BODFORSS

Säkerhet och skydd mot bedrägerier för privatkunders bankkonton och bankkort

Analysledare: Sandra Thorsson
Thomas Kronberg
Hebbe Felten
Datum: 2023-05-08
Version: 1.2
Uppdragsgivare: Villaägarnas Riksförbund

1 INNEHÅLL

2 SAMMANFATTNING

Bodforss Consulting AB har på uppdrag av Villaägarnas Riksförbund genomfört en uppföljande granskning av ett antal bankers skydd mot bedrägerier riktade mot kunder som använder internetbanker och mobila bankappar. Den nya granskningen är något bredare och djupare än den tidigare undersökningen år 2021. Bodforss Consulting AB har likaledes på uppdrag av Villaägarnas Riksförbund år 2022 tagit fram rapporten ”Så kan bankbedrägerierna minska”, där vi bland annat beskriver hur bankerna kan höja säkerheten för kundernas bankkonton.

Vi har i den nya rapporten förutom säkerheten för bankkonton även undersökt vilka säkerhetsmekanismer bankerna har för kortköp, utifrån ett användarperspektiv, det vill säga vad kan kunderna själva styra över för att anpassa sin risknivå. En förkortad sammanställning av resultatet, finns i ett separat dokument.

Säkerhetsnivån hos bankerna är generellt på en bra nivå. BankID är i princip standard hos alla banker idag. De flesta banker har fortfarande kvar bankdosan, med vilken kunden kan logga in och signera i internetbanken eller mobilappen. De största nackdelarna med bankdosan, jämfört med Mobilt BankID, är att det inte är tydligt vad som godkänns i bankdosan.

Den autentiseringsmetod som är svårast för en bedragare att kringgå är, enligt vår bedömning, BankID på kort tillsammans med sladdansluten kortläsare, denna metod kan dock enbart användas på internetbanken i en dator. För mobila enheter är den säkraste metoden att använda Mobilt BankID på samma enhet som inloggningen sker på. Näst bäst är Mobilt BankID med QR-kod, där koden byts med korta intervaller.

BankID inför nya krav för säker start av BankID. Senast 1 maj 2024 måste bankerna enbart använda Mobilt BankID med QR-kod, där koden byts ofta eller Mobilt BankID på samma enhet som skall logga in. Start av BankID med personnummer kommer inte längre att tillåtas. BankID uppmanar sina kunder (bankerna) att ”*Uppdatera så snart som möjligt”*, vilket vi instämmer i. Man kan även konstatera att allt fler av de säkerhetshöjande åtgärder som omnämndes i vår rapport år 2022 nu återfinns hos bankerna.

De viktigaste råden till bankkunderna gällande deras säkerhet för digitala tjänster mot banken, är i stort sett samma som vid förra undersökningen. Kunderna kan förbättra sin säkerhetsnivå genom att undvika att använda sig av de mindre säkra autentiseringsmetoderna och om möjligt inaktivera funktioner de inte använder sig av. Bankkunderna ska aldrig lämna ut autentiseringsinformation till någon som uppmanar dem att göra det. Banken ringer aldrig upp och ber dig logga in på internetbanken eller mobilappen. Ett generellt råd är att alltid vara noga med att kontrollera vem du autentiserar dig mot eller vad du signerar. Bankkunder som blir lurade vid bankbedrägerier läser ofta inte igenom vad de godkänner med sitt BankID.

Konsekvenserna av att en bedragare kommer åt internetbanken blir större om offret har hela sitt bankengagemang på en bank. Bankkunderna kan precis som vi nämnt i 2022 års rapport begränsa sin skada om de skulle falla offer för en bedragare genom att inte lägga alla ägg i samma korg och binda upp sig som helkund hos en bank. Det här går att ta ytterligare ett steg längre, genom att utnyttja att det idag är i stort sett omöjligt för en bedragare att komma åt en bankkunds bankmedel på

nischbanker som bara erbjuder sparkonto, då dessa banker helt enkelt inte tillåter överföringar till annat än bankkundens egna konton på annan bank. Så att ha sina huvudsakliga bankmedel på en bank som inte tillåter annat än överföring till kundens egna konton och endast ha mindre bankmedel för den dagliga livsföringen i en bank med möjlighet till överföring till andra via Swish med mera, blir mycket bedrägerisäkert. En bedragare har då endast möjlighet att komma åt beloppen som finns på banken med överföringsmöjligheter till andra personer.

Den överföringsfördröjning på en bankdag som vi tog upp i vår rapport år 2022, är inget som bankerna har anammat och är därför inte heller något som bankkunderna kan göra inställning för på sina bankkonton. Det skulle i praktiken avsevärt ha kunnat försvåra många bankbedrägerier mot bankkonton där överföring är möjlig till andra personer, då det skulle ha gett mycket större möjligheter att stoppa transaktionerna. I synnerhet i kombination med begränsningar av vilka belopp som kan föras över till nya mottagare.

När det gäller inställningar för kortköp varierar inställningsmöjligheterna hos bankerna, om du har möjlighet att välja, skaffa bankkort i den bank vars inställningar för kortköp passar dig bäst. Har du redan ett bankkort, se till att utnyttja de inställningar din bank erbjuder för kortköp och välj att spärra det du inte behöver i din vardag och aktivera dem endast när du behöver dem.

3 INLEDNING

3.1 BAKGRUND

Detta är andra gången som vi på Bodforss Consulting fått förtroendet av Villaägarnas Riksförbund att granska skydd mot bedrägerier hos ett antal svenska banker. Den förra granskningen genomfördes 2021.

Vi har jämfört de olika bankernas metoder för att autentisera sina kunder och vilka ytterligare aktiviteter som krävs för att genomföra olika transaktioner i internetbanken och mobilappen. Vi har också bedömt vilka autentiseringsmetoder och övriga säkerhetsmekanismer som bäst står emot olika försök till bedrägerier. Utöver detta har vi granskat inställbara säkerhetsfunktioner som är kopplade till bankernas bankkort. Vi har analyserat de säkerhetsfunktioner som är tillgängliga för bankkunden att själv påverka.

3.2 OMFATTNING

Följande banker har granskats ur ett säkerhetsperspektiv:

- Swedbank (Swedbank AB)
- SEB (Skandinaviska Enskilda Banken AB)
- Handelsbanken (Svenska Handelsbanken AB)
- Nordea
- ICA Banken (ICA Banken AB)
- Länsförsäkringar bank (Länsförsäkringar Bank AB)
- Danske Bank

Vi har även granskat säkerhetslösningarna hos två nischbanker i något begränsad omfattning, då de inte har alla tjänster som finns hos bankerna ovan.

- IKANO Bank
- Avanza (Avanza Bank Holding AB)

Granskningen av inställbara säkerhetsfunktioner för bankkorten omfattar alla banker enligt ovan förutom Avanza (Avanza Bank Holding AB), eftersom de inte i dagsläget erbjuder bankkort till sina kunder.

3.3 AVGRÄNSNINGAR

Testerna har utförts under perioden 2023-03-23 till 2023-04-14 och resultat samt analyser beskriver vår bedömning av banksäkerheten under denna period. Testerna utfördes på ett urval av de tjänster bankerna erbjuder till privatpersoner.

Granskningen av bankkort omfattar huvudsakligen säkerhetsfunktioner i internetbanken och mobilappen som är kopplade till kundernas kort och kortfunktioner som kunden själv kan styra över.

Vi har inte säkerhetstestat internetbankerna genom att försöka utnyttja eventuella sårbarheter i kod eller i implementationen av säkerhetskontrollerna. Däremot har vi testat vanliga metoder som används av bedragare för att försöka kringgå säkerhetskontroller.

Vi reserverar oss för eventuella funktionsuppdateringar eller ändringar som gjorts av bankerna efter det att denna granskning genomfördes.

3.4 BEGREPP OCH FÖRKORTNINGAR

Autentiseringsenhet – Den dosa, telefon, eller kort som innehåller användarens hemliga nycklar och används för att identifiera användaren vid inloggning och signering.

Autentisering och elektronisk legitimering – Att identifiera sig som person med hjälp av en e-legitimation eller andra autentiseringsmetoder som bankdosa, lösenord och engångskoder. Elektronisk legitimering och autentisering är egentligen inte helt synonyma, men i denna granskning utgör legitimeringen oftast autentiseringen mot internetbanken och vi använder därför här begreppen synonymt. Vid inloggning med Mobilt BankID visas oftast texten ”*Jag identifierar mig hos XXX”,* vilket är samma som att du legitimerar dig.

Signering – Kan likställas med att skriva under med sin namnteckning (efter att ha legitimerat sig). Elektronisk signering använder sig av matematiska funktioner (kryptografiska algoritmer) som kombinerar indata som ska signeras med användarens hemlighet som finns lagrad i bankdosan eller BankID och räknar ut en svarskod som kan verifieras av banken.

BankID - Ett e-legitimeringssystem som är framtaget och förvaltas av Finansiell ID-Teknik BID AB. Används av 90% av Sveriges befolkning (18+ år)[1]. BankID finns i tre varianter: BankID på kort, BankID på fil och Mobilt BankID. BankID kan användas för att skapa engångskoder för legitimering (autentisering) och signering.

Kommentar angående BankID på fil: Generellt sett tillåter inte många av bankerna denna variant för att logga in i internetbanken, den kan användas för att uträtta ärenden och skriva under digitalt hos myndigheter och vissa företag. BankID på fil fungerar bara från den dator där den installerats i BankID säkerhetsprogram och kan inte flyttas. Alla banker utfärdar inte BankID på fil.

Bankkort – Kredit- eller debitkort som utfärdats av banken för kortbetalningar.

Kortläsare – En enhet som kan läsa smarta kort. Den kan vara utformad med eller utan knappsats och display och vara antingen fristående eller kopplas med sladd till dator. Kortet som stoppas i läsaren är det som innehåller användarens unika hemlighet som används för att skapa engångskoder och signaturer. Kortläsare kan användas antingen för att läsa ett BankID på kort eller för att kommunicera med certifikatet på ett bankkort. För användande av BankID på kort i kortläsare med sladd, krävs även att BankID säkerhetsprogram är installerat på datorn.

