der Schutz deines Geldes hat für uns höchste Priorität. Um diesen zu gewährleisten, überprüfen wir fortlaufend, dass unsere Maßnahmen mit den Entwicklungen der Branche Schritt halten.

[1] Forschungsergebnisse von Barracuda Sentinel – Threat Spotlight: Coronavirus-Related Phishing

5 häufige Gefahren beim Online-Banking

Wir arbeiten konsequent daran, unsere Banking-Plattform bei N26 bestmöglich abzusichern. Doch die Angreifer setzen oft direkt bei den Kunden an. Indem du dich informierst und stets aufmerksam bist, kannst du dich selbst vor solchen Maschen schützen. Hier findest du eine Liste der gängigsten Gefahren, denen du unter Umständen beim Online-Banking ausgesetzt bist:

1. Beim **Phishing** versucht ein Cyberkrimineller, an die persönlichen Daten seiner Opfer zu gelangen und diese für Betrugszwecke zu verwenden. Dazu zählen etwa Anmeldeinformationen, Konto- und Kreditkartendaten und weitere Angaben, die der Täter zum Identitätsdiebstahl nutzen kann. Die Kriminellen setzen häufig auf Drohungen, um ihre Zielpersonen einzuschüchtern und zu manipulieren, damit diese den gestellten Forderungen nachgeben. Gewöhnlich erfolgen solche Phishingversuche über E-Mails oder SMS-Nachrichten und normalerweise enthalten sie Links zu betrügerischen Webseiten.

2. **Social-Engineering**-Taktiken sind in der Regel subtiler und zielen darauf ab, die emotionale Verfassung einer Person zu manipulieren. Die Betrüger machen sich eine Reihe verschiedener Techniken zunutze, um Vertrauen zu ihren Opfern aufzubauen und ihnen Informationen zu entlocken. Unter Umständen setzen sie dabei auf vorgeblich dringende Probleme, um Zielpersonen zu unüberlegten Reaktionen zu drängen.

3

Als **Einstellungsbetrug** (engl. “recruitment scams”) bezeichnet man das Schalten von gefälschten Jobangeboten, um persönliche Daten von gutgläubigen Personen zu sammeln. Möglicherweise werden die Bewerber unter Vorspiegelung falscher Tatsachen sogar angewiesen, Konten zu eröffnen und dabei den Grund für die Kontoeröffnung zu verschleiern. Das ermöglicht es den Betrügern, Bankkonten im Namen ihrer Opfer zu eröffnen und auf diese zuzugreifen – die scheinbar seriösen Stellenangebote sind dabei natürlich nur eine Fassade.

4

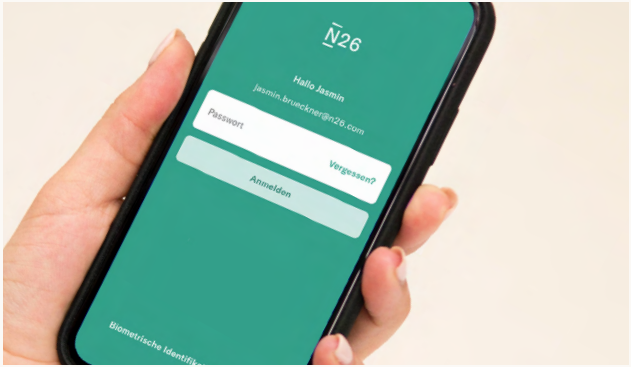
Marktplatzbetrug können Cyberkriminelle begehen, nachdem sie unter Einsatz gestohlener Identitäten Bankkonten eröffnet und/oder durch Phishing die Kontrolle über die Konten ihrer Opfer erlangt haben. Die Betrüger nutzen diese gekaperten Konten, um Fake-Profile auf Online-Marktplätzen anzulegen. So bringen sie nichts ahnende Käufer dazu, ihnen Geld für nicht vorhandene Produkte, gefälschte Immobilienangebote, Gebrauchtwagen und andere fiktive Artikel zu überweisen.

