Corporate Netbank

Instruktioner för datasäkerhet

Säker inloggning

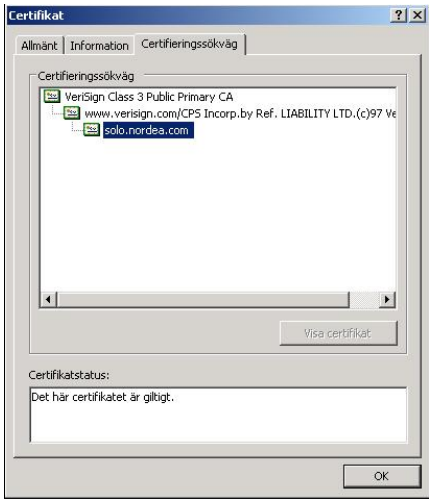
Säkerhetslösning
Användarens identitet verifieras mot Corporate Netbank antingen genom ett:

- Kortläsare med sladd
- Kortläsare utan sladd

Denna inloggningsinformation är personlig. Du får inte överlåta chipkortet till någon annan användare.

Inloggningsinformationen får bara anges sedan du försäkrat dig om att du befinner dig på en säker sida tillhörande Corporate Netbank. 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. Då ska nedanstående bild visas:



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

Antivirus-program
Virus och annan skadlig programvara är ett konkret hot mot alla datoranvändare. Virus kan smitta via USB-minnen (eller andra flyttbara medier), e-post-meddelanden eller laddas ner automatiskt medan du är ute på Internet.

- Kör alltid ett erkänt antivirusprogram på din dator.
- 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.

Bilden kan se lite olika ut beroende på vilken webbläsare du använder och vilken version.

INFORMATION

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

NORDEA.COM/CN

GENVÄGAR

Mer information om Nordeas Cash Management-erbjudanden hittar du på

NORDEA.COM/CASHMANAGEMENT

NORDEA.COM/CN

FAKTA

Corporate Netbank ger dig enkel och säker tillgång till ett flertal olika banktjänster och ger en helhetsbild av ditt företags likviditet med konto- och transaktions-information i realtid.

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 signerade appletar, ActiveX-kontroller 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 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 inloggningsprocess eller popup-fönster) eller har misstankar om säkerheten generellt, kontakta din administratör eller Nordea omedelbart.

Spärra åtkomst till Corporate Netbank
Om du har förlorat din inloggningsinformation eller av andra skäl befarar att kortet kan missbrukas måste kortet spärras omedelbart och ett nytt kort aktiveras. Kontakta Nordea så spärrar vi det gamla kortet och aktiverar ett nytt åt dig.
.