Bankdosa – En dosa som innehåller en unik personlig kryptografisk hemlighet som används för att skapa engångskoder och signaturer. Bankdosan benämns med olika namn beroende vilken bank du har.

PIN-kod – Personal Identification Number, en personlig hemlig kod som oftast består av siffror för att exempelvis låsa upp en bankdosa eller auktorisera en transaktion med ett kreditkort.

QR-kod – Quick Response kod, en slags tvådimensionell streckkod som kan innehålla olika information som en webbadress, eller transaktions-ID.

Kontrollkod – En slumpmässig sifferkod som ska användas av autentiseringsenheten för att skapa en svarskod med hjälp av hemligheten och en kryptografisk algoritm.

[1] https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2022/anvandning-av-internet-och-e-tjanster/#9-av-10-anvander-e-legitimation

TOTP – Time-based One-time Password, en algoritm som genererar en engångskod baserat på tidpunkten för när inloggningen påbörjades.

Mobilapp – En applikation för mobiltelefon eller surfplatta som banken har utvecklat för att kunden inte skall behöva logga in via webbläsaren för att få tillgång till deras internetbank.

NFC läsare – Near Field Communications (i dagligt tal ”blipp”), är en teknik som kan överföra data över korta sträckor. Används till exempel vid kontaktlös betalning med en mobiltelefon eller bankkort, eller för att läsa informationen på ett nationellt ID-kort eller pass.

Biometrisk autentisering – Biometrisk autentisering är en identifieringsmetod som baseras på de unika fysiologiska egenskaperna hos varje individ, som till exempel fingeravtryck eller ansiktsigenkänning.

Flerfaktorsautentisering (MFA) - Flerfaktorsautentisering innebär två eller fler faktorer behövs, dessa kan vara *någonting man vet* (till exempel lösenord och användarnamn), *någonting man har* (exempelvis digitalt certifikat eller en telefon), eller *någonting man är* (biometri som fingeravtryck eller ansiktsigenkänning).

Kontaktlös betalning – En kontaktlös betalning innebär att kunden bara behöver hålla sitt bankkort mot en kortterminal för att göra ett köp. Kunden behöver alltså inte stoppa in bankkortet i och slå koden för att bekräfta transaktionen. Se även NFC-läsare.

Säkert kortköp över internet – 3D Secure[2] är en säkerhetslösning för betalningar på internet som har tagits fram av kortnätverken Visa och Mastercard. Rent praktiskt innebär 3D Secure att kortkunden, utöver sina kortuppgifter, även måste verifiera sig med ytterligare ett sätt för att fullfölja sin betalning, exempelvis med ett lösenord eller med BankID.

Osäkert kortköp över internet – Köp som inte är säkrade med till exempel 3D Secure, det vill säga när kortköp tillåts utifrån den information som går att läsa på bankkortet.

CVC-kod – Card Verification Code är en säkerhetskod, bestående av tre siffror och anges på baksidan av bankkortet. Kunden kan behöva uppge koden vid till exempel internetköp. Genom att kunden uppger koden vet man att hen har tillgång till ett fysiskt kort.

Lösenordshanterare – Ett program för att hålla reda på komplexa och unika lösenord till olika system, där lösenorden skyddas av någon form av autentisering och stark kryptering.

[2] https://sv.wikipedia.org/wiki/3-D_Secure

4 SÄKERHETSANALYS AV AUTENTISERINGSMETODER

Samtliga banker i Sverige som vi har testat erbjuder flerfaktorsautentisering för sina internetbanker. Genom att använda sig av flera faktorer ökas säkerheten i autentiseringen och risken för stulna autentiseringsuppgifter minskar.

Vid ett fysiskt besök på ett bankkontor får du legitimera dig med fotolegitimation när du ska utföra transaktioner. Detta scenario kan likställas med en flerfaktorautentisering eftersom du visar upp din legitimation (*någonting du har*) och banktjänstepersonen verifierar att det är du på bilden (*någonting du är*). När du auktoriserar en transaktion signerar du med din namnteckning.

Bankdosan eller BankID kombinerar flera faktorer eftersom det är *någonting man har* och PIN-koden som är *någonting man vet*. För Mobilt BankID kan kunden välja att använda sig av biometri i stället för PIN-kod och då blir den andra faktorn *någonting man är* (fingeravtrycket eller ansiktet).

Varje faktor som används skapar ett visst mått av omak för den som ska autentisera sig och valet av faktorer måste därför vägas mot värdet av en starkare autentisering. När det gäller bankernas bedömning av vilken nivå av autentisering som krävs för internetbanken, har bankerna historiskt gjort olika riskbedömningar. På senare år har det skett en standardisering kring användandet av BankID och kanske främst Mobilt BankID för autentisering, även om de flesta bankerna stödjer flera olika autentiseringsmetoder. Flera banker har fortfarande kvar olika varianter av bankdosor och det skiljer sig fortfarande en del mellan bankerna vilken autentiseringsmetod de litar mest på.

Med korrekt användning är alla autentiseringsmetoder säkra, men mycket av säkerheten ligger i att utbilda kunderna om att skydda sina inloggningsuppgifter på ett bra sätt. Det breda utbudet av olika autentiseringslösningar, kan göra det svårare för kunder att förstå vad som är skyddsvärt. Vilket har gett upphov till bedrägerimetoder där offer luras att ”låna ut” engångskoder till bedragare som kapat kompisens Facebookprofil, eller liknande. Denna metod av bedrägeri har blivit ovanligare efter införandet av BankID.

Anledningen att det råder förvirring kring vad som är skyddsvärt är troligtvis att en bankkund kan ha svårt att förstå skillnaden på en personlig bankdosa och en kortläsare, där kortet innehåller hemligheten. Detta har drivit på bankernas säkerhetsarbete och man arbetar även med att utbilda kunderna, samtidigt som bankerna går mer mot att försöka knyta autentiseringsenheten till den enhet där kunden loggar in.

De äldre varianterna av bankdosor bygger antingen på att de genererar en tidsbaserad engångskod, skapar en engångskod av en kontrollkod, eller en kombination av båda. Svagheten kring dessa ligger i att de är helt frånkopplade från autentiserings- eller signeringsförloppet och det är dessa som historiskt varit utsatta för olika bedrägeriscenarion.

Mobilt BankID är i vissa fall skiljt från den enhet som kunden autentiserar sig på, men har fördelen av att skriva ut i klartext **vem** kunden identifierar sig mot eller **vad** kunden signerar. På senare tid har QR-koder börjat användas av fler och fler banker, för att kräva en närhet för mobilt BankID till den enhet som autentiseras. QR-koder kopplade till BankID innehåller en textsträng som påminner om en webblänk men som är menad för BankID och inte för webbläsaren (exempel: bankid://autostarttoken=f5adeda0-3e37-4558-92a9-f79124355058). QR kodens ”token” identifierar autentiseringssessionen unikt. För att försvåra för en bedragare att starta en autentiseringssession och vidarebefordra QR koden till offret är koderna bara giltiga några sekunder. Uppdateringstiden för QR-koden varierar hos bankerna från 1 till 30 sekunder.

Vid användning av Mobilt BankID i kombination med mobilapp eller mobilens webbläsare på samma enhet, visas aldrig QR-koden för kunden, i bakgrunden skickas däremot sessionsidentifieraren (token). Kunden autentiserar sig, i detta fall till synes sömlöst, med sin 6-siffriga kod eller med biometri. Att Mobilt BankID fysiskt är på samma enhet som inloggningen sker, är enligt vår bedömning jämförbart med BankID på kort när kortläsaren är ansluten med sladd.

Förutom flerfaktorautentisering, påverkar följande faktorer hur säker en autentisering är mot olika bedrägeriscenarior:

1. Att det är tydligt för kunden vem den identifierar sig mot och syftet med identifieringen eller vad man signerar, *synlighetsprincipen*.
2. Att det finns en fysisk koppling mellan autentiseringsenheten och enheten som loggas in, *närhetsprincipen*.
3. Att kontrollkod och svarskod har begränsad giltighet och inte kan återanvändas, *tidsaspekten*.

4.1 RANGORDNING AV AUTENTISERINGSMETODERS SKYDD MOT BEDRÄGERIFÖRSÖK

Rangordningen av autentiseringsmetoderna i denna rapport är till stor del densamma som vid förra säkerhetsgranskningen, men vi har utökat den något. Tanken är att många av begreppen är samma som tidigare och att det finns en igenkänningsaspekt, som ur ett konsumentperspektiv kan vara värdefullt.

Med bakgrund av ovanstående begrepp går det att rangordna olika autentiseringsmetoder som används i banksammanhang. Vi har rangordnat dem i stigande ordning från de med sämst skydd mot bedrägliga metoder, till de som är svårast att kringgå för en bedragare. Autentiseringsmetoder med minst skydd är inte osäkra, men de kräver att användaren tar ett större ansvar för att skydda dem mot obehöriga.

4.1.1 Minst skydd

- Lösenord eller lösenfraser
- Utskrivna engångskoder (kodkort, återställningskoder)
- Skrap-kort

Lösenord eller lösenfraser ger det sämsta skyddet mot bedragare eftersom människor ofta själva synkroniserar lösenord mellan olika tjänster. Det är också relativt lätt att lura en kund till att avslöja sitt lösenord genom bedrägliga epostmeddelanden och falska internetsajter. Dessutom har lösenord ofta väldigt lång giltighetstid. För att skydda känsliga konton ska lösenord aldrig återanvändas för olika tjänster. Lösenord ska endast användas tillsammans med en annan verifieringsmetod, en så kallad tvåfaktorsautentisering. En lösenordshanterare som skapar slumpmässiga och svåra lösenord är bra att använda där lösenord är den enda metoden för autentisering.

Utskrivna engångskoder används i väldigt liten utsträckning men kan vara ett komplement till andra metoder för autentisering eller som reservmetod i de fall kunden har tappat bort sin mobiltelefon. Kunden måste dock själv skydda engångskoderna väl från obehöriga. Den största bristen med utskrivna engångskoder eller skrap-kort med koder är att koderna är giltiga tills de har använts eller tills en senare kod i listan används. Detta medför att om en bedragare kommer över engångskoderna är det ingen tidspress att använda dem.

