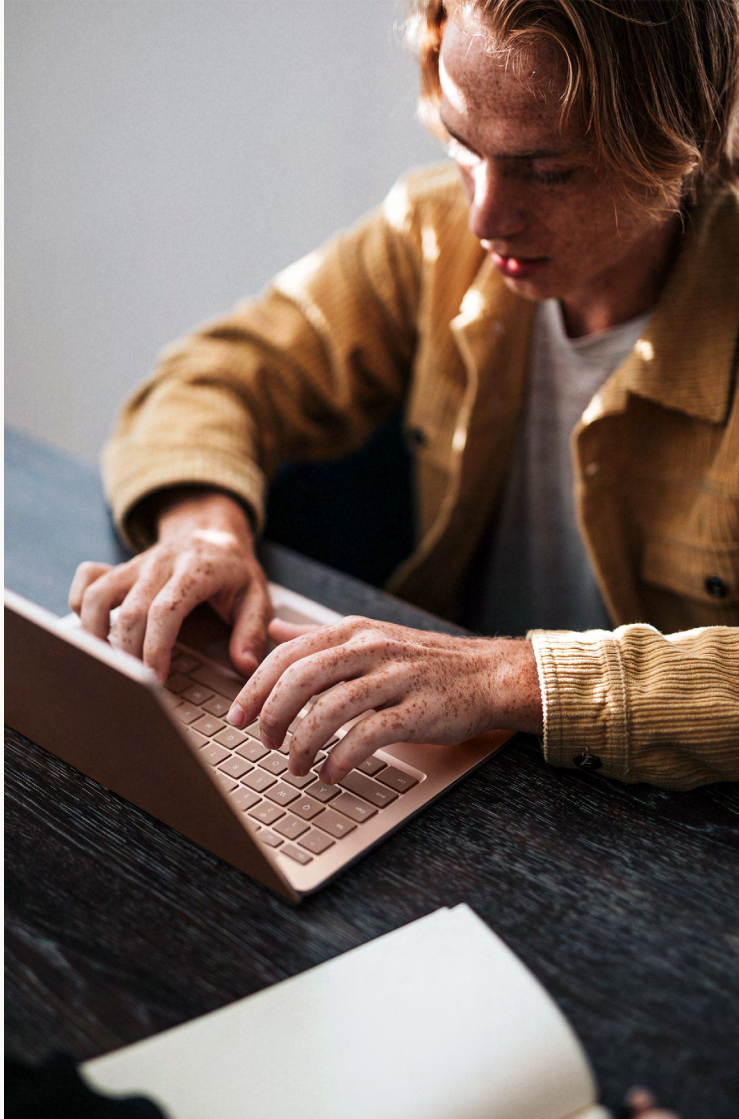
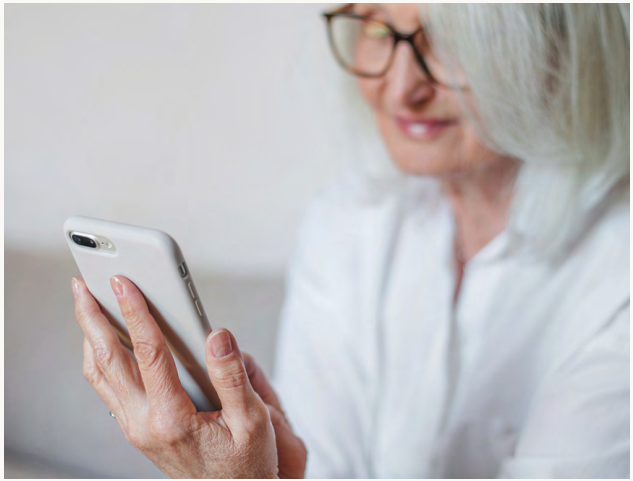
N26

The complete N26 guide to banking safely online



Keeping your money safe when banking online

In a world changed by COVID-19, people around the globe have been encouraged to embrace technology and innovation as we adjust to a new normal. We've seen customers turn towards digital solutions, opt for contactless payments instead of cash, and choose to shop online instead of visiting stores. It's no surprise then, that many people are turning to digital banking in order to avoid going to physical branches. In fact, it's predicted that almost 39% of the global population will access online retail banking services by 2021.



You may be wondering, who is protecting their money?

Being a fully-licensed German bank, N26 is governed by the same regulations as our traditional counterparts. As such, we invest heavily in the security and integrity of our online banking experience. In addition to what goes on behind the scenes at N26, there are things you can do to protect yourself from cybercrime. By launching this guide, we aim to equip you with our best practices and recommendations so that you can keep your money safe online.

Security matters:
An important priority in a digital world

All banks face cybercrime, and N26's growing presence in recent years has meant that we are increasingly on the radar of cybercriminals. Like any other licensed bank, N26 must adhere to strict regulations on security, compliance and financial crime prevention.

