Nordea

Trygg användning av bankkoder 04.2024

1. Bankkoder
Med Nordeas bankkoder avses i denna säkerhetsanvisning användar-ID:t för nätbanken, appen Nordea ID, kodkalkylatorn och koder, lösenord, pinkoder eller aktiveringskoder för att använda dessa samt biometriska identifieringsmetoder eller andra identifieringsverktyg eller identifieringsmetoder som banken godkänner samt lösenord som skapats genom att använda identifieringsuppgifter.

2. Identifiering av kunden
Banken verifierar din identitet med hjälp av bankkoder eller annan identifieringsmetod som banken godkänner då du loggar in i bankens nätbankstjänst eller annan tjänst som banken tillhandahåller och som används med bankkoder.

Med bankkoderna kan du identifiera dig även i andra tjänsteleverantörers internettjänster om denna egenskap inte har uteslutits från dina bankkoder.

3. Personliga koder
Privatkundens bankkoder är alltid personliga. Låt aldrig någon annan använda dina koder, inte ens din familjemedlem. Överlåt inte heller en tjänstförbindelse som du har öppnat med bankkoderna till en annan instans.

4. Företags- och organisationskunders koder
Företags- och organisationskunders bankkoder är kundspecifika. Företags- och organisationskunderna ska se till att förvara bankkoderna omsorgsfullt och på så sätt att de inte är tillgängliga för andra än de som har befogenhet att använda dem.

5. Skydda koderna
Lär dig identifieringsuppgifterna utantill för att använda bankkoderna tryggt. Förvara aldrig dina personliga identifieringsuppgifter, såsom användar-ID, koder, pinkoder eller lösenord tillsammans med andra bankkoder till exempel i din plånbok, handväska, telefon eller hemma.

Skydda apparaten, till exempel tangentbordet eller telefonen, mot insyn när du skriver in bankkoderna så att utomstående inte har möjlighet att komma åt dina koder.

6. Din dators och mobila enhets datasäkerhet
Ta hand om din dators och mobila enhets datasäkerhet genom att uppdatera deras operativsystem och de program och appar som installerats på dem. Skydda din dator även med en brandvägg som begränsar webbtrafiken och med ett antivirusprogram. Ta del av anvisningarna för datasäkerhet som finns på bankens webbplats www.nordea.fi/tietoturva.

7. Inloggning med fingeravtrycksidentifiering eller motsvarande biometriska kännetecken

7.1. Personlig mobilenhet
Du kan börja använda en app på din mobila enhet för att logga in i mobil- eller nätbanken och ansluta fingeravtrycksidentifiering eller motsvarande biometrisk identifieringsmetod till den med antagande om att din enhet är kompatibel med dessa på en tillräcklig nivå. Biometrisk identifiering är trygg och gör det lättare att använda appen.

7.2 Användning av Nordeas appar på en mobil enhet som har flera användare
Användningen av biometriska kännetecken på en enhet gör ingen skillnad mellan användare, och därmed ger aktivering av biometriska kännetecken i appar åtkomst till appens uppgifter för alla som har biometriska kännetecken sparade på enheten i fråga. Banken rekommenderar inte att biometriska kännetecken används i bankens appar på enheter som har flera användare.

7.3 Att slopa biometrisk identifiering
Vid behov kan du slopa biometrisk identifiering i inställningarna av bankens appar eller avaktivera funktionen helt i enhetens inställningar.

8. Nordeas kundtjänst per telefon
Banken identifierar dig med hjälp av bankkoderna när du ringer till Nordea Kundtjänst och knappar in ditt användar-ID med sifferknapparna på din telefon. Koden eller pinkoden anger du vid behov under samtalet.

I appen Nordea ID ingår en funktion med vilken du kan försäkra dig om att samtalet kommer från Nordea. I appen Nordea ID heter denna funktion Bekräfta att samtalet kommer från Nordea. I funktionen frågar banken inte efter bankkoderna utan du ska själv ange koderna i appen Nordea ID varefter banken identifierar dig.

9. Falska förfrågningar om bankkoder
Lämna aldrig ut dina nätbankskoder muntligt till tredje part som ber om dem per telefon eller på något annat sätt. Lämna inte heller ut dina nätbankskoder till exempel utifrån en begäran som du fått per sms eller e-post eller via en länk som skickats på detta sätt. Ladda inte ner programvara på din enhet utifrån förfrågningar från tredje part.

En bank, myndighet eller någon annan pålitlig instans frågar aldrig efter dina nätbankskoder på ovan nämnda sätt.

10. Inloggning i tjänster på webbplatser
Logga in i tjänster via tjänsteleverantörers webbplatser. Logga inte in via länkar eller sökmotorer.

Nordea Bank Abp Hamnbanegatan 5, 00020 NORDEA, hemort Helsingfors, FO-nummer 2858394-9
MMST970DL 06.18

11. Begäran om bekräftelse i appen Nordea ID
När du bekräftar en transaktion med appen Nordea ID ska du kontrollera att uppgifterna i appen stämmer överens med transaktionen du håller på att göra.

Om begäran om bekräftelse i appen inte hänför sig till dina egna ärenden, godkänn inte transaktionen utan kontakta Nordea Kundtjänst.

12. Spärrning av bankkoder
Meddela banken omedelbart om ditt användar-ID, ditt kodkort, din mobila enhet på vilken appen Nordea ID installerats, kodkalkylatorn, pinkoden, ett annat identifieringsverktyg eller ditt lösenord försvinner eller hamnar i en utomståendes händer eller kännedom eller om du misstänker det. Du kan lämna meddelandet personligen på bankens kontor eller genom att ringa Nordea Kundtjänst på 0200 5000 (lna/msa*), från utlandet +358 200 5000 (pris för utrikessamtal) eller kundtjänsten för företagskunder på 0200 2525 (lna/msa*), från utlandet +358 200 2525 (pris för utrikessamtal).

13. Meddelanden om säkerheten vid användningen av bankkoder
Banken publicerar eventuella meddelanden om säkerheten vid användningen av bankkoder på sin webbplats, till exempel på inloggningssidorna till nät- och mobilbanken.

*) lna = lokalnätsavgift, msa = mobilsamtalsavgift