Tidsaspekten, det vill säga bedragarna saknar tidspress om de kommer över lösenord eller utskrivna engångskoder gör att dessa metoder måste anses ha lägst skydd mot bedrägerier.

4.1.2 Medelbra skydd

- Tidsbaserade engångskoder (TOTP, Microsoft Authenticator, Google Authenticator)
- Bankdosa
- Kortläsare utan sladd
- Mobilt BankID utan QR-kod

Tidsbaserade engångskoder, antingen genererade av en applikation eller en bankdosa, är en relativt säker metod för att skapa en tvåfaktorsautentisering. Även bankdosor, kortläsare och Mobilt BankID är säkra om hanteringen av dem sker på ett säkert sätt. De saknar dock *närhetsprincipen* eftersom autentiseringsenheten är helt frikopplad från den enhet (dator, telefon eller surfplatta) som användaren loggar in på.

En av bristerna som identifierats är att tidsbaserade engångslösenord och genererade engångslösenord från kontrollkoder saknar *synlighetsprincipen*. Det kommer sig av att de saknar koppling till vad det är kunden identifierar sig mot eller signerar. Denna brist kan utnyttjas av en bedragare som utger sig för att agera för bankens räkning och kunden kan luras att lämna ifrån sig koder som i sin tur kan användas för inloggning och signering. Bankerna informerar tydligt för kunderna att när de exempelvis signerar en transaktion med belopp ska kunden kontrollera att beloppet är korrekt. Under ett telefonsamtal kan en bedragare lura kunden att signeringen bara är en identifiering. Kunden luras att signera koden 2152 2391 som i själva verket kan vara en signering för en transaktion på 215 223 kronor och 91 öre.

Användningen av ett Mobilt BankID är ett något bättre alternativ. Det är på grund av *synlighetsprincipen*. Det medför att det framgår av visad text i Mobilt BankID vem kunden identifierar sig för eller vad det är som signeras. Det finns dock ändå en risk att kunden kan luras att signera transaktioner genom att bedragaren skapar en stressituation i signeringsögonblicket.

Vid inloggning med Mobilt BankID hos många av bankerna i testet, visas enbart texten ”*Jag identifierar mig hos XXX”,* där XXX motsvaras av bankens namn. Några av bankerna visar ytterligare text som beskriver syftet med identifieringen, "*Min avsikt: Inloggning i Internetbanken*".

Att tydligt visa syftet med kundens identifiering borde göra det svårare för en bedragare som uppger att den ringer ifrån kundens bank och försöker lura kunden att identifiera sig, med uppsåtet att logga in bedragaren i internetbanken.

4.1.3 Bra skydd

- Mobilt BankID med QR-kod
- Kortläsare med QR-kod

Dessa metoder har ett något starkare skydd mot bedragare, eftersom de kombinerar styrkorna från gruppen innan med *närhetsprincipen* genom en koppling till den enhet där kunden försöker logga in. QR-koden säkerställer förvisso inte fysisk kontakt, men ger ändå en ytterligare försäkran om att kunden som försöker logga in har autentiseringsenheten (mobiltelefonen eller kortläsaren för QR-kod) i närheten.

QR-koderna för Mobilt BankID har en relativt kort livslängd, som varierar mellan 1-30 sekunder hos bankerna. Uppdateringen av QR-koder ihop med kortläsare är betydligt längre än 30 sekunder hos vissa av bankerna, vilket är negativt för säkerheten. Vid förra testet skickades QR-koden med epost till en annan person för att dela på autentiseringsenhet och inloggningen. Det var möjligt i de fall QR koden var giltig i 30 sekunder, men förutsatte att den som tog emot koden vara beredd och snabb. Det bedömdes då som osannolikt att det skulle fungera i ett bedrägeriscenario, men vi vill ändå

rekommendera de banker som använder metoden att uppdatera QR koden med så kort tidsintervall som möjligt.

Det finns en viss risk för bedrägeri även vid användande av QR-kod som uppdateras mer frekvent, om bedragaren ”livestreamar” QR-koden från sin dators inloggningsförsök i offrets internetbank. Visas den ”livestreamade” QR-koden på ett trovärdigt sätt på offrets dator och luras offret att skanna den och identifiera sig mot banken, kommer bedragaren att få tillgång till offrets internetbank.

Vi gjorde ett förenklat test av ovanstående princip med ”livestreaming” av QR-koden, med syfte att påvisa att det går att kringgå *närhetsprincipen*. Vi skapade ett videosamtal mellan två mobiltelefoner, där QR-koden filmades från datorskärmen med hjälp av den ena mobiltelefonen och visades på den andra mobiltelefonens skärm. Genom användande av Mobilt BankID på en tredje telefonen skannades QR-koden från den andra mobiltelefonens skärm och autentiserades. Inloggningen till internetbanken på datorn där QR-koden ursprungligen visades blev godkänd.

4.1.4 Bäst skydd

- Kortläsare med sladd (BankID på kort)
- Mobilt BankID på samma enhet

Dessa metoder har det starkaste skyddet mot bedragare, eftersom *närhetsprincipen* är garanterad genom att det finns en direkt fysisk koppling till den enhet där kunden försöker logga in.

Starkast skydd mot bedrägerier på distans, har BankID på kort i kortläsare med sladd till datorn. Den fysiska kontakten mellan kortläsare och dator, gör att det i princip är omöjligt för en bedragare på distans att lyckas med att logga in i sitt tilltänkta offers internetbank. Den enda möjligheten blir då att fjärrstyra offrets dator.

För mobila enheter är den säkraste metoden att använda Mobilt BankID på samma enhet som inloggningen sker på. Den fysiska kontakten säkerställs genom att Mobilt BankID och applikationen där man autentiserar sig befinner sig på samma enhet, principen blir på samma sätt som ovan gällande kortläsare med sladd.

4.2 Kommande säkerhetshöjning av BankID-tjänster

Tjänsterna som BankID erbjuder bankerna gällande bankkundernas identifiering och signering, kommer under 2023 delvis förändras, med syftet att höja säkerheten mot bedrägerier.
Det innebär att en del av de mindre säkra BankID-tjänster, som bankerna fortfarande använder, kommer att tas bort, exempelvis Mobilt BankID utan QR-kod på annan enhet.

BankID uppger följande på sin hemsida riktat mot företag och myndigheter[3]:

*”För att skydda både användare och e-tjänster blir säker start av BankID tvingande för samtliga myndigheter, företag och organisationer som använder BankID i sina e-tjänster. Uppdatera så snart som möjligt, senaste datum för att ha ändringarna i bruk är **1 maj 2024**.”*

Säker start innebär tre krav:

1. **Rörlig QR-kod för BankID på annan enhet.** (Finns redan idag)
   Används när kunden besöker bankens tjänster på en dator, men identifierar sig med BankID på en annan enhet. En rörlig QR-kod förhindrar att bedragare kan lura till sig en stillbild av koden och använda för bedrägerier.

[3] https://www.bankid.com/foretag/saker-start

2. **Autostart för BankID på samma enhet.** (Finns redan idag)
   Används när kunden besöker bankens tjänster på samma enhet som den har Mobilt BankID på. Från bankens tjänst direktstartas BankID-appen utan mellansteg, vilket gör det säkrare eftersom det minskar risken att bedragare kan utnyttja mellansteget för att lura kunderna.
3. **Uppdatering till version 6 av BankID API.** (Versionen lanseras under våren 2023)
   Innebär att en start av BankID med personnummer inte längre kommer att stödjas. Det är en viktig åtgärd som sänker risken för bedrägerier och höjer säkerheten ytterligare.
   De e-tjänster som idag använder personnummerstart vid telefonidentifiering när kunden ringer banken samt vid kortbetalningar behöver också anpassas till:
   - Nytt gränssnitt för telefoni-identifiering med BankID när kunden ringer banken (tillgängligt våren 2023).
   - Nytt gränssnitt för kortbetalningar (tillgängligt hösten 2023).

4.3 ÖVRIGA METODER

Banker kan höja säkerheten för bankkundernas bankmedel med ytterligare autentiseringsmetoder, men även på andra sätt. Exempel på detta är att begränsa överföringar till nya mottagare, inställningsbar överföringsfördröjning vid överföring till andras bankkonton, tidsbaserade funktions- och beloppsgränser, förstärkt identitetskontroll vid hög risk med mera.[4]

[4] Kapitel 4, ” Så kan bankbedrägerierna minska”, Rikard Bodforss, Bodforss Consulting, 2022

5 TESTFÖRFARANDE

Vi har jämfört nivån på de säkerhetskontroller som finns på plats för att skydda kunderna från bedrägeriförsök genom att ta fram olika testfall. För att kunna åstadkomma detta har vi använt ett flertal mobiltelefoner, surfplattor och datorer i kombination med BankID, bankdosor och kortläsare utfärdade av bankerna. Utöver detta har vi inhämtat information via kundtjänst och respektive banks hemsida. Utgångspunkten i bedrägeriscenariot har varit att en tänkt bedragare inte har fysisk närhet till enheten som används för att autentisera offret.

För Testfall 6, genomfördes kontrollen av bankkortens säkerhetsfunktioner gällande kortköp, genom att logga in på respektive bank och kontrollera vilka inställningsmöjligheter som finns. Utöver detta inhämtade vi information via kundtjänst och respektive banks hemsida.

5.1 TESTFALL 1 – ÅTKOMST TILL INTERNETBANK

Utvärdera hur svårt det är för en bedragare att få tillgång till offrets internetbank genom att försöka ansluta till internetbanken från en annan dator eller mobil enhet som inte innehåller eller är kopplad till autentiseringsenheten.

Utvärderingskriterier:
Vi har undersökt om det går att autentisera en inloggning till internetbanken på dator, surfplatta eller mobil från en annan enhet än den som inloggningen sker på. Vi har även tittat på vilka autentiseringsmetoder som tillåts och redovisat skillnader. Vidare har vi värderat säkerheten på respektive autentiseringsmetod, till exempel hur länge är QR-kod giltig innan den byts ut och hur tydligt det är för användaren vad som sker.

Finns det några sätt att runda säkerhetskontrollerna som skall förhindra att fel person legitimeras?

När en inloggning har påbörjats och väntar på autentisering och en ny inloggning påbörjas från annan enhet, hur hanteras detta vid autentiseringen?

