Nordea

Secure use of online access codes 04.2024

1. Access codes
In these security guidelines, Nordea's access codes refer to the Netbank user ID, the Nordea ID app, the code calculator, and the access codes, passwords, PIN codes or activation codes with which they can be used, as well as biometric identifiers or other means or methods of identification accepted by Nordea and any passwords created using identification data.

2. Verifying a customer's identity
Nordea verifies your identity through your access codes or another identification method accepted by it when you log in to the Netbank service or any other service it offers that is used with access codes.

You can also use the access codes to verify your identity in other service providers' online services, unless this feature has been excluded from your access codes.

3. Personal nature of access codes
The access codes of a personal customer are always personal. Never let another person, not even a family member, use any part of them, and never let another party use the service connection opened with the access codes.

4. Access codes of corporate or institutional customers
The access codes of a corporate or institutional customer are customer-specific. Corporate and institutional customers must ensure that their access codes are kept safely and that they will not fall into the hands of parties not authorised to use them.

5. Protection of access codes
You should memorise the identification data related to the use of the access codes. Never store your personal identification data, such as your user ID, codes, PIN or password, in the same place as your other banking access codes, such as in your purse or wallet, handbag, phone or home.

Protect the device, such as the keypad or mobile phone, with which you are using your access codes so that nobody can take possession of or learn the access codes.

6. Your computer's and mobile device's security
Ensure your computer's and mobile device's security by updating their operating systems and the software/apps installed in them. Protect your computer also with a firewall restricting network traffic and with anti-virus software. Read the data security instructions on Nordea's website (www.nordea.fi/security).

7. Login with fingerprint authentication or a similar biometric identifier

7.1. Personal mobile device
You can set up an application with fingerprint authentication or a similar biometric identifier in your device for logging in to Nordea's mobile or online banking services as long as your device has adequate support for this feature. Biometric identifiers are safe and allow a smoother use of the services.

7.2. Use of Nordea's applications on a shared mobile device
You can't assign different biometric identifiers for different users in one device, which means that activating biometric identification in Nordea's apps allows all users who have saved their biometric identifiers in the device to access app data. We do not recommend using biometric identification in our apps on shared devices.

7.3. Deactivating biometric identification
You can deactivate biometric identification in the settings of our apps or by switching the entire feature off in the device's settings.

8. Nordea Customer Service by phone
When you call Nordea Customer Service, we will verify your identity through your access codes when you enter your user ID with the number keys on your phone. Enter your PIN code or a separate code during the call, if asked to do so.

The Nordea ID app includes a feature that allows you to verify that a phone call is from Nordea. This feature is called 'Verify call' in the Nordea ID app. If you use this feature, we will not ask you for your access codes, but instead you must enter your codes in the app, which will allow us to verify your identity.

9. Fraudulent queries about access codes
Never tell your access codes to any third party asking for them over the phone or otherwise. Never disclose your access codes through a request or link sent via a text message, email or similar contact method. Never download software on your device if a third party asks you to do so.

Banks, public authorities and other reliable organisations will never ask for your access codes through the methods mentioned above.

10. Accessing online services
Log in to all your services from the website of the service provider. Avoid clicking links and using search engines when logging in to services.

11. Confirmation requests in the Nordea ID app
If you are confirming a transaction with the Nordea ID app, check that the details shown in the app match the transaction.

If the confirmation requests you see in the app are not related to your transactions, do not confirm the transactions. Contact Nordea Customer Service instead.

12. How to block access codes

If your user ID, code card, mobile device where the Nordea ID app is installed, code calculator, PIN, other means of identification or password is lost, falls in the possession of someone else or becomes known to someone else, or you suspect that this may have happened, report it to us immediately. You can report it by visiting one of our branches in person or by calling us on 0200 70 000 (local rates apply), from abroad +358 200 70 000 (international call charge). If you are a corporate customer, call us on 0200 26262 (local rates apply), from abroad +358 200 26262 (international call charge).

13. Notifications concerning the security of the access codes

If we need to issue notifications concerning the security of the access codes, we will publish the notifications in our digital services, such as the login page of our online and mobile banking services.