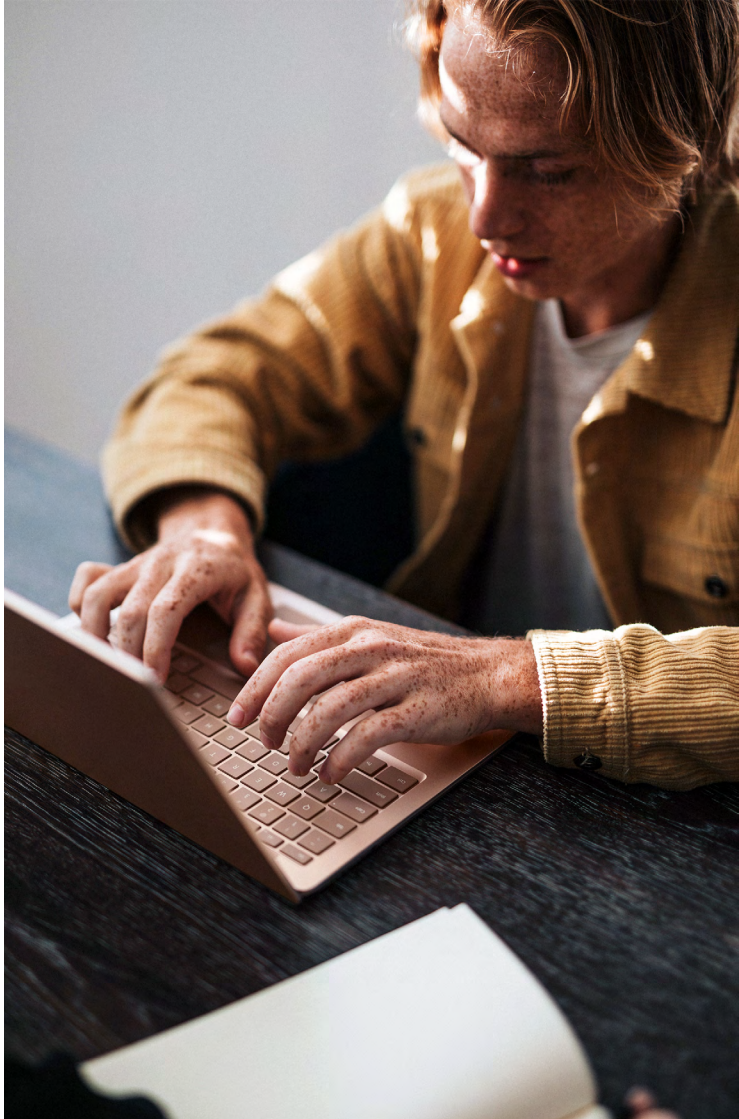
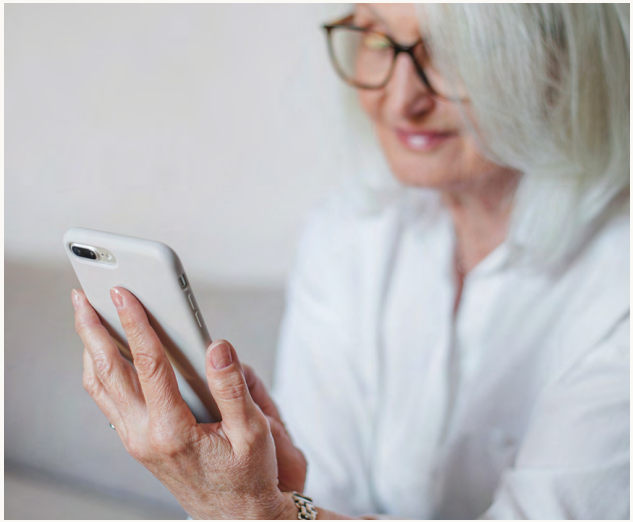
N26

La guía completa de N26 para realizar operaciones bancarias online de forma segura



Cómo mantener tu dinero a salvo utilizando servicios bancarios online

Con el mundo patas arriba a causa de la COVID-19, la gente ha empezado a ponerse en manos de la tecnología y la innovación para adaptarse a la nueva normalidad. Hemos visto cómo los clientes adoptan soluciones digitales, optan por los pagos sin contacto en lugar de pagar en efectivo y prefieren comprar online en vez de acudir a las tiendas. No es de extrañar entonces que haya tanta gente que recurra a los servicios bancarios online para evitar visitar las sucursales físicas. De hecho, se prevé que casi un 39 % de la población global empiece a utilizar los servicios bancarios online de aquí a 2021.