Finns det möjlighet för användaren att spärra oönskade inloggningsmetoder, till exempel användarnamn med lösenord/kod?

5.2 TESTFALL 2 – ÖVERFÖRING AV TILLGÅNGAR

Vilka tekniska kontroller finns på plats för att begränsa bedragarens möjlighet att föra över tillgångar från offret efter att ha kommit in på internetbanken.

Utvärderingskriterier:
Hur många identifikationer/signeringar krävs för att föra över pengar till ny mottagare?
Presenteras vad användaren godkänner vid en signering?
Finns det några begränsningar i vad som tillåts baserat på olika metoder för identifiering/signering?
Har banken ytterligare skyddsåtgärder?
Vilka beloppsgränser gäller vid transaktion till annat konto?

5.3 TESTFALL 3 – SKAPA NYTT BANKID

Ett skräckscenario är när en bedragare lyckas utfärda ett nytt mobilt BankID i offrets namn till en egen enhet. Detta BankID kan bedragaren sedan använda för att agera som offret utan att behöva lura av offret fler koder. Ett nytt BankID kan användas hos alla aktörer som godtar BankID, exempelvis andra banker.

Utvärderingskriterier:
Utfärdar banken BankID?
Vad krävs i så fall för att skapa ett nytt BankID?
Skickas meddelande till innehavaren om nytt BankID skapas/aktiveras?
Finns det några ytterligare skyddsmekanismer för att stoppa bedrägerier?

5.4 Testfall 4 – Kontroll utloggningstid vid inaktiv inloggning

Hur lång tid är en inloggad användares session aktiv om det inte sker någon aktivitet i sessionen. Scenariot är att användaren glömt att logga ut vid användande av en publik dator och då skulle någon annan kunna komma åt uppgifter ifrån användares internetbank. Skulle den obehöriga personen även kunna förstöra något för användaren?

Utvärderingskriterier:
Hur lång tid är en inaktiv session aktiv?
Vilken skada kan en person göra om den får tillgång till en aktiv session hos internetbanken utan att behöva autentisera sig igen eller signera något?

5.5 Testfall 5 – Bedrägeridetektion

Har banken någon detektion av ovanliga beteenden hos användaren och vidtas i så fall någon åtgärd från banken för att aktivt förhindra ett misstänkt bedrägeri?

Utvärderingskriterier:
Vi har i första hand genom att ställa frågor till bankerna försökt få fram relevant information. I de fall vi inte fått några svar har vi undersökt genom praktiska tester.

Tillåts inloggning på flera olika enheter samtidigt?

Påverkar avbrutna inloggningar (BankID verifieringarna) möjligheten att logga in (OBS! Ej användande av felaktig kod till själva BankID-enheten)?

Vi har också testat att lägga upp transaktion och godkänna den (transaktionen behöver inte genomföras, utan kan återkallas efter testet):

- med högt belopp, till nytt konto i annan bank
- med högt belopp, till eget konto i annan bank
- med högt belopp till flera nya konton andra banker
- med lägre belopp till flera nya konton andra banker

5.6 Testfall 6 – Säkerhet kortköp ur ett användarperspektiv

Vilka säkerhetsmekanismer kan användare själva styra gällande säkerheten för sitt kort?

Utvärderingskriterier:
Vilka säkerhetsfunktioner kan en användare själv styra över, till exempel aktivera kort för köp över internet eller ej, beloppsgränser och regionsspärrar.

Resultaten av de olika testfallen vägs samman med eventuella kompenserande kontroller för att göra en helhetsbedömning.

6 ANALYS AV TESTRESULTAT - TESTFALL 1-5

6.1 SWEDBANK

Begreppet bankdosa motsvaras av säkerhetsdosa hos Swedbank.

6.1.1 Testfall 1 Åtkomst till internetbanken

Vid inloggning i internetbanken krävs det att kunden använder Mobilt BankID med QR-kod, bankdosa eller BankID på kort. QR-koden som används vid inloggning byts varje sekund.

När det gäller inloggning i mobilappen krävs Mobilt BankID installerat på samma enhet eller bankdosa.

När kunden loggar in med Mobilt BankID visas följande:

"Jag identifierar mig hos Swedbank och Sparbankerna. Min avsikt: Inloggning i Internetbanken. Tänk på! Banken kommer aldrig ringa för att be dig logga in. Har du blivit uppringd? Avbryt och avsluta genast samtalet och ring till Digital Support."

Om en inloggning har påbörjats och väntar på autentisering och en ny inloggning påbörjas från en annan enhet avbryts båda inloggningsförsöken och ett felmeddelande kommer upp. Kunden får aldrig chansen att skanna QR-koden som kommer upp.

Det finns ingen möjlighet att spärra vissa inloggningsfunktioner som kunden eventuellt inte vill använda sig av.

6.1.2 Testfall 2 Överföring av tillgångar

Det krävs två signeringar för att föra över pengar till en ny mottagare. En signering för att lägga till den nya mottagaren och ytterligare en signering för att utföra själva överföringen till den nya mottagaren.

Vid signering av överföring med Mobilt BankID presenteras:
Ny mottagare: *"Jag godkänner att en ny överföringsmottagare läggs till. Konto, Namngett till KONTONAMN"*

Vid överföring: *"Jag godkänner följande överföringar: - KONTONAMN, belopp"*

Vid användande av bankdosa syns det inte i bankdosan vad kunden signerar, vilket kan vara en säkerhetsrisk.

Vid inloggning med Mobilt BankID går det enbart att signera överföringar med Mobilt BankID, inloggning med Bankdosa har motsvarande princip att det går endast att godkänna överföringar med Bankdosan.

Swedbank har något som de kallar för *utökad användning av Mobilt BankID,* som ger kunden tillåtelse att: *Lägga till betalningsmottagare, Lägga till autogiron, Ändra beloppsgränsen för Swish.*

Om kunden inte har utökad användning av Mobilt BankID, kan kunden använda sin bankdosa eller använda ett kodkort med engångskoder, för att lägga till och aktivera utökad användning av Mobilt BankID.

I internetbanken och mobilappen kan kunden föra över pengar och betala räkningar på upp till 999 999 kronor per signering, även till en helt ny mottagare. Behöver kunden betala eller föra över mer pengar kan kunden dela upp beloppet i flera betalningar eller överföringar.

Ytterligare skyddsåtgärder har inte identifierats.

6.1.3 Testfall 3 Skapa nytt BankID

För att ansöka om ett BankID krävs inloggning med bankdosa eller med befintligt Mobilt BankID. Om kunden saknar Mobilt BankID sedan tidigare kan kunden ansöka om ett, antingen med ett giltigt pass eller nationellt ID, då måste den mobila enheten ha en fungerande och aktiv NFC-läsare. Kunden får en notis från BankID mobilappen om att ett nytt BankID har skapats med information om namn, datum och tid.

När ansökan om BankID är godkänd behöver kunden aktivera det nya BankID med QR-kod samt uppge en ny PIN-kod för det. Nytt BankID kommer då att ersätta det gamla på den aktuella enheten.

6.1.4 Testfall 4 Kontroll utloggningstid vid inaktiv inloggning

Banken har en inaktivitetstid som är fem minuter. Efter tre minuter kommer det upp en varningsruta som räknar ner från två minuter och sedan loggas kunden ut automatiskt om ingen aktivitet görs.

Väl inloggad i internetbanken kan du föra över pengar mellan egna konton utan ytterligare signering, samt köpa eller sälja fonder och aktier.

6.1.5 Testfall 5 Bedrägeridetektion

Inloggning tillåts inte på flera enheter samtidigt. Vid inloggning i ytterligare en enhet blir kunden direkt utloggad ur den första enheten.

Test med att avbryta flera inloggningar i rad, påverkar inte en senare genomförd inloggning. Transaktioner upp till 999 999 kronor går bra att signera till en ny mottagare och verkar inte trigga någon ytterligare säkerhetskontroll.

6.1.6 Omdöme – betyg 4 av 5 och bäst i test

Det är bra ur säkerhetssynpunkt att Mobilt BankID utan QR-kod på annan enhet inte tillåts som inloggningsmetod. QR-koden uppdateras ofta, vilket också är bra.

Kunden kan inte vara inloggad på internetbanken samtidigt olika enheter, vilket minskar risken för att kunden glömmer logga ut en enhet, som andra kan komma åt.

Det är också bra att nya mottagare måste signeras innan man kan föra över pengar till dem, men det finns inga beloppsgränser utöver de generella när väl en mottagare är signerad och tillagd.

När kunden loggar in med Mobilt BankID visas förutom standardtexten *"Jag identifierar mig hos Swedbank och Sparbankerna."* även texten *”Min avsikt: Inloggning i Internetbanken*”, vilket är positivt ur säkerhetssynpunkt.

Banken är även tydlig med den information som presenteras för kunden vid signeringar, vilket är bra.

Inaktivitetstiden innan kunden blir utloggad är 5 minuter, vilket är bra.

6.2 SEB

Begrepp bankdosa motsvaras av digipass hos SEB.

6.2.1 Testfall 1 Åtkomst till internetbanken

Vid inloggning i internetbanken krävs det att kunden använder Mobilt BankID med QR-kod, BankID på kort med kortläsare ansluten till datorn eller bankdosa där inloggning sker med personnummer och koder. QR-koden som används vid inloggning byts varje sekund.

Inloggning i mobilappen kräver att ett Mobilt BankID är installerat på samma enhet eller en bankdosa.

När kunden loggar in med Mobilt BankID visas följande:
"Jag identifierar mig hos SEB".

När en inloggning i mobilappen har påbörjats och väntar på autentisering och en ny inloggning påbörjas från annan enhet går det bra att slutföra bägge inloggningarna. Om en inloggning i internetbanken har påbörjats och väntar på autentisering och en ny inloggning påbörjas i internetbanken blir bägge inloggningarna avslutade.

Om inloggning i internetbanken och mobilappen påbörjas samtidigt blir det begränsad funktionalitet i mobilappen och internetbankens inloggning avslutas.

Eftersom banken inte har Mobilt BankID utan QR-kod som inloggningsmetod, bedömer vi risken för att en bedragare lyckas lura kunden vid samtidig inloggning i internetbanken som liten.

