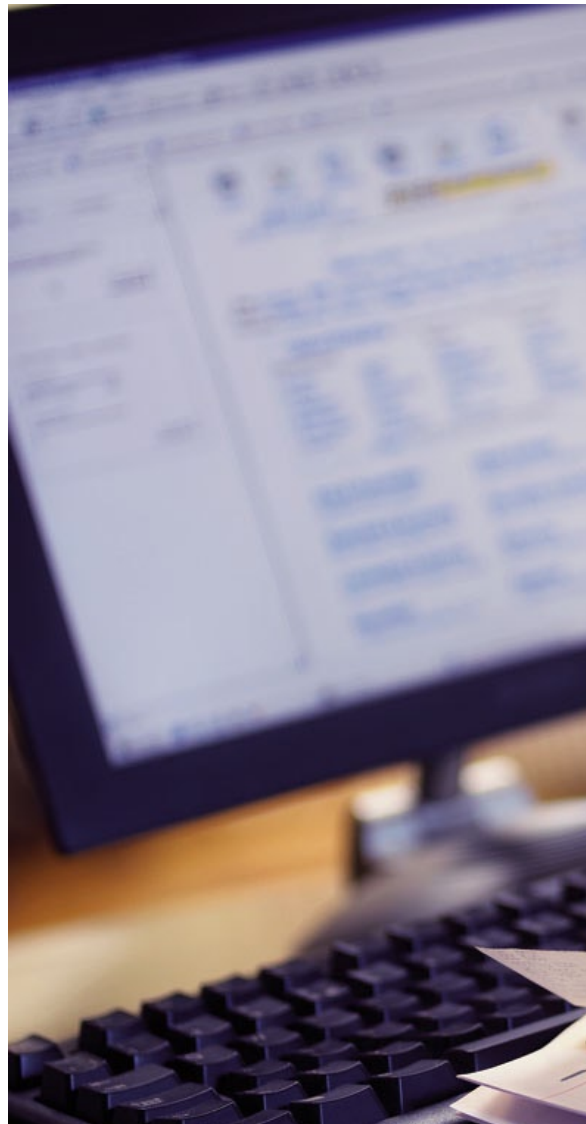
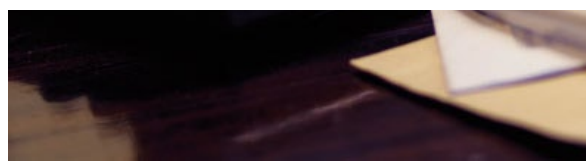


Internet- säkerhet och banktjänster

September 2007



Svenska Bankföreningen



Skydda din dator

Att använda Internet för att utföra bankärenden är enkelt och bekvämt. Men tänk på att din datormiljö måste vara skyddad och att du aldrig ska lämna ut personliga uppgifter som till exempel koder eller kortnummer till obehöriga.

Bankföreningen har sammanställt en kortfattad information om vad du som bankkund bör känna till för att känna dig trygg och säker när du använder Internet för att utföra bankärenden.

Så här skyddar du din dator

En dator som är uppkopplad mot Internet måste skyddas för att inte drabbas av virus eller angrepp, till exempel informationsstöld.

Det finns virus i form av programkod som kan installeras på din dator utan att du märker det, så kallade trojaner eller spionprogram. Sådan programkod kan till exempel komma via e-postmeddelanden från en okänd avsändare eller via besök på en bedräglig webbsida som i bakgrunden laddar ner spionprogram på användarens dator. En obehörig användare kan via sådan programkod stjäla information, avläsa tangentbordstryckningar eller till och med utnyttja din dator som en server via fjärrstyrning.

För att undvika problem är det mycket viktigt att använda ett uppdaterat virusskydd, antispiönprogram och brandvägg. Det är också viktigt att uppdatera datorns operativsystem och webbläsare. Dina leverantörer av programvaror samt Internet- och bredbandsoperatörer brukar tillhandahålla information om hur du skyddar din dator och din Internetuppkoppling. De flesta leverantörer av operativsystem och antivirusprogram har tjänsten automatisk uppdatering som innebär att när nya uppdateringar finns laddas de ner via Internet och installeras på din dator.

Vad är syftet med bankernas olika säkerhetslösningar?

Syftet med säkerhetslösningarna för banktjänster på Internet är att informationen om dina tillgångar och transaktioner inte ska vara åtkomlig för någon annan än dig själv. Bankernas säkerhetslösningar används dels för att säkerställa din identitet när du begär tillgång till din information och banktjänsterna, dels gör den det möjligt för dig att uttryckligen bekräfta för banken en begäran om att en transaktion ska utföras.

