Corporate Netbank
Datasikkerhedsinstrukser

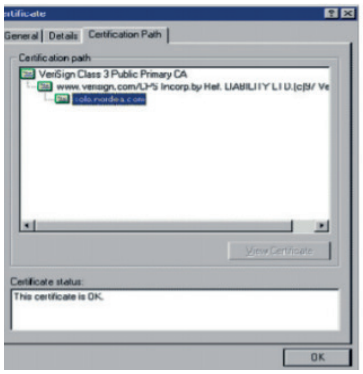
Brugeridentifikation
Brugerens identitet i Corporate Netbank verificeres ved brug af en identifikationsmetode:

- Nordea Koder app
- kortlæser uden kabel
- kortlæser med kabel

Den mobile enhed eller dit kort må ikke overdrages til andre brugere. Du bør kun indtaste login-oplysningerne, når du starter en sikker session af Nordeas Corporate Netbank.

Kontrollér, at der er en hængelås i browserens statuslinje eller til højre i browserens adresselinje. Hængelåsen bekræfter, at browseren har en krypteret forbindelse til Nordea. For at være helt sikker på, at forbindelsen er til Nordea, kan du klikke på hængelåsen (se Fig. 1).

Fig.1 Billedet kan se forskelligt ud afhængigt af browser og browserversion.



Sikker dataoverførsel via internettet
Den krypterede forbindelse (SSL-kryptering) sikrer, at data, der overføres mellem din browser og Nordea, hverken kan ses eller manipuleres af uautoriserede brugere.

Antivirusprogram
Virus og anden ondsindet software udgør en trussel for alle pc-brugere idag. Virus kan stamme fra e-mail eller downloades, mens du er på internettet eller via USB nøgler/andre flytbare medier. Sørg for altid at have et anerkendt antivirusprogram på din pc og kontrollér, at antivirusprogrammet har de seneste virusdefinitioner.

I tilfælde af et virusangreb skal du omgående kontakte din virksomheds it-ansvarlige og lade være med at bruge pc'en, før virussen er fjernet.

Internetbrowsere
Din browser og dens indstillinger har meget stor betydning for sikkerheden på din pc. Mens du er på internettet, kan din browser acceptere at afvikle eksterne programmer, men det bør ikke ske vilkårligt.

Vi anbefaler derfor, at du:
- bruger den seneste version af din internetbrowser
- indstiller browseren, så den beder dig om at acceptere overførsel af programmer fra pc'en til internettet eller omvendt
- kun downloader filer fra leverandører, som du kan stole på, når det gælder sikkerhed
- kun accepterer signerede ActiveX-kontroller (IE 11) og andre eksekverbare programmer fra pålidelige leverandører eller blokerer fuldstændigt for import
- som minimum bruger browserens standard sikkerhedsindstillinger.

Firewall

Du bør altid have en firewall som beskyttelse mod usikre netværk. Hvis din pc er koblet til virksomhedens lokale netværk, er der normalt en firewall mellem dette netværk og internettet. Denne firewall beskytter mod uautoriseret adgang til det lokale netværk fra internettet. Hvis du ikke har en firewall, fx hvis du bruger en standalone pc, anbefaler vi, at du installerer en personlig firewall på din pc og sikrer dig, at den kun tillader den nødvendige trafik.

For at få adgang til Corporate Netbank skal du åbne protokollen HTTPS på port 443 i din firewall. Du opnår det højeste sikkerhedsniveau ved kun at åbne for trafik UD gennem porten i din firewall og fx kun til Nordeas URL-adresse:
https://solo.nordea.com/nsc/engine.

Rapportér mistænkelige aktiviteter

Hvis du oplever unormal adfærd (fx lang logon-proces eller pop op-vinduer) eller mistænker sikkerheden generelt, så kontakt straks din administrator eller Nordea.

Spærring af adgang til Corporate Netbank

Hvis du har mistanke om, at andre har fået kendskab til din pinkode, eller din mobile enhed er bortkommet, skal du straks slette enheden i "Min profil" eller kontakte din administrator eller lokale Support.
Hvis du har mistanke om, at dit kort bliver misbrugt, skal kortet straks spærres. Kontakt din administrator eller lokale Support.

Ønsker du flere oplysninger om Corporate Netbank, kan du kontakte din lokale rådgiver i Nordea.