Det finns ingen möjlighet att spärra vissa inloggningsmetoder som användaren eventuellt inte vill använda sig av.

6.2.2 Testfall 2 Överföring av tillgångar

Banken kräver inte signering för att lägga till en ny mottagare. Däremot krävs det en signering vid överföring till en ny mottagare. Det går även bra att ange ett kontonummer direkt. Är det flera upplagda överföringar läggs de i en lista där överföringarna kan signeras tillsammans.

I vissa fall kan banken kräva att kunden även verifierar en överföring med en SMS-kod som skickas till kundens registrerade mobilnummer. Till exempel kan det vara en ovanligt stor överföring som kunden inte brukar göra särskilt ofta. Detta leder till en extra verifiering. De exakta villkoren som styr detta kan eller vill SEB kundtjänst inte uppge. Denna typ av extra verifiering försvårar ett bedrägeri avsevärt.

Vid signering av överföring med Mobilt BankID och BankID på kort, presenteras följande för kunden:
”Jag skriver under hos SEB. Jag godkänner de här uppdragen, Antal uppdrag, Totalbelopp,
Från konto, Mottagare, datum, belopp

Tänk på! Banken kommer aldrig ringa dig för att be dig skriva under något, Har du blivit uppringd? Avbryt och avsluta genast samtalet och kontakta SEB”

Om det är flera uppdrag i listan som ska godkännas, måste alla uppdrag skrollas igenom, innan kunden kan signera.

Det går enbart att signera en överföring med samma metod som använts vid inloggningen, exempelvis vid inloggning med bankdosa går det endast att godkänna överföringar med bankdosan.

Är kunden inloggad med bankdosa eller Mobilt BankID kan kunden göra överföringar och internationella betalningar på högst 150 000 kronor. Begränsningen gäller per dygn och per typ av transaktion. För svenska betalningar är gränsen 1 miljon kronor. Behöver kunden överföra mer än vad gränsen tillåter måste den vara inloggad med BankID på kort.

6.2.3 Testfall 3 Skapa nytt BankID

För att skapa ett BankID behöver kunden ha en bankdosa eller ett befintligt BankID och använda sig av internetbanken. Kunden kan behöva verifiera sin identitet en extra gång genom att skanna och blippa sitt svenska pass eller nationella ID-kort.

Det går att förnya ett BankID om kunden är inloggad i internetbanken med ett befintligt BankID eller med bankdosan. En engångskod skickas till kundens registrerade mobilnummer innan kunden kan signera en beställning av ett nytt Mobilt BankID. En QR-kod skannas med den mobila enhet som nytt Mobilt BankID skall installeras på.

Första gången kunden loggar in på internetbanken med mobilt BankID behöver det verifieras med hjälp av en engångskod via SMS, med befintligt BankID eller med bankdosan. Detta gäller oavsett om det nya BankID har utfärdats av SEB eller någon annan bank.

Vid vårt test att skapa ett nytt mobilt BankID fick vi ingen avisering från banken när ett nytt Mobilt BankID hade skapats, men om notiser är aktiverade i Mobilt BankID appen meddelas om du har ett befintligt BankID sedan tidigare.

Om kunden saknar bankdosa eller befintligt BankID behöver kunden boka ett möte för att få hjälp av banken för att skapa ett nytt BankID.

6.2.4 Testfall 4 Kontroll utloggningstid vid inaktiv inloggning

Banken har en inaktivitetstid som är fem minuter.

Väl inloggad i internetbanken kan du köpa eller sälja aktier samt ta bort överföringsuppdrag utan ytterligare signering. Det går även att lägga till nya sparade mottagare eller ändra kontonummer till de mottagare som redan sparats utan att autentisering krävs. Det går även att byta kontonummer till en registrerad mottagare och behålla dess namn, gäller både för betalningsmottagare och överföringsmottagare.

6.2.5 Testfall 5 Bedrägeridetektion

Inloggning tillåts vanligtvis inte på flera enheter samtidigt i internetbanken hos SEB. Det går dock i vissa lägen att logga in i två webbläsare på olika enheter samtidigt, exempelvis genom att vara inloggad på samma Microsoft-konto på de olika enheterna, vilket inte nämnvärt borde påverka risken för bedrägeriförsök.

Test med att avbryta flera inloggningar i rad, påverkar inte en senare genomförd inloggning.

Vid transaktioner kan banken kräva att kunden även verifierar med en SMS kod som skickas till kundens registrerade mobilnummer. Till exempel kan det vara en ovanlig överföring som kunden inte brukar göra, som leder till denna extra verifiering. Kundtjänst kan inte upplysa om de villkor som styr detta.

6.2.6 Omdöme – betyg 4 av 5

Det är bra ur säkerhetssynpunkt att Mobilt BankID utan QR-kod på annan enhet, inte tillåts som inloggningsmetod. QR-koden uppdateras ofta, vilket också är bra.

Det går bra att vara inloggad på olika enheter samtidigt, men det kan vara en viss säkerhetsrisk om kunden glömmer logga ut en enhet, som andra kan komma åt.

Banken är tydlig med den information som presenteras för kunden vid signeringar, vilket är bra.

Vi tycker att det är märkligt att det finns möjlighet att ändra en sedan tidigare sparad mottagares kontonummer **utan** att kunden måste signera ändringen. Det skulle potentiellt kunna användas i bedrägligt syfte om en bedragare får tillgång till internetbanken.

Banken kräver en extra verifiering vid ”ovanliga” överföringar vilket är mycket bra och vi tycker också att den extra verifieringen av nya BankID är föredömlig.

Inaktivitetstiden innan kunden blir utloggad är 5 minuter, vilket är bra.

6.3 HANDELSBANKEN

6.3.1 Testfall 1 Inloggning

Vid inloggning i internetbanken krävs det att kunden använder Mobilt BankID med QR-kod eller kortläsare som är ansluten till datorn med eller utan sladd. QR-koden som används vid inloggning ändras varannan sekund och funktionen är aktiv i en minut innan den avbryts.

När det gäller inloggning i mobilappen krävs Mobilt BankID installerat på enheten. Det går även att logga in i mobilappen med personlig kod (fyrsiffrig). Om kunden loggar in med personlig kod kan kunden inte använda sig av alla funktioner som eventuellt kan kräva extra autentisering. I dessa fall måste kunden signera bankengagemangen med BankID på kort.

När kunden loggar in med Mobilt BankID visas följande:
"Jag identifierar mig hos Svenska Handelsbanken AB (publ).
Min avsikt: Inloggning i mobilappen privat
Tänk på! När du loggar in ska det alltid vara på ditt eget initiativ. Om du blivit uppringd och ombedd att logga in kan det vara ett försök till bedrägeri, avsluta samtalet och kontakta oss på 0771-77 88 99."

Om en inloggning har påbörjats och väntar på autentisering och en ny inloggning påbörjas från annan enhet avbryts båda inloggningsförsöken och kunden kan inte påbörja någon ny inloggning förrän efter en minut.

Det finns ingen möjlighet att spärra specifika inloggningsfunktioner som kunden eventuellt inte vill använda sig av.

6.3.2 Testfall 2 Överföring av tillgångar

Enbart överföring till ny mottagare kräver signering med kortläsare. Överföringar till redan sparade mottagare genomförs direkt utan signering.

Vid signering av överföring till ny mottagare presenteras det i Mobilt BankID enligt följande:
”Jag skriver under hos Svenska Handelsbanken AB (publ)
NY ÖVERFÖRING, Belopp, Till konto, Mott bank, Från konto, Datum, Referensnummer”

Beloppsgränsen för en överföring till ny mottagare i mobilappen är 250 000 kronor, för internetbanken med Mobilt BankID är det 50 000 kronor och för internetbanken med kortläsare är det 30 000 kronor. Beloppsgränsen för överföringar till sparad mottagare i mobilappen är 500 000 kronor och för sparad mottagare i internetbanken 200 000 kronor. Beloppsgränsen för överföringar mellan egna konton är 2 000 000 kronor.

Ytterligare skyddsåtgärder för överföringar har inte identifierats.

6.3.3 Testfall 3 Skapa nytt BankID

Ett nytt BankID kan skapas i mobilappen och internetbanken. Det kan även utfärdas genom att kunden är inloggad med bankkort via kortläsare med sladd i dator.

Kunden får ingen avisering från banken när ett nytt Mobilt BankID har skapats.

6.3.4 Testfall 4 Kontroll utloggningstid vid inaktiv inloggning

Banken har en inaktivitetstid som är fem minuter. Kunden får upp en varningsruta efter 4 minuter och loggas sedan ut automatiskt.

Väl inloggad i internetbanken kan kunden föra över mellan egna konto. Det vill säga konton som kunden själv disponerar, till exempel barns eller sparade mottagare samt ta bort eller ändra belopp i kommande betalningar eller överföringar utan ytterligare signering med till exempel Mobilt BankID.

6.3.5 Testfall 5 Bedrägeridetektion

Inloggning tillåts på flera enheter samtidigt. Test med att avbryta flera inloggningar i rad, påverkar inte en senare genomförd inloggning.

Vid signering av överföringar med olika belopp och nya mottagare i andra banker, kan inte någon extra säkerhetskontroll detekteras.

6.3.6 Omdöme – betyg 4 av 5

Det är bra ur säkerhetssynpunkt att Mobilt BankID utan QR-kod på annan enhet inte tillåts som inloggningsmetod. QR-koden uppdateras ofta, vilket också är bra.

Kunden kan välja att logga in med bankdosa med sladd, vilket möjliggör närhetsprincipen, vilket är bra men det är inte ett krav.

Kunden kan inte vara inloggad på internetbanken samtidigt på olika enheter, vilket minskar risken för att kunden glömmer logga ut en enhet, som andra kan komma åt.

När kunden loggar in med Mobilt BankID i mobilappen, visas förutom standardtexten *"Jag identifierar mig hos Svenska Handelsbanken AB (publ)."* även texten *"Min avsikt: Inloggning mobilappen privat*", vilket är positivt ur säkerhetssynpunkt.

Banken är tydlig med den information som presenteras för kunden vid signeringar, vilket är bra.