Pero ¿estará su dinero a salvo?

Como banco alemán plenamente acreditado, N26 se ciñe a los mismos reglamentos que nuestros homólogos tradicionales. En consecuencia, invertimos mucho en la seguridad e integridad de nuestra experiencia bancaria online. Además de las medidas internas que adoptamos en N26, también hay prácticas que puedes llevar a cabo tú mismo para proteger tu dinero de los ciberdelincuentes. Con esta guía queremos informarte sobre nuestras mejores prácticas y recomendaciones para que puedas proteger tu dinero online.

La seguridad: una prioridad crucial en un mundo digitalizado

Todos los bancos se enfrentan a la ciberdelincuencia, pero N26 está en el punto de mira de los ciberdelincuentes debido al crecimiento que ha experimentado durante los últimos años. Como cualquier otro banco acreditado, N26 debe cumplir reglamentos estrictos en materia de seguridad, cumplimiento normativo y prevención de delitos.

En un entorno digital, la seguridad es una prioridad que cobra especial importancia. Los estafadores siempre están buscando nuevas formas de perfeccionar sus métodos para aprovecharse de la ingenuidad de los clientes cuando menos se lo esperan. Sus métodos pueden ser rápidos, innovadores y tremendamente creativos: por ejemplo, en marzo de 2020, durante el primer mes de la pandemia global de la COVID-19, los ataques de phishing relacionados con el coronavirus se incrementaron en un 667 % en todo el mundo.[1]

Es por eso que en N26 mejoramos constantemente las medidas de seguridad. Nuestra prioridad es garantizar la seguridad de tu dinero en todo momento, asegurándonos de que nuestras medidas se ajusten a los últimos desarrollos del sector.

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

5 amenazas comunes que sufren los servicios bancarios online

Aunque trabajamos sin descanso para que los servicios bancarios digitales de N26 sean seguros, los delincuentes buscan constantemente nuevas formas de aprovecharse directamente de los clientes. La mejor prevención frente a estas estafas es que tú, como cliente, también te informes y conciencies. Estas son algunas de las estafas más comunes relacionadas con los servicios bancarios online:

1. El **phishing** es un tipo de estafa que los ciberdelincuentes utilizan para engañar a sus víctimas y que estas les comuniquen datos personales sensibles, como, por ejemplo: credenciales de acceso, datos de la cuenta y la tarjeta de crédito y otra información que puede utilizarse para suplantar su identidad. Suelen utilizar un lenguaje amenazante para intimidar a sus víctimas y manipularlas para que satisfagan sus exigencias. Normalmente, este tipo de ataques se realizan a través de correos electrónicos y SMS que suelen contener enlaces a sitios web maliciosos.

2. Las tácticas de **ingeniería social** suelen ser sutiles y coactivas, y resultan increíblemente eficaces a la hora de manipular el estado emocional de una persona. Los estafadores usan diferentes técnicas para crear confianza y engañar a personas ingenuas para que estas acaben revelándoles información de forma voluntaria. Pueden intentar someter a sus víctimas metiéndoles prisa, haciendo referencia a asuntos muy urgentes.

3

En las **falsas ofertas de empleo**, los delincuentes publican anuncios que contienen información fraudulenta para obtener datos personales de gente que no sospecha nada. Incluso pueden pedirles a los candidatos que abran cuentas con falsas excusas y decirles que oculten los motivos de sus acciones. Esto permite a los estafadores abrir cuentas bancarias a nombre de sus víctimas y acceder a ellas con el pretexto de ofertas de empleo reales.

4

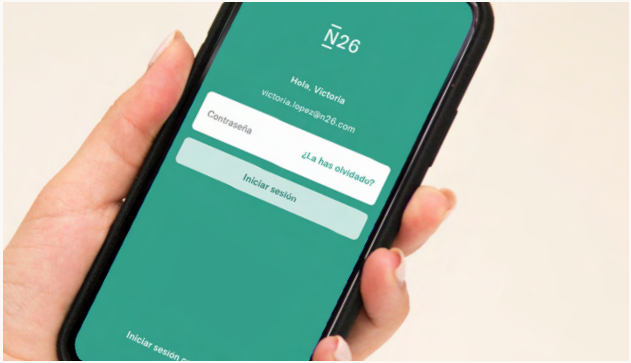
El **fraude de mercado** es un delito que los ciberdelincuentes pueden cometer creando cuentas bancarias con identidades suplantadas y haciéndose con el control de cuentas mediante el phishing. Los estafadores utilizan estas cuentas robadas para crear perfiles falsos en mercados online, para que los compradores transfieran fondos a cambio de productos inexistentes, ofertas inmobiliarias falsas, vehículos de segunda mano y otros artículos ficticios.

