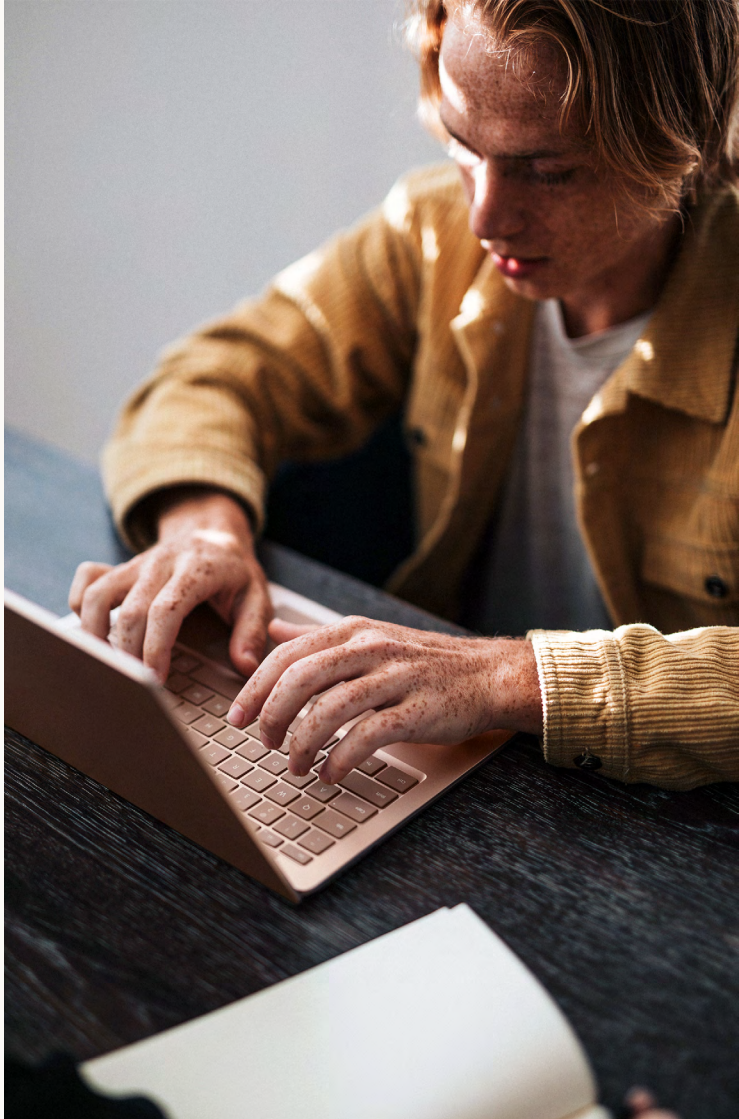
N26

Notre guide Sécurité pour utiliser votre banque en toute confiance



Effectuer ses transactions en ligne en toute sécurité

Dans un monde transformé par la COVID-19, les populations ont été poussées à tirer parti des technologies et de l'innovation, le temps de s'adapter à une nouvelle normalité. Nous avons vu des clients se tourner vers des solutions numériques, opter pour des paiements sans contact plutôt qu'en espèces, ou encore acheter en ligne plutôt que de se rendre en magasin. Il n'est donc pas étonnant que de nombreuses personnes recourent aux banques digitales au lieu de se rendre en agence. En fait, près de 39 % de la population mondiale devrait avoir accès à des services bancaires de détail en ligne d'ici 2021.

Vous vous demandez peut-être qui protège leur argent ?

En tant que banque allemande entièrement agréée, N26 est régie par les mêmes réglementations que ses homologues bancaires traditionnels. Ainsi, nous investissons massivement pour garantir la sécurité et l'intégrité de nos transactions en ligne. En parallèle de toutes nos procédures et réglementations pour protéger votre argent, vous pouvez aussi agir pour vous protéger de la cybercriminalité. Avec ce guide, nous voulons vous partager les meilleures pratiques et recommandations, afin que vous puissiez conserver votre argent en ligne en toute sécurité.

[1] Étude de Barracuda Sentinel - Threat Spotlight: Coronavirus-Related Phishing

Les questions de sécurité : une priorité aussi numérique

Toutes les banques sont confrontées à la cybercriminalité, et N26 étant une banque qui gagne en renommée, elle est de plus en plus la cible des cybercriminels. Tout comme les autres banques agréées, N26 doit se conformer à des réglementations strictes en matière de sécurité, de conformité et de prévention des crimes financiers.