5

Bei einem **Datendiebstahl** nehmen Cyberkriminelle große Unternehmen ins Visier, um empfindliche Kundendaten wie Namen, Adressen, Versicherungsangaben, Kreditkartendaten, Transaktionsdaten und so weiter abzugreifen. Anstatt sich mit den Sicherheitssystemen einer Bank abzumühen, entscheiden sich die Verbrecher häufig für Unternehmen, bei denen Menschen oft etwas einkaufen – von Fluggesellschaften über Einzelhändler bis hin zu Streaming-Diensten. Die gestohlenen Daten ermöglichen den Zugriff auf private Bankkonten, welche wiederum für Einkäufe und/oder andere betrügerische Aktivitäten genutzt werden.

Wichtige Sicherheitsmaßnahmen zum Schutz deines digitalen Bankkontos

Wir bei N26 haben zusätzliche Sicherheitsmaßnahmen eingeführt, um ein sicheres Banking-Erlebnis für unsere Kunden zu schaffen. Im Folgenden stellen wir dir einige der wichtigsten Sicherheitsfeatures zum Schutz deines digitalen Bankkontos vor:



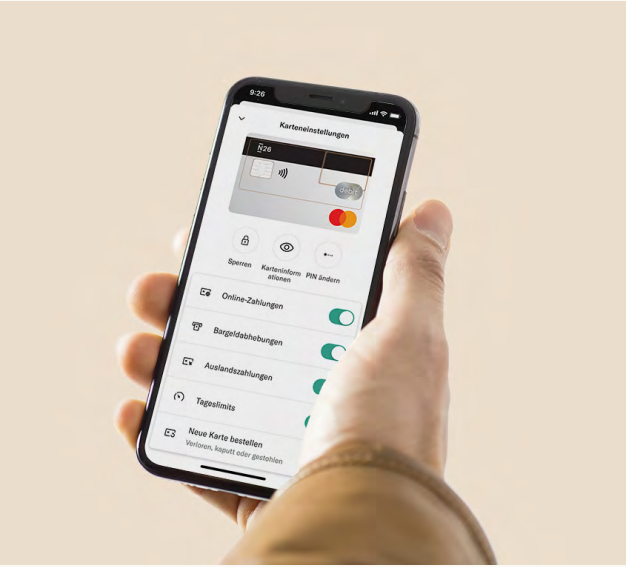
Ein einziges gekoppeltes Gerät: Der Zugriff auf dein N26 Konto ist nur über dein gekoppeltes Smartphone möglich – so kannst nur du auf dein Geld zugreifen.

Zwei-Faktor-Authentifizierung: Du brauchst zum Einloggen in dein N26 Konto nicht nur dein gekoppeltes Gerät, sondern musst zudem dein Passwort eingeben oder de biometrische Authentifizierung verwenden. Auf diese Weise überprüfen wir, dass du der rechtmäßige Kontoinhaber bist.

Fingerabdruck- und Gesichtserkennung: Biometrische Daten tragen dazu bei, dass nur du dich in dein Konto einloggen kannst. Sorgen über ein gestohlenes Passwort gehören damit der Vergangenheit an.

Push-Nachrichten in Echtzeit: Behalte deine Transaktionen dank Push-Nachrichten in Echtzeit stets im Blick. Diese Funktion bietet dir die Möglichkeit, jede Transaktion sofort auf deinem Smartphone zu überprüfen.

Sperren deiner Karte per App: Solltest du jemals den Verdacht haben, dass jemand an deine Kartendaten gelangt ist, kannst du deine Karte sofort sperren oder deinen PIN-Code ändern – mit nur wenigen Klicks in der N26 App.



3D Secure: Dieser Authentifizierungsschritt erfordert, dass du Online-Zahlungen vor deren Verarbeitung über deine N26 App autorisiert. So merkst du direkt, wenn jemand versucht, deine Karte für Online-Käufe zu verwenden und kannst es verhindern.