5

El **robo de datos** se da cuando los ciberdelincuentes atacan grandes empresas para acceder a datos confidenciales de los clientes, como pueden ser: nombres, direcciones, datos sobre seguros, datos de tarjetas de crédito, datos de transacciones, etc. En lugar de enfrentarse a los sistemas de seguridad de un banco, los ciberdelincuentes atacan empresas a las que la gente suele contratar online: aerolíneas, comercios minoristas o servicios de streaming online. Los datos robados pueden utilizarse para acceder a cuentas bancarias que después se utilizan para realizar compras y cometer otros tipos de fraude.

Funciones de seguridad importantes que contribuyen a la seguridad de tu cuenta bancaria digital

N26 se esfuerza por crear una experiencia bancaria segura para sus clientes. Estas son algunas de las funciones de seguridad más importantes para proteger tu cuenta:



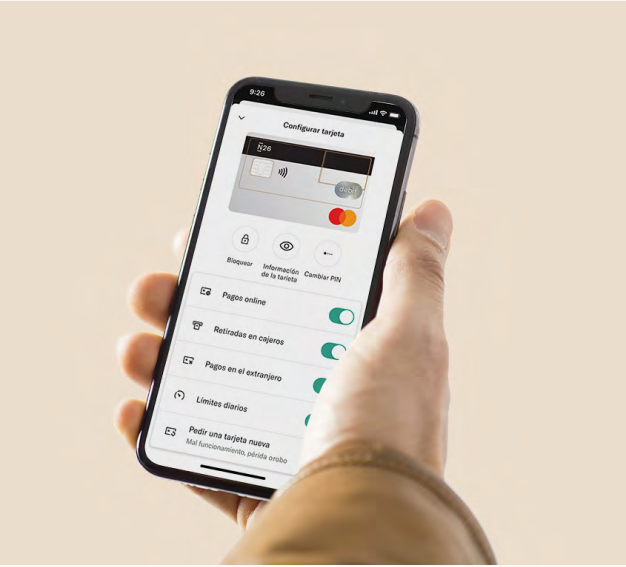
Un solo dispositivo vinculado: solo puedes acceder a tu cuenta N26 a través del móvil que has vinculado a ella; así te aseguramos que solo tú tengas acceso a tu dinero.

Autenticación de doble factor: además de iniciar sesión en tu cuenta N26 a través de tu dispositivo vinculado, debes introducir tu contraseña o verificar tu identidad por medios biométricos para demostrar que eres el titular legítimo de la cuenta.

Huella digital y reconocimiento facial: los datos biométricos nos ayudan a garantizar que solo tú puedas iniciar sesión en tu cuenta; así no tendrás que preocuparte porque te roben la contraseña.

Notificaciones instantáneas: controla todas tus transacciones en tiempo real con los mensajes push instantáneos. Así tendrás la posibilidad de revisar cada transacción al instante, directamente a través de tu móvil.

Bloquear la tarjeta desde la app: si sospechas que te han robado los datos de la tarjeta, puedes bloquearla inmediatamente o cambiar tu PIN en pocos clics en la app.



3D Secure: este paso de autenticación te obliga a autorizar los pagos online a través de tu app de N26 antes de que se tramiten, para que puedas identificar y prevenir fácilmente el uso fraudulento de tu tarjeta online antes de que se produzca.

Rastreo de ubicación: si permites que la app de N26 rastree tu ubicación, nuestros sistemas podrán detectar si tu tarjeta se está utilizando en una ubicación distinta a la que estás actualmente, así como otros patrones de uso sospechosos.

Verificación de identidad: como banco regulado, N26 colabora con asociados regulados del sector para verificar a cada uno de nuestros clientes antes de que abran una cuenta, por lo que podemos garantizar la integridad de las personas que abren cuentas en nuestra entidad.

Bloqueos de pagos inteligentes: controla las posibilidades de uso de tu tarjeta en la app desactivando fácilmente los pagos online, las retiradas en cajeros, las transacciones con banda magnética o los pagos en el extranjero con un solo clic.

Bandeja de entrada segura: si necesitamos ponernos en contacto contigo sobre un asunto importante, te enviaremos un mensaje al buzón de la app, por lo que solo tú podrás leerlo y responder.

10 consejos sencillos para protegerte online

Ya sea para comprar, utilizar servicios bancarios o administrar tu bandeja de entrada, estos consejos te ayudarán a que tú y tus datos estéis protegidos en el ciberespacio.