Hur fungerar bankernas säkerhetslösningar?

Bankerna i Sverige använder olika säkerhetslösningar för tillgång till banktjänster via Internet. Nedan förklarar vi kortfattat innebörden av de mest använda metoderna.

Personlig kod, engångskod

En personlig kod kan vara en kod du väljer själv eller en du blivit tilldelad. Koden är kopplad till exempelvis personnummer eller kundnummer. Personlig kod kan till exempel användas för att ge tillgång till ett begränsat urval av informationstjänster i Internetbanken.

Personlig kod kan kombineras med användning av engångskoder. Banken skickar då ut ett kodkort med koder. En kod används i samband med en be-

gåran att banken ska utföra en viss tjänst. Koden kan endast användas en gång och är sedan förbrukad. Banken skickar ut ett nytt kodkort innan det gamla är förbrukat.

Kodkortet är en värdefull handling som ska förvaras utan åtkomst för obehörig. Kodkort med tillhörande personlig kod bör heller aldrig förvaras tillsammans.

Säkerhetsdosa

En säkerhetsdosa har ett litet fönster och ett siffer-tangentbord. Den kan likna en liten miniräknare till utseendet. Dosan är personlig, vilket innebär att den är knuten till en viss innehavare genom exempelvis ett unikt kundnummer och kan endast användas med en PIN-kod. Med dosan framställs engångskoder som kan användas både för identifiering och för att verkställa uppdrag i Internetbanken. De engångskoder som framställs med säkerhetsdosa har mycket kort giltighetstid.

En säkerhetsdosa ska förvaras så att den inte är åtkomlig för obehörig och PIN-koden ska hållas hemlig.

Certifikat

Ett certifikat är en elektronisk ID-handling som innehåller personuppgifter om innehavaren. Certifikatet kan lagras, exempelvis på en dator eller i ett så kallat smart kort. Ett certifikat som lagras på en dator brukar benämnas mjukt certifikat eller filcertifikat. Ett certifikat som lagras på ett smart kort brukas benämnas hårt certifikat eller kortcertifikat.

Till ett certifikat hör en personlig nyckel som endast kan användas tillsammans med ett lösenord, som endast certifikatinnehavaren känner till. Genom att använda ett personligt lösenord aktiveras nyckeln och därmed kan en viss information ges ett kryptografiskt skydd. Certifikat används både för identifiering och för att verkställa uppdrag i Internetbanken. I samband med inloggning väljer innehavaren det certifikat som ska användas och anger lösenordet. Banken kontrollerar certifikatets giltighet och kan identifiera innehavaren. På motsvarande sätt kan innehavaren ange lösenordet för att skapa en elektronisk signatur, exempelvis i samband med att banken tar emot ett betalningsuppdrag.

Certifikat med tillhörande personlig nyckel ska förvaras utan åtkomst för obehörig och det lösenord som innehavaren har valt ska hållas hemligt.

Viktigt att känna till om falsk e-post och falska hemsidor

Phishing är ett samlingsbegrepp för en typ av bedrägerier där falska e-postmeddelanden och falska webbplatser används för att lura en person att lämna ut en hemlig uppgift.

Ett bedrägeriförsök kan innebära att du får ett e-postmeddelande som ser ut att komma från din bank. Meddelandet innehåller en uppmaning att klicka på en länk till en webbplats och där lämna vissa uppgifter, till exempel personnummer, kortnummer eller koder. Det kan vara mycket svårt att skilja den falska webbplatsen från din riktiga banks webbplats. Motivet till att du ska lämna uppgifterna påstås ofta vara att banken behöver verifiera vissa uppgifter för att du inte ska riskera att drabbas av ett bedrägeri.

I vissa fall kan mottagaren av ett e-postmeddelande uppmanas att lämna uppgifter genom att direkt svara på meddelandet. Det förekommer även att kunder har blivit kontaktade på telefon eller via så kallat chatforum på Internet och uppmanats lämna ifrån sig uppgifter.