Dans un environnement numérique, la sécurité est une priorité encore plus importante. Les fraudeurs sont constamment à la recherche de nouvelles techniques d'approche pour entrer en contact avec des clients peu méfiants, lorsqu'ils s'y attendent le moins. Ils peuvent être rapides, malicieux et extrêmement créatifs dans leurs approches. Par exemple, en mars 2020, au cours du premier mois de la pandémie de COVID-19, les attaques d'hameçonnage liées au coronavirus ont augmenté de 667 % dans le monde.[1]

C'est la raison pour laquelle N26 ne cesse de s'ajuster et s'adapter en matière de sécurité. Notre priorité est de toujours garantir la sécurité de votre argent, en veillant à ce que nos mesures soient conformes aux derniers développements de l'industrie.

[1] Étude de Barracuda Sentinel - Threat Spotlight: Coronavirus-Related Phishing

5 menaces courantes lors des transactions en ligne

Pendant que nous travaillons assidûment pour assurer en permanence la sécurité des transactions numériques avec N26, des personnes malveillantes cherchent le meilleur moyen pour arnaquer les clients. Le meilleur rempart contre leurs procédés est de vous sensibiliser en tant que client pour que vous restiez toujours vigilant. Voici les types de procédés les plus courants lors des transactions en ligne :

1. L'**hameçonnage** est un type de fraude utilisé par les cybercriminels pour pousser le client à partager des données personnelles sensibles, telles que ses identifiants de connexion. Ces informations de compte et de carte bancaire, ainsi que d'autres données pouvant être utilisées à des fins d'usurpation. Ces cybercriminels ont souvent recours à la menace pour intimider leurs cibles, et les pousser à satisfaire leurs demandes. Ces tentatives sont le plus souvent transmises par email et SMS, et elles contiennent habituellement des liens vers des sites internet malveillants.

2. Le **piratage psychologique**, tactique généralement subtile et coercitive, est extrêmement efficace pour manipuler émotionnellement la victime. Les fraudeurs recourent à diverses techniques pour créer de la confiance et amener les individus peu méfiants à leur donner des informations de leur plein gré. Ils peuvent essayer de les obtenir en créant des contraintes parfois pour forcer leurs cibles à céder.

3

Les **arnaques au recrutement** ont lieu lorsque des criminels publient des annonces contenant des informations frauduleuses, visant à recueillir les données personnelles d'individus peu méfiants. Ils peuvent demander aux candidats d'ouvrir des comptes en inventant des prétextes et masquer ainsi la raison derrière leurs actions. Les fraudeurs peuvent de ce fait ouvrir et accéder à des comptes bancaires au nom de leurs cibles sous couvert d'offres d'emplois légitimes.

4

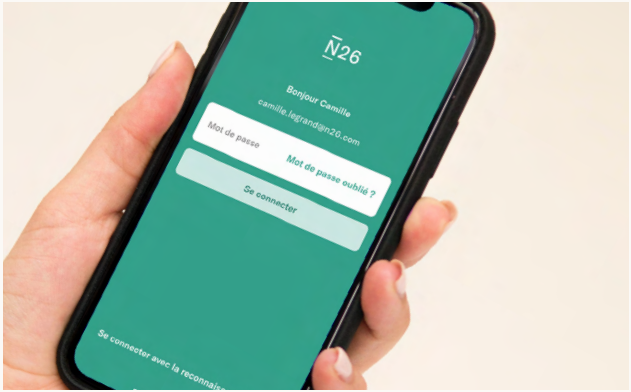
La **fraude sur les marchés en ligne (Marketplace fraud)** se réfère aux crimes commis par les cybercriminels après avoir créé un compte bancaire avec des identités volées et/ou après avoir pris le contrôle d'un compte en utilisant la technique de l'hameçonnage. Les fraudeurs utilisent ces comptes volés pour créer de faux profils sur des marchés en ligne et pousser des acheteurs naïfs à virer des fonds pour des produits inexistants, de fausses annonces immobilières, des voitures d'occasion, et d'autres articles fictifs.

5

Le **vol de données** a lieu lorsque des cybercriminels ciblent de larges entreprises dans le but d'accéder aux données confidentielles de clients, notamment à leur nom, adresse personnelle, informations d'assurance, détails de carte bancaire, etc. Plutôt que de s'attaquer aux systèmes de sécurité d'une banque, les cybercriminels ciblent à la place des entreprises régulièrement sollicitées pour des transactions en ligne, des compagnies aériennes aux détaillants, en passant par les sites de streaming en ligne. Les informations volées peuvent être utilisées pour accéder aux comptes bancaires de clients, qui peuvent ensuite être utilisés pour effectuer des achats ou commettre d'autres types de fraudes.