Det är dåligt ur säkerhetssynpunkt att överföringar till redan sparade mottagare inte kräver signering, utan genomförs direkt. Första gången en ny mottagare skapas och överföring till den görs, krävs dock signering.

Inaktivitetstiden innan kunden blir utloggad är 5 minuter, vilket är bra.

6.4 NORDEA

Begreppet E-kod hos Nordea är en kortläsare utan sladd, QR-läsare läser enbart QR-koder och ID-dosa är en bankdosa med QR-läsare.

6.4.1 Testfall 1 Inloggning

Vid inloggning till internetbanken krävs det att kunden använder Mobilt BankID med QR-kod, bankdosa med QR-läsare, kortläsare utan sladd eller QR-läsare.

Inloggning i mobilappen kräver Mobilt BankID installerat på samma enhet, biometrisk autentisering genom fingeravtryck eller med personlig kod.

Vid inloggning med Mobilt BankID och QR-kod ändras QR-koden var 30:e sekund.
När kunden loggar in med Mobilt BankID visas följande: *"Jag identifierar mig hos NORDEA".*

När det gäller QR-koden som används tillsammans med QR-läsare byttes den inte ut under 10 minuter, innan testet avbröts.

Bankdosa med QR-läsare har inte testats då vi inte hade någon sådan tillgänglig under testperioden.

Om en inloggning har påbörjats och väntar på autentisering och en ny inloggning påbörjas från annan enhet är det inga problem att logga in på från båda enheterna. Kunden kan alltså vara inloggad på två olika enheter samtidigt. Eftersom banken inte har Mobilt BankID utan QR-kod som inloggningsmetod, bedömer vi risken för att en bedragare lyckas lura kunden vid samtidig inloggning i internetbanken som liten.

Det finns möjlighet i mobilappen att avaktivera personlig kod som inloggningsfunktion om kunden eventuellt inte vill använda sig av detta.

6.4.2 Testfall 2 Överföringar av tillgångar

Det krävs en signering vid överföring till ny mottagare. Banken kräver inte signering för att lägga till den nya mottagaren, det går även bra att ange ett kontonummer direkt. Är det flera överföringar som skall göras samtidigt kan de läggas i en lista och signeras tillsammans.

Vid signering av en överföring med Mobilt BankID presenteras:
”Jag skriver under hos Nordea, Jag vill betala, belopp, mottagare, till konto, kontonummer, datum, från konto.”
Vid signering av flera överföringar samtidigt, visas enbart *”total belopp, från konto och antal överföringar”.*

Vid överföringar i mobilapp, om kunden loggat in med fingeravtryck eller personlig kod, krävs ytterligare verifiering med BankID.

Det finns en gräns för hur stora överföringar och betalningar kunder kan göra sammanlagt per dag. Gränsen är individuell och om kunden går över sin gräns får den ett felmeddelande när den försöker göra en överföring. Kunden kan ändra beloppsgränsen genom att ringa Kundservice och legitimera sig och sedan signera höjningen med hjälp av Mobilt BankID eller kort och kortläsare.

Ytterligare skyddsåtgärder har inte identifierats gällande överföringar.

6.4.3 Testfall 3 Skapa nytt BankID

Det går att förnya ett BankID med befintligt BankID. Det går att skapa ett nytt BankID första gången med kortläsare, QR-läsare eller personlig kod. Vid personlig kod krävs att kunden fyller i sitt registrerade mobilnummer dit en engångskod skickas. När kunden skapar ett BankID första gången sker en ID-kontroll som görs med ett svenskt pass eller ett svenskt ID-kort.

Kunden får ingen avisering från banken när ett nytt Mobilt BankID skapas.

6.4.4 Testfall 4 Kontroll utloggningstid vid inaktiv inloggning

Banken har en inaktivitetstid som är fem minuter.

Väl inloggad i internetbanken kan kunden göra överföringar mellan egna konto utan ytterligare signering. Köp eller försäljning av aktier och fonder kan genomföras utan extra autentisering när kunden är inloggad i banken.

6.4.5 Testfall 5 Bedrägeridetektion

Banken tillåter inloggning på flera enheter samtidigt. Test med att avbryta flera inloggningar i rad, påverkar inte en senare genomförd inloggning.

Vid signering av överföringar med olika belopp och nya mottagare i andra banker, kan inte någon extra säkerhetskontroll detekteras.

6.4.6 Omdöme – betyg 3 av 5

Det är bra ur säkerhetssynpunkt att Mobilt BankID utan QR-kod på annan enhet inte tillåts som inloggningsmetod.
Uppdateringstiden av QR-koden för Mobilt BankID, skulle kunna kortas ner för att öka säkerheten. Detsamma gäller även för QR-kod till QR-läsare, vilken har en ovanligt lång livstid.

Om en inloggning har påbörjats och väntar på autentisering och en ny inloggning påbörjas från annan enhet är det inga problem att logga in på från båda enheterna. Eftersom banken inte har Mobilt BankID utan QR-kod som inloggningsmetod, bedömer vi risken för att en bedragare lyckas lura kunden vid samtidig inloggning i internetbanken, som liten.

Det är positivt att det finns möjlighet i mobilappen att avaktivera personlig kod som inloggningsfunktion om kunden inte vill använda sig av detta, men negativt ur säkerhetssynpunkt att det går att aktivera en mer osäker inloggningsmetod.

Den information som presenteras för kunden i Mobilt BankID vid signering av enskilda överföringar är mycket bra, det är mindre bra att flera överföringsuppdrag som signeras samtidigt inte presenteras mer i detalj.

Det går bra att vara inloggad på olika enheter samtidigt, vilket kan vara en viss säkerhetsrisk om kunden glömmer logga ut en enhet, som andra kan komma åt.

Inaktivitetstiden innan kunden blir utloggad är 5 minuter, vilket är bra.

6.5 ICA-BANKEN

Begrepp bankdosa motsvaras av personlig dosa hos ICA Banken.
ICA-bankens kortdosa är en kortläsare utan sladd. Den går ej att beställa längre, de som finns ute hos kunderna går att använda tills batteriet tar slut.

6.5.1 Testfall 1 Inloggning

Vid inloggning till internetbanken krävs det att kunden använder Mobilt BankID med QR-kod, bankdosa där kunden anger personnummer och får tillbaka en kontrollkod eller kortläsare tillsammans med kundens bankkort samt personnummer och lösenord.
QR-koden som används vid inloggning med Mobilt BankID byts varannan sekund.

När det gäller inloggning i mobilappen på en mobiltelefon krävs att Mobilt BankID är installerat på samma enhet, bankdosa eller kortläsare.

När kunden loggar in med Mobilt BankID visas följande: *"Jag identifierar mig hos ICA Banken".*

Om en inloggning har påbörjats och väntar på autentisering och en ny inloggning påbörjas från annan enhet går det att vara inloggad på två enheter samtidigt i ca 10 sekunder. Efter 10 sekunder kommer en varningstext upp som lyder: *"Detta gjordes för din säkerhet, eftersom du även loggat in i en annan kanal. Du har blivit utloggad"*

Det finns ingen möjlighet att spärra vissa specifika inloggningsmetoder som användaren eventuellt inte vill använda sig av.

6.5.2 Testfall 2 Överföring av tillgångar

Banken kräver ingen signering för upplägg av nya mottagare. Signering krävs för att genomföra en transaktion till externa mottagare.

Vid signering med Mobilt BankID presenteras:
”Jag skriver under hos ICA Banken. Jag godkänner uppdrag med totalsumman, antal.”

6.5.3 Testfall 3 Skapa nytt BankID

För att ansöka om ett BankID kan kunden göra det med en bankdosa, samt behöver styrka ID med giltigt pass eller nationellt ID-kort och görs genom NFC-skanning på den enheten där BankID ska installeras.

Det går även att ansöka om ett nytt BankID med ett befintligt BankID. Nytt BankID kommer då att ersätta det gamla på den aktuella enheten. När ansökan om BankID är godkänd behöver kunden aktivera det nya BankID genom att skanna en QR-kod samt uppge en ny PIN-kod för det.

Kunden får ingen avisering från banken när ett nytt Mobilt BankID utfärdas.

6.5.4 Testfall 4 Kontroll utloggningstid vid inaktiv inloggning

Banken har en inaktivitetstid som är fem minuter. Det kommer upp en varningsruta 30 sekunder innan kunden blir utloggad automatiskt.

Väl inloggad i internetbanken kan kunden göra interna transaktioner och förändringar av befintliga uppgifter och konton, samt köp och försäljning av fonder utan att ny autentisering krävs.

6.5.5 Testfall 5 Bedrägeridetektion

Kunden kan vara inloggad två gånger samtidigt på samma dator. Banken tillåter dock inte dubbla inloggningar på två olika datorer. Efter 10 sekunder blir den första inloggningen utloggad och en varningstext visar:
"*Detta gjordes för din säkerhet, eftersom du även loggat in I en annan kanal. Du har blivit utloggad*"

Test med att avbryta flera inloggningar i rad, påverkar inte en senare genomförd inloggning.
Vid utfört test av att signera överföringar med olika belopp och nya mottagare i andra banker, kan inte någon extra säkerhetskontroll detekteras

6.5.6 Omdöme— betyg 3 av 5

ICA Banken uppdaterar QR-koden med kort intervall, vilket är bra.

Det är bra ur säkerhetssynpunkt att Mobilt BankID utan QR-kod på annan enhet inte tillåts som inloggningsmetod.

Om en inloggning har påbörjats och väntar på autentisering och en ny inloggning påbörjas från annan enhet, går det att vara inloggad på två enheter samtidigt i ca 10 sekunder innan den första inloggningen avslutas. Vi bedömer risken för att en bedragare kan utnyttja detta som liten eftersom Mobilt BankID utan QR-kod på annan enhet inte är en giltig inloggningsmetod.

Kunden kan i princip inte vara inloggad på internetbanken samtidigt via olika enheter, vilket minskar risken något för att kunden glömmer logga ut en enhet, som andra kan komma åt.

Information som presenteras för kunden vid signeringar med Mobilt BankID är inte så tydlig som hos många av de andra bankerna. Vid överföringar eller betalningar visas en totalsumma och antal överföringar, men ingen detaljerad information om vilka överföringar eller betalningar som görs, vilket är ett minus.

