Corporate Netbank

Instruksjon om datasikkerhet

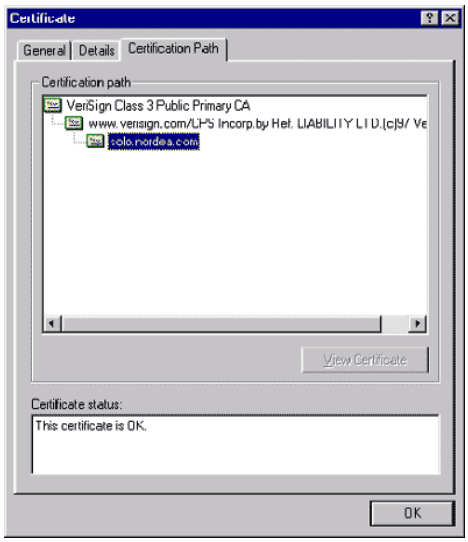
Sikker pålogging

Brukeridentifikasjon
Brukerens identitet kan verifiseres mot Corporate Netbank på følgende måter:

- Nordea eID med kabel
- Nordea eID uten kabel

Innloggingsinformasjonen er personlig. Chipkort må ikke gis til andre brukere.

Innloggingsinformasjonen må bare legges inn når du er på de sikre sidene i Nordeas Corporate Netbank. Se etter hengelåsen i nederste felt i nettleseren eller til høyre for adressefeltet i nettleseren. Hengelåsen er en bekreftelse på at nettleseren sender kryptert data til Nordea. For å være helt sikker på at dataene går til Nordea, klikk på hengelåsen og følgende bilde vises:



Sikre dataoverførslene via Internett
På grunn av krypteringen (SSL-kryptering) kan ikke dataene ses eller bli manipulert av en ikke-autorisert person når de overføres mellom nettleseren din og Nordea.

Antivirusprogram
Virus og andre ondsinnede programmer er en konkret trussel for alle PC-brukere i dag. Virus kan overføres fra en USB-enhet (eller andre flyttbare media), fra e-post eller kan lastes ned når du er inne på Internett.

Bruk alltid et anerkjent antivirusprogram på PC-en din.

- Sikre at programmet inneholder de siste antivirusfilene.
- Oppdages virus, må du kontakte den IT-ansvarlige eller IT-sikkerhet i bedriften med én gang og unngå å bruke PC-en til viruset er fjernet.

Hvordan dette bildet ser ut kan variere mellom de forskjellige nettleserne og nettleserversjonene.

INFORMASJON

For mer informasjon om Corporate Netbank, kontakt din kundeansvarlige i Nordea.

NORDEA.COM/CN

SNARVEIER

Mer informasjon om Nordea's cash management tjenester finner du her:

NORDEA.COM/CASHMANAGEMENT

NORDEA.COM/CN

FAKTA

Corporate Netbank tilbyr enkel og sikker tilgang til et vidt spekter av banktjenester og inneholder detaljert oversikt over likviditeten med saldo- og transaksjonsinformasjon i sanntid.

Nettlesere på Internett
Nettleseren og måten den er konfigurert på har også en stor innflytelse på sikkerheten på PC-en din. Blant annet når du er inne på Internett, kan nettleseren din akseptere å kjøre et eksternt program, men det bør ikke gjøres tilfeldig.

Du anbefales å:
- bruke den siste versjonen av nettleseren på Internett
- konfigurere nettleseren slik du blir bedt om å akseptere at et program overføres mellom PC og Internett
- bare laste ned filer fra leverandører som du kan stole sikkerhetsmessig på
- bare akseptere signerte applet-er, aktiveX-kontroller og andre innlastbare program fra pålitelige leverandører eller ikke tillate import i det hele tatt
- sette nettleserens standardsikkerhet som minimum.

Brannmur
Du bør alltid ha en brannmur som beskytter deg mot usikre nettverk. Er PC-en din koblet til bedriftens lokale nettverk, er det vanligvis en brannmur mellom det lokale nettverket og Internett. Brannmuren hindrer uautorisert tilgang til det lokale nettverket fra Internett.

Bruker du for eksempel en frittstående PC uten brannmur, vil vi anbefale deg å installere en personlig brannmur på PC-en din og sikre at bare den trafikken som er nødvendig tillates.

For å få tilgang til Nordeas Corporate Netbank må du åpne HTTPS-protokollen for port 443 i brannmuren. Høyest sikkerhetsnivå betyr å tillate kun utgående trafikk gjennom porten i brannmuren, for eksempel bare Nordeas URL-adresse:
https://solo.nordea.com/nsc/engine

Rapporter mistenkelig aktivitet
Dersom du opplever at nettbanken oppfører seg unormalt (f.eks unormalt lang responstid ved innlogging eller rare pop-up vinduer) ta kontakt med din administrator eller Support i Nordea.

Sperre tilgangen til Corporate Netbank
Har du mistet innloggingsinformasjonen eller har mistanke om misbruk, må kortet sperres øyeblikkelig, og et nytt kort må aktiveres.

Du kan sperre kortet og be om aktivering av nytt kort ved å kontakte Support i Nordea.