In a digital environment, security is an even more of a priority. Fraudsters are constantly looking for new ways to evolve their tactics and reach unsuspecting customers when they least expect it. They can be quick, innovative and extremely crafty in their approaches - for example, in March 2020, in just the first month of the COVID-19 global pandemic, coronavirus related phishing attacks increased by 667% globally[1].

This is why N26 is consistently optimizing its security efforts. Our priority is to keep your money safe by ensuring that our measures align with the latest developments in the industry.

[1] Research by Barracuda Sentinel - Threat Spotlight: Coronavirus-Related Phishing

5 common threats when banking online

While we work diligently to keep digital banking with N26 safe and secure, bad actors often look for ways to take advantage of customers directly. The best prevention for these schemes is education and diligence from you, the customer. Here are some of the most common types of schemes you might encounter banking online:

1. **Phishing** is a means to commit fraud and is used by cybercriminals to trick their targets into sharing sensitive personal data, such as: login credentials, account and credit card details, and other information which can be used for impersonation purposes. They'll often use threatening language designed to intimidate their targets, and to manipulate them into complying with their demands. Typically, such attempts are transmitted via email and SMS messaging, and usually contain links to malicious websites.

2. **Social engineering** tactics are generally subtle and coercive, and are extremely effective in terms of manipulating a person's emotional state. Fraudsters will employ an array of techniques to build trust and deceive unsuspecting individuals into handing over information freely. They may try to achieve this by fabricating time-critical issues in order to force their targets into submission.

3 **Recruitment scams** take place when criminals post advertisements, containing fraudulent information, as a means of collecting personal data from unsuspecting individuals. Applicants may even be instructed to open accounts under false pretences, while being told to conceal the reason behind their actions. This allows fraudsters to open and access bank accounts in their targets' names under the guise of legitimate recruitment offers.

4 **Marketplace fraud** is a crime that cybercriminals are able to commit after creating bank accounts with stolen identities and/or gaining control of accounts through phishing. Fraudsters use these stolen accounts to create fake profiles in online marketplaces, so that unsuspecting buyers will transfer funds for non-existent products, fake property listings, second-hand cars, and other fictional items.

5 **Data theft** occurs when cybercriminals target large companies for the purpose of accessing privileged customer data, including: names, residential addresses, insurance information, credit card details, transaction data, and so on. Rather than taking on the security systems of a bank, cybercriminals often choose to target companies that people often transact with online - from airlines, to retailers, to online streaming services. Stolen information can be used to access retail banking accounts, which can then be used to make purchases and/or commit other types of fraud.

Important security features that help keep your digital bank account safe

N26 puts enormous effort into creating a safe banking experience for its customers. Here are some of the most important security features that help keep your account safe:

A single paired device: Your N26 account can only be accessed via your paired smartphone - you can rest assured that only you have access to your money.

Two-factor authentication: In addition to logging into your N26 account via your paired device, you must provide your password, or verify yourself biometrically, to prove that you are a legitimate account holder.

Fingerprint and face recognition: Biometric data helps us to ensure that only you can log into your account, so you don't need to worry about your password being compromised.

Instant notifications: Stay on top of your transactions, in real-time, with instant push-notifications. This way, you'll have the opportunity to review each transaction immediately, directly via your smartphone.

In-app card locking: If you ever have reason to believe that your card details have been compromised, you can immediately lock your card or change your PIN in a few easy taps.

3D Secure: This authentication step requires you to authorise online payments via your N26 app before they are processed - so you can easily identify and prevent fraudulent online use of your card before it happens.

Location Tracking: By enabling your N26 app to track your location, our systems are able to detect if your card is being used in a different location from where you are, along with other potentially suspicious usage patterns.

Identity verification: As a regulated bank, N26 works with regulated industry partners to verify each one of our customers before accounts are opened, so that we are able to ensure the integrity of the customers opening accounts with us.

Smart payment blocks: Stay in control of how your card can be used in your app by easily disabling online payments, ATM withdrawals, magnetic stripe transactions, or payments abroad, with a single swipe.

Secure inbox feature: If we need to contact you about something important, we'll send a message via the in-app mailbox, ensuring that only you can read and respond.

10 simple tips to keep yourself safe online

Whether shopping, banking or managing your inbox, here are some tips to keep you and your data safe in the digital space.

Shop only at trusted websites of well-known retailers

Create strong passwords with letters, numbers and symbols - and never use the same one across multiple accounts

Check that websites are secure - look for the lock by the URL and examine the credentials with a simple click

Never post sensitive personal information online via social media platforms

Keep your N26 app and mobile OS updated for the latest bug fixes

Watch out for offres that are too good to be true - they probably are

Be careful with public or shared WIFI connections - always choose secure WPA2 connections over WEP connections and use a VPN where possible

Enable location tracking on your N26 app, so we can spot irregular transactions that may not have been made by you

Choose email providers with security and spam filters and two-factor authentication like Gmail and Yahoo!