Standortverfolgung: Du kannst deiner N26 App erlauben, deinen Standort zu verfolgen – denn so können unsere Systeme erkennen, ob deine Karte an einem Ort verwendet wird, an dem du dich gar nicht befindest. Außerdem können die Systeme so auch weitere potenziell verdächtige Nutzungsmuster erkennen.

Identitätsverifizierung: Als regulierte Bank arbeitet N26 mit ebenfalls regulierten Partnern zusammen, um jeden unserer Kunden vor der Eröffnung eines Kontos zu verifizieren. Auf diese Weise ist es uns möglich, die Kundenintegrität zu gewährleisten.

Intelligente Zahlungssperren: Du hast in deiner App die volle Kontrolle darüber, wie deine Karte verwendet werden kann. Aktiviere und deaktiviere mit wenigen Klicks Online-Zahlungen, Bargeldabhebungen oder Zahlungen im Ausland.

Sicheres Postfach: Wenn wir dich über wichtige Neuigkeiten informieren müssen, schicken wir dir eine Nachricht an das In-App-Postfach “Nachrichten von N26”. So sorgen wir dafür, dass nur du sie lesen und beantworten kannst.

10 einfache Tipps für deine Sicherheit im Netz

Ob beim Shopping, Banking oder Verwalten deines Postfachs: Hier findest du einige Tipps, wie du dich und deine Daten im digitalen Raum schützen kannst.

Kaufe nur auf vertrauenswürdigen Webseiten bekannter Händler ein.

Nutze starke Passwörter mit Buchstaben, Zahlen sowie Symbolen – und verwende niemals dasselbe Passwort für mehrere Konten.

Überprüfe die Sicherheit von Webseiten – halte Ausschau nach dem Schloss neben der URL. Klicke darauf, um dir die Zertifikatsinformationen anzusehen.

Veröffentliche in den sozialen Medien unter keinen Umständen sensible persönliche Informationen.

Aktualisiere stets deine N26 App und das Betriebssystem deines Smartphones, um immer die aktuellsten Sicherheitsfeatures zu haben.

Nimm dich vor Angeboten in Acht, die zu gut sind, um wahr zu sein – oft handelt es sich um Betrug.

Sei vorsichtig, wenn du öffentliche oder geteilte WLAN-Verbindungen nutzt – entscheide dich stets für sichere WPA2- anstatt WEP-Netzwerke und verwende wann immer möglich ein VPN.

Nutze E-Mail-Provider wie Gmail und Yahoo!, die über Sicherheitsmaßnahmen verfügen, Spamfilter einsetzen und Zwei-Faktor-Authentifizierung anbieten.

Verwende zum Einloggen den Fingerabdrucksensor oder die Gesichtserkennung.

Aktiviere die Standortverfolgung in deiner N26 App, damit wir verdächtige Transaktionen erkennen können, die möglicherweise nicht du getätigt hast.

So erkennst du eine betrügerische Nachricht

Du bist nicht sicher, ob eine Nachricht oder E-Mail, die angeblich dein Bankkonto betrifft, echt ist? Dann wende dich bitte immer zuerst an unseren Kundenservice, bevor du irgendetwas unternimmst. Folgende Punkte sind Anzeichen für eine betrügerische oder verdächtige Nachricht:

Dringlichkeit: Lass dich nicht dazu verleiten, sofort tätig zu werden. Halte kurz inne und überprüfe, ob du etwas Ungewöhnliches feststellen kannst. Cyberkriminelle setzen oft auf vorgeblich dringliche Meldungen, um deinen Entscheidungsprozess zu beeinflussen. Denk daran: Kein seriöses Unternehmen wird dich jemals dazu nötigen, sofort zu handeln.

Kleinere Fehler und Ungereimtheiten: Achte auf nicht personalisierte Begrüßungen sowie Rechtschreib- und Formatierungsfehler. Das sind Anzeichen für einen potenziellen Phishing-Versuch.

