Corporate Netbank
Instruktioner för datasäkerhet

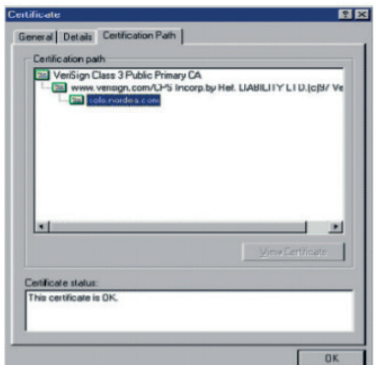
Säkerhetslösning
Användarens identitet verifieras mot Corporate Netbank med hjälp av något av följande:

- Nordea Koder-appen
- Svenskt Mobilt BankID
- Kortläsare utan sladd
- Kortläsare med sladd

Du får inte överlåta den mobila enheten eller ditt kort till någon annan användare. Försäkra dig om att du befinner dig på en säker sida som tillhör Corporate Netbank innan du anger din inloggningsinformation.

Titta efter ett hänglås i webbläsarens statusfält eller till höger om adressfältet i webbläsaren. Hänglåset betyder att webbläsaren har en krypterad tunnel till Nordea. Du kan kontrollera att tunneln går till Nordea genom att klicka på hänglåset (Se fig. 1)

Fig. 1
Bilden kan se lite olika ut beroende på vilken webbläsare du använder och vilken version webbläsaren har.



Säker dataöverföring via Internet
Tack vare den krypterade tunneln (SSL kryptering) kan informationen inte läsas eller manipuleras av någon obehörig när den sänds mellan din webbläsare och Nordea.

Antivirusprogram
Virus och annan skadlig programvara är ett konkret hot mot alla datoranvändare. Virus kan smitta via e-post-meddelanden, laddas ner automatiskt medan du surfar på internet eller via USB-minnen och andra flyttbara medier. Kör alltid ett erkänt antivirusprogram på din dator och se till att ditt antivirusprogram innehåller de senaste uppdateringarna.

Om du upptäcker en virusattack, kontakta genast ditt företags IT-avdelning eller IT-säkerhetsansvariga och undvik att använda datorn till dess att viruset avlägsnats.

Webbläsare
Konfigureringen av din webbläsare har stor betydelse för datorsäkerheten. Din webbläsare kan vara inställd för att acceptera att köra externa program, men detta bör inte ske urskillningslöst.

Vi rekommenderar att du
- använder den senaste versionen av din webbläsare
- konfigurerar webbläsaren så att du blir tillfrågad om du vill föra över program från datorn till internet, eller tvärtom

- endast laddar ner filer från leverantörer som du litar på

- endast accepterar ActiveX-kontroller (IE 11) och liknande från pålitliga leverantörer, alternativt avstår helt från importer

- som ett minimiskydd använder webbläsarens standardinställningar för säkerhet.

Brandvägg

Du bör alltid ha en brandvägg som skydd. Om din dator är ansluten till företagets lokala nätverk brukar det normalt finnas en brandvägg mellan det nätverket och internet. Brandväggen hindrar obehöriga från att ta sig in från internet. Om du saknar brandvägg, till exempel om du använder en fristående dator, rekommenderar vi att du installerar en personlig brandvägg på din dator och bara tillåter nödvändig trafik.

För att komma till Nordeas Corporate Netbank öppnar du protokollet HTTPS på port 443 i brandväggen. Högst säkerhetsnivå får du genom att endast öppna för utgående trafik, OUT, genom porten i brandväggen, och exempelvis bara till Nordeas URL adress: https://solo.nordea.com/nsc/engine.

Rapportera misstänkta aktiviteter

Om du upplever onormal aktivitet, (t.ex. lång inloggnings-process eller popup-fönster) eller har misstankar om säkerheten generellt, så kontakta din administratör eller Nordea omedelbart.

Spärra åtkomst till Corporate Netbank

Om du misstänker att din PIN-kod eller din mobila enhet har kommit på avvägar måste du kontakta din administratör eller Support. Om det gäller Nordea Koder-appen ska du omedelbart ta bort din mobila enhet i 'Min profil'.

Om du misstänker att ditt kort kan missbrukas måste kortet spärras. Kontakta din administratör eller Support.

För mer information om Corporate Netbank, vänligen vänd dig till din kontaktperson i Nordea.