Use fingerprint scanning or facial recognition to log in

Telltale signs of a suspicious message

If you are unsure about a message or email you have received on your bank account, always reach out to the N26 Support team before taking action. Some signs of a fraudulent or suspicious message include:

Urgency: Whenever you are asked to take immediate action - stop and take note of anything unusual. Cybercriminals often use time-critical alerts to interrupt the decision-making process. Remember, legitimate companies will never try to coerce you into doing something on the spot.

Incorrect URLs: Before clicking on any links, make sure to check the URL of the website in question. You can do so by hovering over the link in order to see the intended destination. Also, legitimate URLs are often used fraudulently - check for characters that wouldn't normally be present.

Subtle errors and inconsistencies: Look out for generic introductions, spelling errors and formatting mistakes. These are signs of a potential phishing attempt.

Websites that aren't secure: Always be skeptical of redirected websites. Look for the padlock symbol that indicates a secure connection; click on it and verify the website credentials. You will be able to check whether or not the Secure Sockets Layer (SSL) certificate is valid, and to whom it has been issued.

Requests for information: Pay close attention when you are asked to submit any personal details. Keep in mind that N26 will never ask you to share sensitive information outside of a secure environment.

Inside N26:
How digital banks combat cybercrime

N26's Security, Anti-Financial Crime and Fraud Prevention divisions are each made up of numerous specialists and experts who help protect our customers from financial crime. They answer the most common questions about how N26 deals with fraud as a digital bank.

What are banks required to do to prevent fraud?

All regulated banks are required to comply with regulatory requirements and report any suspicious behavior on our platform to the authorities. N26 is no different, and must fulfil these legal obligations just like any other bank.

Are digital banks less secure than traditional banks?

Digital banks may operate with a number of different licenses, which could mean that not all are held to the same regulatory standards of security and fraud prevention, especially if they hold fintech or e-money licenses. That said, as a fully-licensed German bank, N26 is governed by the same regulations as all our traditional counterparts. That, and our central focus on security makes us every bit as safe as a traditional bank.

How does N26 detect and monitor fraud?

N26 has a specialised team focused on monitoring and identifying suspicious transactions on our platform. With the help of advanced statistical models and algorithms, alongside human behavioural analysis, our team of experts help ensure that your money is always in safe hands.

Why are banks so secretive about how they deal with fraud?

The reasons are twofold. First, being governed by strict data privacy and banking secrecy laws, banks are never able to share details of a case except with law enforcement authorities. Second, banks closely guard the details of our fraud prevention measures so as not to tip-off fraudsters who could use the information to evade detection or target customers more effectively.

How is preventing fraud different in a digital banking environment?

Information is processed much more quickly in a digital environment, and banking is no exception. At N26, we use this to our advantage, with tools that allow us to monitor and identify patterns of fraudulent behavior in real time, all the way from customer signup. An emphasis on technology, AI, data and advanced algorithms combined with human intelligence allows us to verify and monitor individuals to ensure that any suspicious behaviours are flagged quickly.

What does N26 do when fraudulent behaviour is detected within its customer base?

When our team of experts detect irregular activity, we take all mitigation measures, as per regulatory law, to prevent further damage - this includes: closing and reporting offending accounts to the authorities. When suspicious transactions indicate the existence of money laundering, terrorist financing, or any other criminal offence, N26 immediately reports these activities to the German Financial Transaction Investigation Unit (FIU) or local supervisory entities.

What are some of the ways that N26 has invested in security?

In 2019, N26 made a number of changes to further elevate our security approach. First, we built an all-new Trust and Safety team. They work within IT Security to safeguard users, their accounts and their data against cybercriminals. Next, we introduced the A-Team, a division of specialized experts that support customers when suspicious or fraudulent activity is detected on their account. Additionally, N26 doubled the size of its AML team and financial crime unit, and established new transaction monitoring processes and platforms. These enable us to detect and prevent malicious activity based on historical data, which ultimately allows us to remain several steps ahead of malicious actors. We invest heavily in technology and AI to run advanced statistical models and algorithms, alongside human behaviour analysis.

What's next in the world of cybersecurity and cybercrime prevention?

As people lead more digitized and connected lives, the world of cybersecurity needs to keep up. With more third-party apps set to enter the banking environment in the future, the use of AI and machine learning in fraud monitoring and detection will be key to ensuring security is properly managed at scale. While many of these tools are already used at N26, we believe that today's digital innovators will play an important role in helping us to shape the cybersecurity industry going forward.

Important contacts when banking with N26

If you believe your account or card details have been compromised, change your password and lock your card in the N26 app immediately. You can also contact N26 at the addresses below:

TO REPORT
a suspicious transaction - Reach us on in-app chat or email support@n26.com immediately

TO FLAG
a suspicious message or website - Forward the email and/or website URL to phishing@n26.com

TO SHARE
an idea to improve security at N26 - Drop us a message at security@n26.com

N26

The complete N26 guide to banking safely online