Tänk på att:

- banken aldrig uppmanar sina kunder att via e-post lämna ut uppgifter som till exempel kortnummer eller koder
- inte svara på e-postmeddelande där du uppmanas lämna ut personliga och hemliga uppgifter och klicka inte på länkar i sådana meddelanden
- om du råkar klicka på en länk i ett sådant meddelande så använd aldrig en webbplats som öppnas via länken, inte ens om den liknar en "riktig" webbplats
- kontrollera att det är din banks riktiga webbadress som anges i webbläsarens adressfönster innan du loggar in till din Internetbank.
- när du har loggat in till din Internetbank ska webbadressen börja med https:// och en symbol med ett litet hänglås ska vara synlig i webbläsarens statusfält, ofta nederst på sidan
- följa din banks instruktioner och råd för Internetbanktjänster, bland annat om hur du kan kontrollera bankens säkerhetscertifikat.

Din bank frågar aldrig efter dina koder eller personliga uppgifter

Banken tar aldrig kontakt med dig via e-post eller telefon för att uppmana dig att lämna ut personliga uppgifter som till exempel kortnummer eller koder. Säkerheten i bankens tjänster bygger på att bankens egna system håller reda på nödvändig infor-

mation och att de hemliga koder eller lösenord som du använder endast är kända av dig. Det är alltså ologiskt att en bank skulle fråga efter sådana uppgifter.

I de fall du själv tar kontakt med din banks Internet-tjänst eller telefonbanktjänst gäller att du anger lösenord och koder enligt de instruktioner banken har lämnat för tjänsten. Det kan förekomma kontrollfrågor hos exempelvis bankens kundcenter, men bara då du som kund på eget initiativ kontaktat banken.

Så här hanterar du kort, koder, dosor, certifikat eller personliga uppgifter

Kort, koddosor, meddelanden med lösenord och certifikat är värdehandlingar. Det betyder att sådana handlingar eller uppgifter ska förvaras på en trygg och säker plats och på ett sådant sätt att de inte är åtkomliga för någon obehörig.

Tänk på att:

- aldrig låna ut dina kort, lösenord eller andra värdehandlingar till någon annan
- aldrig förvara en anteckning av ett lösenord så att den kan kopplas till ett kort, koddosa eller certifikat
- vara försiktig med i vilka miljöer du använder ditt kort, tänk på att uppgifterna på kortet kan leda till obehöriga uttag eller transaktioner på ditt konto om det kommer i orätta händer
- ett certifikat som är installerat på en dator ska inte kunna användas eller kopieras av någon annan person och det är viktigt att datorn är skyddad för obehörigt intrång, se "Så här skyddar du din dator"
- vara extra uppmärksam på hur du hanterar dina handlingar och uppgifter om du utför bankärenden från en dator i en publik miljö som till exempel ett Internetcafé. Var noga med att logga ut när du är klar med dina bankärenden.

Om du tror att du har råkat ut för ett bedrägeri - kontakta omedelbart din bank.

Om betalningar vid e-handel

Bankerna tillhandahåller betalningsprodukter som kan användas vid handel över Internet, så kallad e-handel.

Vissa lösningar bygger på att webbplatsen erbjuder en koppling till din banks Internetbank som innebär att köpet genererar en transaktion som kunden godkänner efter inloggning till Internetbanktjänsten. En sådan betalning brukar kallas direktbetalning eller e-betalning via bank.

En mera spridd betalningsform är att använda bank- eller betalkort vid köp över Internet. Det förekommer här att den kortutställande banken erbjuder en särskild lösning via Internetbanken, där kunden till befintligt kort kan erhålla ett temporärt kortnummer med begränsad giltighetstid. Det förekommer även andra lösningar där en personlig kod kopplas till kortnumret. Hör med din kortutställare vilka lösningar som finns tillgängliga för dig.

En del webbplatser erbjuder olika betalningsformer där du som kund har möjlighet att välja mellan till exempel direktbetalning, kortbetalning, postförskott eller betalning mot faktura.

Tänk på att:

- handla endast på webbplatser som är kända
- om du är osäker på om en webbplats är trovärdig så undersök om det finns referenser eller utvärderingar av en känd extern part
- aldrig lämna ut kortnummer på en oskyddad webbsida. En skyddad webbsida ska börja med https:// i webbadressfältet och en symbol med ett litet hänglås ska vara synlig i webbläsarens statusfält, ofta nederst på sidan
- studera webbplatsens instruktioner och säkerhetspolicy före köp.
- det alltid ska vara möjligt att via informationen på webbplatsen kunna kontakta företaget för personlig information och service.
- om du anser att du inte har genomfört ett köp som genomförts från ditt konto, kontakta omedelbart din bank.