Fehlerhafte URLs: Überprüfe die URL der entsprechenden Webseite, bevor du auf einen Link klickst. Bewege den Cursor über den Link, um die Zieladresse einzusehen. Betrüger verwenden oft leichte Abwandlungen der offiziellen URLs – achte daher genau auf Zeichen, die sonst nicht Teil der Adresse sind.

Unsichere Webseiten: Sei stets auf der Hut, wenn du es mit Webseiten zu tun hast, die dich weiterleiten. Halte Ausschau nach dem Schloss-Symbol. Dieses zeigt an, dass die Verbindung sicher ist. Klicke darauf und überprüfe die Informationen der Webseite. So erkennst du, ob das SSL-Zertifikat (“Secure Sockets Layer”) gültig ist und für wen es ausgestellt wurde.

Datenanfragen: Wenn du nach persönlichen Daten gefragt wirst, solltest du besonders wachsam sein. Denk daran, dass N26 dich nie außerhalb einer sicheren Umgebung nach sensiblen Informationen fragen wird.

Inside N26: So gehen digitale Banken gegen Cyberkriminalität vor

Die Sicherheits-, Financial Crime und Fraud Prevention Abteilungen von N26 bestehen aus erfahrenen Spezialisten, die unsere Kunden vor Finanzkriminalität schützen. Sie haben die häufigsten Fragen dazu beantwortet, wie N26 als digitale Bank mit Betrug umgeht.

Was müssen Banken tun, um Betrug zu verhindern?

Alle regulierten Banken sind verpflichtet, die regulatorischen Anforderungen zu erfüllen und verdächtiges Verhalten auf ihrer Plattform den Behörden zu melden. N26 ist da keine Ausnahme und muss diese gesetzlichen Verpflichtungen wie jede andere Bank auch erfüllen.

Sind digitale Banken weniger sicher als traditionelle?

Digitale Banken können verschiedene Lizenzen nutzen. Das bedeutet unter Umständen, dass sie nicht alle denselben regulatorischen Standards in den Bereichen Sicherheit und Betrugsprävention unterliegen. Dies gilt insbesondere für Fintech- und E-Geld-Lizenzen. Als deutsches Institut mit Vollbanklizenz unterliegt N26 jedoch denselben Vorschriften wie alle traditionellen Banken. Diese Tatsache und unser Schwerpunkt auf Sicherheit machen uns mindestens genauso sicher wie traditionelle Banken.

Wie erkennt und überwacht N26 Betrugsversuche?

N26 verfügt über ein Spezialteam, das sich auf die Überwachung und Identifizierung verdächtiger Transaktionen auf unserer Plattform konzentriert. Mithilfe fortschrittlicher statistischer Modelle und Algorithmen sowie Verhaltensanalyse sorgt unser Team dafür, dass dein Geld stets in sicheren Händen ist.

Warum verraten Banken nur so wenig darüber, wie sie mit Betrug umgehen?

Dafür gibt es zwei Gründe. Erstens: Da Banken strengen Datenschutz- und Bankgeheimnisgesetzen unterliegen, dürfen sie

die Einzelheiten eines Falles nur den Strafverfolgungsbehörden mitteilen. Zweitens: Banken behalten die Details der ergriffenen Betrugspräventionsmaßnahmen für sich, um den Kriminellen keine Hilfestellung zu geben. Diese könnten die entsprechenden Informationen nutzen, um unerkannt zu bleiben oder Kunden noch gezielter anzusprechen.

Wie unterscheidet sich Betrugsprävention bei digitalen Banken gegenüber traditionellen?