Des fonctionnalités de sécurité importantes pour sécuriser votre banque digitale

N26 multiplie les efforts et les initiatives pour offrir une expérience bancaire sûre à ses clients. Voici quelques-unes des fonctionnalités de sécurité les plus importantes pour garantir la sécurité de votre compte :



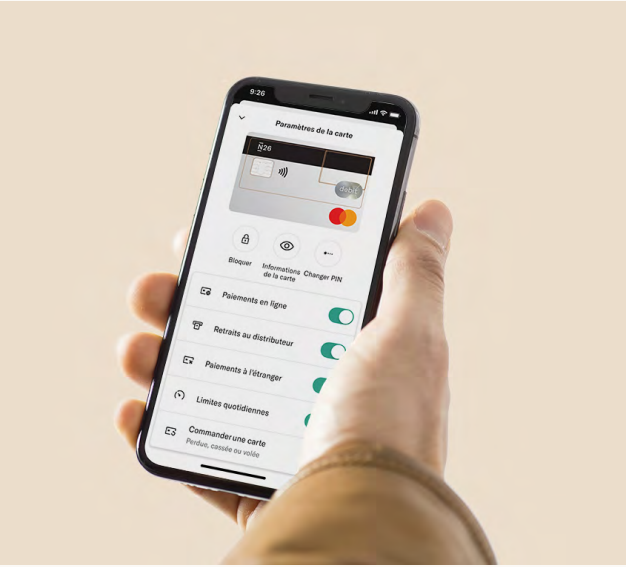
Un appareil appairé unique : vous ne pouvez accéder à votre compte N26 qu'à partir du smartphone appairé. Vous êtes ainsi assuré d'être le seul à pouvoir accéder à votre argent.

Authentification à deux facteurs : en plus de vous connecter à votre compte N26 depuis votre appareil appairé, vous devez fournir votre mot de passe, ou effectuer une vérification biométrique, pour prouver que vous êtes bien l'unique titulaire légitime du compte.

Empreinte digitale et reconnaissance faciale : les données biométriques nous aident à garantir que vous êtes le seul à pouvoir vous connecter à votre compte. Votre mot de passe ne risque donc pas d'être compromis.

Notifications instantanées : surveillez de près vos transactions, en temps réel, grâce aux notifications push instantanées. Ainsi, vous pourrez examiner immédiatement chaque transaction, directement sur votre smartphone.

Verrouillage de carte intégré à l'application : si jamais vous pensez que les détails de votre carte ont été compromis, vous pouvez immédiatement verrouiller votre carte ou changer votre PIN en quelques étapes simples, rapides et directement depuis votre téléphone en toute autonomie.



3D Secure : cette étape d'authentification nécessite que vous autorisiez les paiements en ligne par l'intermédiaire de votre application N26 avant qu'ils ne soient traités, ce qui vous permet d'identifier et d'empêcher facilement une utilisation frauduleuse en ligne de votre carte. D'autant qu'à tout moment, vous pouvez depuis votre mobile bloquer les achats en ligne et les débloquer quand vous le souhaitez.

Géolocalisation : en activant la géolocalisation dans votre application N26, nos systèmes sont capables de détecter si votre carte est utilisée à un emplacement différent du vôtre, ainsi que d'autres modes d'utilisation potentiellement suspects.

Vérification d'identité : en tant que banque agréée, N26 travaille avec des partenaires réglementés de l'industrie afin de vérifier l'identité de chaque client avant l'ouverture d'un compte. Cela nous permet de nous assurer de l'intégrité des clients ouvrant des comptes chez nous.

Blocages des paiements intelligents : contrôlez la manière dont votre carte est utilisée dans votre application en désactivant facilement les paiements en ligne, les retraits au guichet automatique, les transactions par bande magnétique ou les paiements à l'étranger, en un seul glissement de doigt.

Fonctionnalité de boîte de réception sécurisée : pour vous contacter en cas d'urgence, nous vous envoyons un message via la boîte email intégrée à l'application. Ainsi vous êtes le seul à pouvoir le lire et à y répondre.

10 astuces simples pour garantir la sécurité de votre compte en ligne

Que vous fassiez des achats, des transactions bancaires ou que vous gériez votre boîte de réception, voici quelques astuces pour garantir une sécurité optimale et protéger vos données personnelles dans cette ère numérique.

Faites vos achats uniquement sur des sites internet dignes de confiance de marchands connus et reconnus par les autorités.