Inaktivitetstiden innan kunden blir utloggad är 5 minuter, vilket är bra.

6.6 LÄNSFÖRSÄKRINGAR BANK

Begreppet bankdosa motsvaras av säkerhetsdosa hos Länsförsäkringar Bank.

Inloggning med Mobilt säkerhetsID är ett begränsat Mobilt BankID med inloggning där personnummer anges samt QR-kod skannas, är till för dem som enbart vill se och göra överföringar mellan sina egna konton samt Swisha och fungerar enbart hos Länsförsäkringar Bank. Vi har inte testat detta närmare utan bedömer att säkerhetsnivån är samma som för Mobilt BankID med QR-kod.

6.6.1 Testfall 1 Inloggning

Vid inloggning till internetbanken krävs det att kunden använder Mobilt BankID med QR-kod, Mobilt säkerhetsID, BankID på datorn, eller bankdosa. QR-koden som används vid inloggning med Mobilt BankID byts varannan sekund.

När det gäller inloggning i mobilappen krävs Mobilt BankID på samma enhet, Mobilt säkerhetsID eller bankdosa.

När kunden loggar in med Mobilt BankID visas följande: *”Jag identifierar mig hos Länsförsäkringar.”*

Det är inte möjligt att påbörja inloggningar på olika enheter samtidigt.

Det finns ingen möjlighet att spärra vissa inloggningsmetoder som kunden eventuellt inte vill använda sig av.

6.6.2 Testfall 2 Överföring av tillgångar

Överföring till nytt konto i annan bank kräver signering.
Vid signering av överföring presenteras:
”Jag skriver under hos Länsförsäkringar. Överföring på X kr till EGET_VALT_MOTTAGARNAMN (kontonummer)Totalsumma att signera X kr. Uppdrag lämnat till banken den datum”

Det är möjligt att ställa in en standardinställning för signering i hela internetbanken enligt följande: Signera med det alternativ som användes vid inloggning, signera med bankdosa, signera med Mobilt BankID eller signera med BankID.

För överföringar till konto i annan bank eller annan kund hos Länsförsäkringar gäller beloppsgränsen 250 000 kronor inom en 7-dagarsperiod. Behöver kunden göra en större överföring måste kunden kontakta telefonbanken eller sitt lokala länsförsäkringsbolag.

Ytterligare skyddsåtgärder har inte identifierats gällande överföringar.

6.6.3 Testfall 3 Skapa nytt BankID

Om kunden väljer att skapa ett nytt BankID med bankdosa krävs giltigt pass eller nationellt ID-kort som skannas med hjälp av NFC-läsare på den enheten där nytt BankID ska installeras.

Det går även att ansöka om ett nytt BankID med ett befintligt BankID.
När ansökan om BankID är godkänd behöver kunden aktivera det nya BankID genom att skanna en QR-kod samt uppge en ny PIN-kod för det.

Kunden får ingen avisering från banken när ett nytt Mobilt BankID skapas.

6.6.4 Testfall 4 Kontroll utloggningstid vid inaktiv inloggning

Banken har en inaktivitetstid som är fem minuter.

Väl inloggad i internetbanken kan kunden göra interna transaktioner utan ytterligare signering.

6.6.5 Testfall 5 Bedrägeridetektion

Inloggning tillåts inte på flera enheter samtidigt. Om kunden gör för många inloggningsförsök visas meddelande: *"En identifiering eller underskrift för det här personnumret är redan påbörjad. Försök igen"*

Vid utfört test av att signera överföringar med olika belopp och nya mottagare till andra banker, kan inte någon extra säkerhetskontroll detekteras.

6.6.6 Omdöme – betyg 4 av 5

Det är bra ur säkerhetssynpunkt att Mobilt BankID utan QR-kod på annan enhet inte tillåts som inloggningsmetod. QR-koden uppdateras ofta, vilket också är bra.

Kunden kan inte vara inloggad på internetbanken samtidigt på olika enheter, vilket minskar risken för att kunden glömmer logga ut en enhet, som andra kan komma åt.

Banken är tydlig med den information som presenteras för kunden vid signeringar, vilket är bra.

Kunden har frihet att ställa in vilken säkerhetsmetod som ska vara standard för signering i internetbanken. Det kan vara positivt om kunden är säkerhetsmedveten och förstår sitt val, alternativt kanske en icke säkerhetsmedveten kund gör ett mindre bra val som minskar säkerheten för kunden.

Inaktivitetstiden innan kunden blir utloggad är 5 minuter, vilket är bra.

6.7 IKANO BANK

6.7.1 Testfall 1 Inloggning

Mobilappen är endast till för att hantera kort och inloggning till den kräver Mobilt BankID på samma enhet.

Ikano Bank har flera olika inloggningslänkar till internetbanken på sin hemsida.

Vid inloggning till internetbanken via de tre första alternativen krävs att kunden använder Mobilt BankID med QR-kod eller BankID på datorn (BankID på kort).
QR-koden som används vid inloggning byts varannan sekund.

Det finns en dock en annan länk för inloggning med följande text:
Har du problem att logga in? Om du inte har Bolån kan du i stället prova att logga in här ***(länk).***
Denna länk går till en inloggningssida utan QR-kod, i stället anges personnummer och autentisering sker med BankID installerat på datorn eller Mobilt BankID. *"Skydda din kod. Logga inte in om någon ringer och ber dig om det."* visas dock på inloggningssidan.

När kunden loggar in med Mobilt BankID visas följande:
"Jag identifierar mig hos Ikano Bank AB (publ)"

Vid test av inloggning som har påbörjats och väntar på autentisering i startad Mobil BankID utan QR-kod och en ny inloggning påbörjas från annan enhet med samma metod, avbryts den första inloggningen, meddelandet *"Åtgärden avbruten. Försök igen"* visas och i Mobilt BankID meddelas *"Åtgärden avbruten (tryck OK)"*. Den andra inloggningens autentisering kommer dock upp i den Mobila BankID som var aktiv vid det första inloggningsförsöket efter tryck på *"OK"* och om kunden inte är uppmärksam på det utan godkänner den, skulle det kunna leda till att en bedragare som har startat den andra parallella inloggningen får tillgång till internetbanken.

Det finns även en länk inifrån internetbanken, som leder till en äldre version av internetbanken, inloggning dit sker med angivande av personnr och mobilt BankID utan QR-kod eller BankID på datorn. Vilket kan vara en risk om det utnyttjas av en bedragare, med mobilt BankID utan QR-kod.

Vi har inte kunnat identifiera att kunden själv kan spärra vissa inloggningsfunktioner som den eventuellt inte vill använda sig av.

6.7.2 Testfall 2 Överföring av tillgångar

Överföringar enbart till egna konton i andra banker, konto i den andra banken måste även vara godkänt för autogiro.
Eget konto i annan bank kan läggas till utan signering, men banken kontrollerar att det är samma innehavare i den andra banken innan det kan användas (kan ta 2-3 bankdagar). Överföringar kan göras i båda riktningar mellan Ikano Banken och kundens andra bank.

Ingen autentisering krävs för överföringar mellan egna konton i olika banker.

Beloppsgränser är upp till 500 000 kronor per dag eller 1 500 000 kronor per vecka. Vid högre belopp behöver kunden skicka in ett skriftligt uppdrag.

6.7.3 Testfall 3 Skapa nytt BankID

Banken utfärdar inte BankID.

6.7.4 Testfall 4 Kontroll utloggningstid vid inaktiv inloggning

Banken har en inaktivitetstid som är fem minuter.

Väl inloggad i internetbanken kan kunden göra överföringar mellan egna konton och banker, överföringsuppdrag kan tas bort, ändring av kundens telefonnummer och epost kan göras utan att ytterligare signering krävs.

6.7.5 Testfall 5 Bedrägeridetektion

Inloggning tillåts på flera enheter samtidigt.
Om kunden gör flera avbrutna inloggningsförsök med Mobil BankID med QR-kod, spärras inloggningen under en viss tid på den aktuella mobila enheten. Om flera avbrutna inloggningsförsök görs med Mobil BankID utan QR-kod, spärras inte inloggningen.

Test av överföringar till nya konton i annan bank som inte är innehavarens kan inte genomföras.

6.7.6 Omdöme- – betyg 3 av 5

Banken har ett spretigt utseende på sin internetbank, med flera inloggningslänkar.

De har som huvudalternativ inloggning med BankID med QR kod eller BankID på kort vilket hade varit mycket bra om de hade varit de enda inloggningsmetoderna. Det är dock anmärkningsvärt att banken erbjuder en mindre säker inloggningsmetod om kunden har problem med den ordinarie inloggningen.

Mobilt BankID utan QR-kod på annan enhet, tillsammans med hanteringen av parallella inloggningsförsök, är inte helt tillfredsställande och skulle kunna utnyttjas av en bedragare för att få tillgång till internetbanken. Säkerhetsnivån är inte konsekvent och vi skulle gärna se att banken snarast tar bort möjligheten att logga in med mobilt BankID utan QR-kod.

Det går bra att vara inloggad på olika enheter samtidigt.

Inaktivitetstiden innan kunden blir utloggad är 5 minuter, vilket är bra.

Banken utfärdar inte BankID.

Eftersom banken endast tillåter överföringar till kundens egna konton i andra banker är det dock extremt svårt för en bedragare som lyckats lura sig in i internetbanken att föra ut några tillgångar till ett främmande konto.

6.8 AVANZA

6.8.1 Testfall 1 Inloggning

Vid inloggning till internetbanken krävs det att kunden använder BankID på samma enhet, Mobilt BankID på annan enhet med QR-kod eller användarnamn och lösenord i kombination med en mobilapp som generar engångskoder. Inloggning med användarnamn och lösenord måste aktiveras innan den kan användas. QR-koden som används vid inloggning visas i 30 sekunder och sedan avbryts inloggningen.

När det gäller inloggning i mobilappen krävs Mobilt BankID på samma enhet, Mobilt BankID på annan enhet (utan QR-kod), användarnamn och lösenord tillsammans med engångskod via mobilapp eller biometrisk autentisering med fingeravtryck eller ansiktsigenkänning. Inloggning med användarnamn och lösenord måste aktiveras innan användning. Biometrisk autentisering kräver aktivering innan det går att använda och då på en enhet åt gången.