In einer digitalen Umgebung werden Daten bedeutend schneller verarbeitet und Banking ist dabei keine Ausnahme. Wir bei N26 nutzen dies zu unserem Vorteil: Wir setzen auf Tools, die es uns bereits ab der Registrierung des Kunden ermöglichen, Muster betrügerischen Verhaltens in Echtzeit zu überwachen und zu identifizieren. Unser Schwerpunkt auf Technologie, KI, Daten und fortschrittlichen Algorithmen in Verbindung mit menschlicher Intelligenz gestattet es uns, Personen zu verifizieren und zu überwachen. So stellen wir sicher, dass verdächtige Verhaltensweisen schnell erkannt werden.

Was unternimmt N26, wenn betrügerisches Verhalten bei einem Kunden festgestellt wird?

Wenn unser Expertenteam Unregelmäßigkeiten aufdeckt, ergreifen wir alle gesetzlich vorgeschriebenen Maßnahmen zur Schadensbegrenzung. Dazu zählen mitunter die Schließung der Konten und die Meldung derselben an die Behörden. Falls verdächtige Transaktionen auf Geldwäsche, Terrorismusfinanzierung oder eine andere Straftat hinweisen, meldet N26 diese Aktivitäten unverzüglich der deutschen Zentralstelle für Finanztransaktionsuntersuchungen (“Financial Transaction Investigation Unit”; FIU) oder lokalen Aufsichtsbehörden.

Wie hat N26 in die Sicherheit der Bank investiert?

2019 hat N26 einige Neuerungen eingeführt, um das Sicherheitssystem noch weiter zu stärken. Dazu gehört der Aufbau eines Trust and Safety Teams innerhalb von IT-Security: Dieses Team beschäftigt sich mit dem Schutz von N26 Nutzern, ihrer Konten und persönlichen Informationen gegen Cyberkriminalität. Darüber hinaus wurde das A-Team aufgebaut – ein Team von Spezialisten, das sich eigens der Unterstützung von Kunden widmet, auf deren Konten verdächtige oder betrügerische Aktivitäten festgestellt werden. Darüber hinaus hat N26 die Größe des eigenen AML-Teams und der Einheit für Finanzkriminalität verdoppelt sowie Transaktionsüberwachungs- prozesse und -plattformen etabliert. Diese Maßnahmen ermöglichen es uns, schädliche Aktivitäten auf Grundlage historischer Daten aufzudecken und zu verhindern. So können wir Kriminellen immer einige Schritte voraus sein. Wir investieren stark in Technologie und KI. Neben Verhaltensanalyse setzen wir auch auf fortschrittliche statistische Modelle und Algorithmen.

Wie sieht die Zukunft der Cybersicherheit und Cyberkriminalitätsprävention aus?

Da die Menschen ein zunehmend digitalisiertes und vernetztes Leben führen, muss die Welt der Cybersicherheit mit dieser Entwicklung Schritt halten. In Zukunft werden immer mehr Drittanbieter-Apps Einzug in das Banking-Umfeld halten. Der Einsatz von KI und maschinellem Lernen bei der Überwachung und Aufdeckung von Betrug ist von zentraler Bedeutung für die Wahrung der Sicherheit. Viele dieser Tools sind bei N26 bereits in Verwendung. Wir sind überzeugt davon, dass die digitalen Innovatoren von heute eine wichtige Rolle für die künftige Gestaltung der Cybersicherheitsbranche spielen werden.

Wichtige Anlaufstellen bei N26

Falls du denkst, dass sich jemand unbefugten Zugriff auf dein Konto oder deine Kartendaten verschafft hat, ändere bitte umgehend dein Passwort und sperre deine Karte in der N26 App. Du kannst N26 unter den folgenden Adressen erreichen:

MELDEN einer verdächtigen Transaktion:
Kontaktiere uns umgehend im In-App-Chat oder schicke uns eine E-Mail an support@n26.com.

MELDEN einer verdächtigen Nachricht oder Webseite:
Leite die E-Mail und/oder die URL der Webseite an phishing@n26.com weiter.

TEILEN einer Idee zur Verbesserung der Sicherheit bei N26:
Schreibe uns eine Nachricht an security@n26.com.

N26

Der N26 Ratgeber für
sicheres Online-Banking