Créez des mots de passe forts et robustes en privilégiant les combinaisons de lettres, de chiffres et de symboles ainsi que majuscules et minuscules et n'utilisez jamais le même mot de passe pour différents comptes.

Méfiez-vous des offres trop belles pour être vraies. Ce sont probablement des arnaques.

Mettez régulièrement à jour votre application N26 et votre système d'exploitation mobile, pour recevoir les dernières corrections et ajustements des systèmes de sécurité.

Ne publiez jamais d'informations personnelles sensibles en ligne sur les réseaux sociaux.

Vérifiez que les sites internet sont sécurisés, cherchez le cadenas à côté de l'adresse URL et examinez les identifiants en un simple clic.

Choisissez des fournisseurs d'e-mail sécurisés avec des filtres de courrier indésirable et authentification à deux facteurs, tels que Gmail, Yahoo ou d'autres fournisseurs de référence.

Utilisez l'analyse d'empreinte digitale ou la reconnaissance faciale pour vous connecter.

Activez la géolocalisation sur votre application N26, pour nous permettre d'identifier les transactions irrégulières que n'avez certainement pas effectuées.

Faites attention aux connexions Wi-Fi partagées ou publiques, choisissez toujours des connexions sécurisées WPA2 plutôt que WEP, et utilisez un VPN si possible.

Signes révélateurs d'un message suspect

Si vous n'êtes pas sûr d'un message ou d'un email que vous avez reçu concernant votre compte bancaire, contactez toujours l'équipe d'assistance de N26 avant d'agir. Voici quelques signes révélateurs de message suspect :

L'urgence : chaque fois que l'on vous demande d'agir immédiatement, arrêtez-vous et relevez tout ce qui vous semble inhabituel. Les cybercriminels utilisent souvent des alertes avec des contraintes de temps pour corrompre le processus de prise de décision. Sachez que les entreprises licites n'essaieront jamais de vous forcer à faire quelque chose immédiatement.

Des erreurs et des incohérences subtiles : méfiez-vous des présentations génériques, des fautes d'orthographe et des erreurs de formatage. Ce sont les signes d'une tentative potentielle d'hameçonnage.

Des adresses URL incorrectes : avant de cliquer sur un lien, assurez-vous de consulter l'URL du site internet en question. Vous pouvez le faire en survolant le lien afin de voir la page d'atterrissage. Par ailleurs, même des adresses URL authentiques sont souvent utilisées de manière frauduleuse. Vérifiez la présence de caractères qui ne devraient normalement pas être présents.

Des sites internet non sécurisée : méfiez-vous toujours des sites internet avec redirection. Vérifiez la présence du symbole en forme de cadenas qui indique une connexion sécurisée, cliquez dessus et vérifiez les références du site internet. Vous pourrez vérifier si le certificat SSL (Secure Sockets Layer) est valide, et à qui il a été émis.

Demandes d'informations : faites très attention aux demandes d'envoi d'informations personnelles. Gardez à l'esprit que N26 ne vous demandera jamais de partager des informations sensibles en dehors d'un environnement sécurisé.

Côté N26 : Comment les banques digitales combattent-elles la cybercriminalité?

Les équipes spécialistes sécurité, de lutte contre la criminalité financière et de prévention de la fraude de N26 veillent au quotidien pour protéger nos clients de tout type de fraude et assurer la sécurité de leur argent. Ils répondent aujourd'hui aux questions les plus courantes concernant ces enjeux de sécurité et les risques liés à tout type de fraude.

Que doivent faire les banques pour empêcher les fraudes ?

Toutes les banques agréées doivent se conformer aux exigences réglementaires et signaler aux autorités tout comportement suspect sur notre plateforme. N26 ne fait pas exception, et doit remplir ces obligations juridiques comme toute autre banque.

Les banques digitales sont-elles moins sécurisées que les banques traditionnelles ?

Les banques digitales peuvent opérer avec un certain nombre de licences différentes, ce qui pourrait signifier qu'elles ne se conforment pas toutes aux mêmes standards réglementaires de sécurité et de prévention des fraudes, surtout si elles détiennent des licences fintech ou e-money. En tant que banque allemande entièrement agréée, N26 est régie par les mêmes réglementations que ses homologues traditionnels. De plus, nous mettons l'accent sur la sécurité, ce qui nous rend aussi sûrs qu'une banque traditionnelle.

Comment N26 détecte-t-elle et surveille-t-elle les fraudes ?