Compra solo en sitios web de confianza o vendedores de prestigio.

Crea contraseñas seguras con letras, números y símbolos, y nunca utilices la misma para varias cuentas.

Comprueba que los sitios web sean seguros: busca el candado junto a la URL y examina las credenciales haciendo clic en él.

Nunca publiques datos personales sensibles online o en las redes sociales.

Mantén actualizada la app de N26 y el sistema operativo del móvil con las últimas correcciones de fallos.

Mucho ojo con las ofertas demasiado buenas para ser reales: probablemente no lo sean.

Ten cuidado con las redes wifi públicas o compartidas; elige siempre conexiones seguras WPA2 en lugar de las conexiones WEP y utiliza una VPN siempre que puedas.

Elige proveedores de email con filtros de seguridad y spam, además de autenticación de doble factor, como Gmail y Yahoo!

Permite la ubicación en tu app de N26 para que podamos detectar las transacciones irregulares que puede que no hayas realizado.

Utiliza el escáner de huellas digitales o el reconocimiento facial para iniciar sesión.

Características que delatan a un mensaje sospechoso

Si te ha llegado un mensaje o email sobre tu cuenta bancaria pero no acaba de convencerte, ponte en contacto con el equipo de asistencia de N26 antes de hacer nada. Las características de un mensaje fraudulento o sospechoso pueden incluir:

Urgencia: cuando alguien te pida que hagas algo de inmediato, párate a mirar si detectas algo raro. Los ciberdelincuentes suelen utilizar alertas urgentes para interrumpir nuestro proceso de toma de decisiones. Recuerda que las empresas reales nunca intentan coaccionarte para que hagas algo enseguida.

Errores e inconsistencias sutiles: fíjate en las introducciones genéricas, los fallos ortográficos y los errores de formato. Estos revelan posibles intentos de phishing.

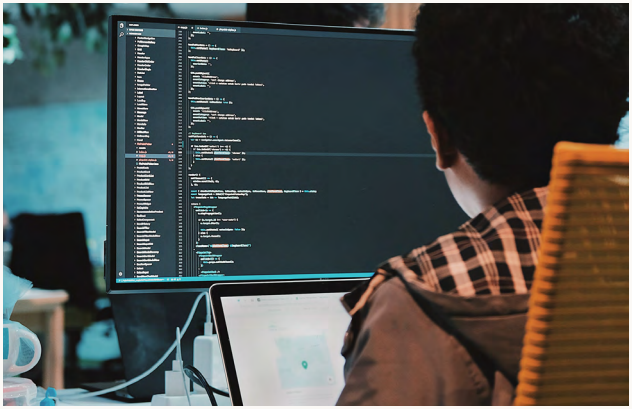
URL incorrectas: antes de hacer clic en ningún enlace, no olvides comprobar la URL del sitio web en cuestión. Puedes hacerlo pasando el puntero por encima del enlace para ver el destino del mismo. También pueden estar utilizando una URL real, así que busca caracteres que difieran de lo habitual.

Sitios web que no son seguros: duda siempre de los sitios web redirigidos. Busca el símbolo del candado que indica que la conexión es segura, haz clic en él y verifica las credenciales del sitio web. Podrás comprobar si el certificado Secure Sockets Layer (SSL) es válido y a nombre de quién está emitido.

Solicitudes de información: presta mucha atención cuando te pidan que envíes datos personales. Recuerda que N26 nunca te pedirá que compartas datos sensibles fuera de un entorno seguro.

Dentro de N26: cómo combaten la ciberdelincuencia los bancos digitales

Las divisiones de seguridad, prevención y lucha contra delitos y fraude de N26 están formadas por numerosos especialistas y expertos que ayudan a proteger a nuestros clientes de los delitos financieros. A continuación, responden a las preguntas más comunes sobre cómo N26 aborda el fraude como banco digital.



¿Qué obligaciones tienen los bancos en materia de prevención del fraude?

Todos los bancos regulados están obligados a cumplir las disposiciones reglamentarias y denunciar ante las autoridades toda conducta sospechosa en nuestra plataforma. N26 también debe cumplir estas obligaciones legales, como cualquier otro banco.

¿Los bancos digitales son menos seguros que los tradicionales?

Los bancos digitales pueden basar sus actividades en licencias distintas, es decir, que no todos están sujetos a los mismos reglamentos de seguridad y prevención del fraude, sobre todo si poseen licencias de tecnología financiera y dinero electrónico. Dicho esto, como banco alemán plenamente acreditado, N26 está sujeto a los mismos reglamentos que todos nuestros homólogos tradicionales. Tanto eso como el tener el tema de la seguridad siempre presente, nos hace tan seguros como un banco tradicional.