N26 a une équipe spécialisée axée sur la surveillance et l'identification des transactions suspectes sur notre plateforme. En utilisant des modèles statistiques, d'algorithmes avancés et d'analyses du comportement humain, notre équipe d'experts s'assure que votre argent est toujours entre de bonnes mains.

Pourquoi les banques sont-elles toujours aussi opaques sur leur gestion des fraudes ?

Les raisons sont doubles. Tout d'abord, étant régies par des lois strictes sur la confidentialité des données et le secret bancaire, les banques ne peuvent jamais partager les détails d'une affaire sauf avec la police. Ensuite, les banques protègent étroitement les détails concernant les mesures de prévention des fraudes, afin de ne pas donner de piste aux fraudeurs, qui pourraient utiliser ces informations pour ne pas se faire repérer ou pour cibler des clients plus efficacement.

En quoi la prévention des fraudes est-elle différente dans un environnement bancaire numérique ?

Les informations sont traitées beaucoup plus rapidement en ligne, et le secteur bancaire n'y fait pas exception. Chez N26, nous utilisons cela à notre avantage, avec des outils qui nous permettent de surveiller et d'identifier des comportements frauduleux en temps réel, dès l'inscription du client. Un accent sur la technologie, l'intelligence artificielle, les données et les algorithmes avancés combiné à l'intelligence humaine nous permet de vérifier et de surveiller des individus afin de garantir un signalement rapide des comportements suspects.

Que fait N26 en cas de détection de comportement frauduleux dans sa base de clients ?

Lorsque notre équipe d'experts détecte une activité irrégulière, nous prenons toutes les mesures d'atténuation, conformément aux lois réglementaires, pour empêcher des dégâts supplémentaires dont la fermeture et le signalement aux autorités des comptes incriminés. Lorsque des transactions suspectes indiquent des cas de blanchiment d'argent, de financement d'activité terroriste, ou de toute autre activité criminelle, N26 signale immédiatement ces activités à l'unité d'investigation des transactions financières allemande (Financial Transaction Investigation Unit, FIU) ou aux entités de supervision locales.

Quels sont les investissements de N26 en matière de sécurité ?

En 2019, N26 a continué d'adapter au mieux son approche de la sécurité pour qu'elle soit toujours plus optimale pour ses clients. Avec une équipe élargie et renforcée, les experts confiance et sécurité s'engagent au quotidien pour protéger les utilisateurs, leurs comptes et leurs données contre les cybercriminels. Ils sont par ailleurs guidés par une division d'experts spécialisés qui assistent spécifiquement les clients lorsqu'une activité suspecte ou frauduleuse est détectée sur leur compte afin d'optimiser la réactivité et la gestion avec nos clients de tels désagréments. De plus, N26 a doublé la taille de son effectif LCB (Lutte contre le blanchiment des capitaux), et a mis en place des processus et des plateformes de surveillance des transactions. Cela nous a permis de détecter et d'empêcher des activités malveillantes en nous basant sur des données historiques. Nous avons ainsi pu conserver une longueur d'avance sur les personnes malveillantes. Nous investissons énormément dans la technologie et dans l'intelligence artificielle pour exécuter des modèles statistiques et des algorithmes avancés, accompagnés d'une analyse comportementale.

Quelles seront les prochaines innovations dans le domaine de la cybersécurité et de la prévention de la cybercriminalité ?

À mesure que les populations mènent une vie de plus en plus numérique et connectée, le domaine de la cybersécurité se doit de tenir la cadence. Des applications tierces supplémentaires devant intégrer l'environnement bancaire, recourir à l'intelligence artificielle et à l'apprentissage automatique pour détecter et surveiller des fraudes est la clé pour garantir une gestion adéquate de la sécurité à grande échelle. Même si la plupart de ces outils sont déjà utilisés par N26, nous sommes convaincus que les innovateurs numériques actuels nous seront d'une grande aide pour faire avancer l'industrie de la cybersécurité.

Contacts importants lors des transactions avec N26

Si vous pensez que les détails de votre compte ou de votre carte ont été compromis, modifiez votre mot de passe et verrouillez votre carte immédiatement dans l'application N26. Vous pouvez également contacter N26 aux adresses ci-dessous :

POUR SIGNALER une transaction suspecte :
contactez-nous immédiatement sur le tchat ou l'email intégrés à l'application support@n26.com

POUR SIGNALER un message ou un site internet suspect :
transférez l'email ou l'adresse URL du site internet à phishing@n26.com

Pour PARTAGER une idée afin d'améliorer la sécurité chez N26
laissez-nous un message à security@n26.com

N26

Notre guide Sécurité pour utiliser votre banque en toute confiance