¿Cómo detecta y monitoriza N26 los fraudes?

N26 dispone de un equipo de expertos que se encarga de monitorizar e identificar las transacciones sospechosas en nuestra plataforma. Ayudándose de modelos estadísticos y algoritmos avanzados, además de un análisis de la conducta humana, nuestro equipo de expertos ayuda a garantizar que tu dinero esté siempre en buenas manos.

¿A qué se debe el secretismo de los bancos sobre cómo abordan el fraude?

Existen dos motivos. Primero, como estamos sujetos a leyes rigurosas de protección de datos y secreto bancario, no podemos comunicar los detalles de un caso, salvo a las autoridades policiales. Segundo, los bancos no revelamos los detalles de nuestras medidas de prevención del fraude para que no se enteren los estafadores, que pueden utilizar esta información para eludir su detección o atacar a los clientes con mayor eficacia.

¿En qué se diferencia la prevención del fraude en un banco digital?

En un entorno digital, la información se procesa con mucha más rapidez, y los servicios bancarios no son ninguna excepción. En N26 utilizamos eso a nuestro favor, con herramientas que nos permiten monitorizar e identificar patrones de conducta fraudulenta en tiempo real, desde el momento en que un cliente se registra. Utilizamos tecnología, inteligencia artificial, datos y algoritmos avanzados, en combinación con la inteligencia humana, para verificar y monitorizar a las personas y garantizar que toda conducta sospechosa se detecta con rapidez.

¿Qué hace N26 cuando detecta una conducta fraudulenta entre sus clientes?

Cuando nuestro equipo de expertos detecta una actividad irregular, tomamos todas las medidas de mitigación que establecen las leyes para evitar males mayores, incluida la de cerrar y denunciar las cuentas infractoras ante las autoridades. Cuando las transacciones sospechosas apuntan a un blanqueo de capitales, financiación terrorista o cualquier otro delito penal, N26 denuncia estas actividades de inmediato ante la Unidad de Investigación de Transacciones Financieras de Alemania (Financial Transaction Investigation Unit, FIU) o a los organismos supervisores locales.

¿Cómo ha invertido N26 en seguridad?

En 2019, N26 realizó una serie de cambios para mejorar aún más nuestro enfoque de seguridad. Primero, creamos un equipo completamente nuevo centrado en seguridad y confianza IT con el objetivo de proteger a los usuarios, sus cuentas y sus datos contra los ciberdelincuentes. A continuación, presentamos el A-Team, una división de expertos especializados que ayudan a los clientes cuando se detecta actividad sospechosa o fraudulenta en su cuenta. Por otro lado, N26 duplicó el tamaño de su equipo de AML y su unidad de delitos financieros, y estableció procesos y plataformas de monitorización de transacciones. Estos nos permiten detectar y prevenir las actividades maliciosas basándonos en datos históricos, lo cual, en última instancia, nos permite adelantarnos a los delincuentes. Invertimos mucho en tecnología e inteligencia artificial para desarrollar modelos estadísticos y algoritmos avanzados, además de analizar la conducta humana.

¿Qué novedades nos esperan en el mundo de la ciberseguridad y la prevención de la ciberdelincuencia?

A medida que la gente se digitaliza y se conecta cada vez más, el mundo de la ciberseguridad tiene que mantener el ritmo. En el futuro habrá más apps de terceros en el entorno bancario, por lo que el uso de inteligencia artificial y aprendizaje automático para monitorizar y detectar el fraude será crucial para garantizar que la seguridad se gestione de forma adecuada. Aunque N26 ya emplea muchas de estas herramientas, creemos que las innovaciones digitales actuales jugarán un papel importante para dar forma al sector de la ciberseguridad del futuro.

Contactos importantes cuando utilices N26

Si crees que te pueden haber robado los datos de la cuenta o la tarjeta, cambia la contraseña y bloquea la tarjeta en la app de N26 de inmediato. También puedes contactar con N26 directamente a través de estas direcciones:

PARA DENUNCIAR una transacción sospechosa:
habla con nosotros a través del chat de la app o envía un email a support@n26.com inmediatamente.

PARA MARCAR un mensaje o sitio web sospechosos:
reenvía el email o la URL del sitio web a phishing@n26.com.

PARA COMUNICAR una idea que mejore la seguridad en N26:
envía un mensaje a security@n26.com.

N26

La guía completa de N26 para realizar operaciones bancarias online de forma segura