I mobilappen används inte QR-kod vid valet BankID på annan enhet, personnummer skall anges. Om en bedragare påbörjar en ny inloggning samtidigt som kundens inloggning redan pågår avbryts inloggningen på bägge enheterna och meddelandet *"Det går inte att logga in just nu, försök igen senare"* visas i mobilappen hos bägge enheterna. I kundens aktiva Mobilt BankID meddelas *"Åtgärden avbruten (tryck OK)"*. Om bedragarens inloggning startas igen kommer dess autentisering, att komma upp i kundens Mobila BankID som var aktiv vid det första inloggningsförsöket och om kunden inte är uppmärksam på det utan godkänner den, skulle det kunna leda till att en bedragare får tillgång till internetbanken.

När kunden loggar in med Mobilt BankID visas följande:
"*Jag identifierar mig hos Avanza Bank AB."*

Det går bra att vara inloggad på fler enheter samtidigt.

Det finns möjlighet att spärra vissa inloggningsfunktioner som användaren eventuellt inte vill använda sig av till exempel inloggning med användarnamn och lösenord eller biometrisk autentisering.

6.8.2 Testfall 2 Överföring av tillgångar

Banken tillåter endast överföringar till egna konton i andra banker.
Kunden kan lägga till egna konton utan signering, men banken kontrollerar att det är samma innehavare i den andra banken innan överföringen genomförs.
Överföringar kräver signering, med Mobilt BankID, BankID på samma enhet eller SMS-kod som skickas till kundens föranmälda telefonnummer.
Vid signering av överföring presenteras:
"Jag skriver under hos Avanza Bank AB, Jag godkänner följande överföringar:
kontonr, Total summa, Jag ger uppdraget till banken datum tid"

Om kunden ändrar föranmält telefonnummer, spärras möjligheten att göra uttag över 10 000 kronor i 24 timmar som en säkerhetsåtgärd.

När kunden uppdaterar mejladress och/eller telefonnummer skickar banken en bekräftelse till kundens gamla kontaktuppgifter.

Enligt kundtjänst finns inga allmänna beloppsgränser eftersom det är enbart mellan egna konton i andra banker som pengar kan överföras

Ytterligare skyddsåtgärder har inte identifierats gällande överföringar.

6.8.3 Testfall 3 Skapa nytt BankID

Banken utfärdar inte BankID.

6.8.4 Testfall 4 Kontroll utloggningstid vid inaktiv inloggning

Inaktivitetstiden hos Avanza kan väljas av användaren själv. Det är antingen 30 minuter eller 1 timma. Vid inloggning med biometrisk autentisering, det vill säga fingeravtryck eller ansiktsigenkänning kan utloggningstiden vid inaktivitet väljas upp till 24 timmar.

Väl inloggad i internetbanken kan kunden göra överföringar mellan eller till egna konton i andra banker samt att aktier kan köpas och säljas utan att ytterligare signering krävs av till exempel Mobilt BankID.

Telefonnummer och mailadress kan ändras utan signering. Mottagarkonton i andra banker kan tas bort utan signering.

6.8.5 Testfall 5 Bedrägeridetektion

Inloggning tillåts på flera enheter samtidigt. Test med att avbryta flera inloggningar i rad, påverkar inte en senare genomförd inloggning.

Test av överföringar till nya konton i annan bank som inte är innehavarens kan inte genomföras.

6.8.6 Omdöme – betyg 3 av 5

Avanza har inte några bankdosor vilket är bra ur säkerhetssynpunkt. Mindre bra är att användare kan aktivera inloggning med användarnamn och lösenord. Det är även en brist att banken tillåter inloggning med Mobilt BankID utan QR kod från annan enhet vid inloggning i mobilappen.

Den relativt långa tiden samma QR-kod visas drar också ned betyget något.

Banken är tydlig med den information som presenteras för kunden vid signering av överföring, vilket är bra.

Den valbara lägsta tiden för utloggning efter inaktivitet på internetbanken är 30 minuter, vilken är ganska lång jämfört med de andra bankerna och det skulle vara bra, ur säkerhetssynpunkt, att erbjuda en lägre tid för kunderna.

Mobilt BankID utan QR-kod, tillsammans med hanteringen av parallella inloggningsförsök, är inte helt tillfredsställande och skulle kunna utnyttjas av en bedragare för tillgång till internetbanken.

Det går att vara inloggad på olika enheter samtidigt i internetbanken och mobilappen.

Banken utfärdar inte BankID.

Eftersom banken endast tillåter överföringar till kundens egna konton i andra banker är det dock extremt svårt för en bedragare som lyckats lura sig in i internetbanken att föra ut några tillgångar till ett främmande konto. Det finns dock en risk att en bedragare skulle kunna använda

depåfunktionerna och genom köp och försäljning av aktier orsaka offret ekonomisk skada och själv tjäna pengar genom att exempelvis manipulera aktiekurser.

6.9 DANSKE BANK

Begreppet bankdosa motsvaras av kodbox hos Danske Bank.

6.9.1 Testfall 1 Inloggning

Vid inloggning till internetbanken krävs det att kunden använder Mobilt BankID med QR-kod, BankID på samma enhet eller bankdosa.
QR-koden ändras inte utan autentiseringen avbryts efter 30 sekunder om inte rätt kod skrivits in.

När det gäller inloggning i mobilappen krävs Mobilt BankID installerat på samma enhet, Mobilt BankID på annan enhet (utan QR-kod) eller lösenord, aktivering av lösenord görs med hjälp av bankdosa första gången.

När kunden loggar in med Mobilt BankID i internetbanken visas följande: *”Jag skriver under hos Danske Bank Sweden. Inloggning hembanken. Med min elektroniska signatur bekräftar jag att jag vill logga in i Hembanken.*

VARNING - Banken kommer aldrig ringa upp dig och be dig logga in i Hembanken.
HAR DU BLIVIT UPPRINGD ELLER SJÄLV RINGT UPP EFTER UPPMANING?
Varning för bedragare som kontaktar kunder via telefon, sms eller mail. Lämna inte ifrån dig koder från din kodbox och klicka inte på länkar om du inte är helt säker på avsändaren. Ladda inte heller ner program för att dela din dator/mobila skärm på uppmaning.”

När kunden loggar in med Mobilt BankID i mobilappen visas följande:
”Jag identifierar mig hos Danske Bank Sweden.

Min avsikt: Inloggning i mobilbanken.

VARNING - Banken kommer aldrig kontakta dig och be dig logga in i Mobilbanken.

Varning för bedragare som kontaktar kunder via telefon, sms, chatt eller mail. Lämna inte ifrån dig koder från din kodbox och klicka inte på länkar om du inte är helt säker på avsändaren. Ladda inte heller ner program för att dela din dator/mobila skärm på uppmaning.”

Om en inloggning har påbörjats och väntar på autentisering och en ny inloggning påbörjas från annan enhet avbryts båda inloggningarna.

6.9.2 Testfall 2 Överföring av tillgångar

Överföring till nytt konto i annan bank kräver en signering.

Vid signering av överföring med Mobilt BankID presenteras:
”Från konto EGETVALT-KONTONAMN, kontonummer, Text på kontoutdrag, Till kontonummer, Banknamn, Text på mottagarens kontoutdrag, Belopp, Datum, Avgift”

I mobilappen är beloppsgränsen 125 000 kronor per överföring och dygn.
I internetbanken är beloppsgränsen 1 250 000 kronor per överföring och 12,5 miljoner kronor per dygn. Vi har inte sett några begränsningar baserade på metod för identifiering och signering.

Ytterligare skyddsåtgärder gällande överföringar har inte identifierats.

6.9.3 Testfall 3 Skapa nytt BankID

Om kunden inte har något BankID används den bankdosa som banken tillhandahåller.
För att för att förnya ett BankID krävs ett befintligt BankID. När ansökan om BankID är godkänd behöver kunden fylla i sitt telefonnummer och blir sedan omdirigerad till en ny webbsida för att aktivera det nya BankID genom att skanna en QR-kod samt uppge en ny PIN-kod för det.

Kunden får ingen avisering från banken när ett nytt Mobilt BankID skapas.

6.9.4 Testfall 4 Kontroll utloggningstid vid inaktiv inloggning

Banken har en inaktivitetstid som är fem minuter. Det kommer upp en varningsruta efter 4 minuter där kunden kan välja att logga ut eller fortsätta vara inloggad. Efter ytterligare en minut blir kunden automatiskt utloggad.

Väl inloggad i internetbanken kan du föra över mellan egna konto utan ytterligare signering.

6.9.5 Testfall 5 Bedrägeridetektion

Inloggning tillåts på flera enheter samtidigt. Test med att avbryta flera inloggningar i rad, påverkar inte en senare genomförd inloggning.

Vid utfört test av att signera överföringar med olika belopp och nya mottagare i andra banker, kan inte någon extra säkerhetskontroll detekteras.

6.9.6 Omdöme – betyg 3 av 5

Bankens QR-koden är statisk vilket är ett minus.

Att det finns inloggning med lösenord i mobilappen, minskar säkerheten, men vägs upp av att kunden måste aktivera den, om den skall fungera.

Mobilt BankID utan QR-kod på annan enhet kan användas i mobilappen, vilket är en mindre säker metod än Mobilt BankID med QR-kod och bör undvikas.

Banken är mycket tydlig i den information som presenteras för kunderna vid inloggningar och signeringar vilket är bra.

Om en inloggning har påbörjats och väntar på autentisering och en ny inloggning påbörjas från annan enhet avbryts båda inloggningarna, vilket är bra ur säkerhetssynpunkt i syfte att förhindra ett bedrägeriförsök i samband med inloggningen i banken.

Det går bra att vara inloggad på olika enheter samtidigt, det kan dock vara en viss säkerhetsrisk om kunden glömmer logga ut en enhet som andra kan komma åt.

Inaktivitetstiden innan kunden blir utloggad är 5 minuter, vilket är bra.

Beloppsgränser vid transaktioner är ganska höga, i förhållande till att ingen hänsyn tas till signeringsmetoden.

7 ANALYS AV TESTRESULTAT - TESTFALL 6

Detta kapitel behandlar enbart Testfall 6 - Kortsäkerhet ur ett användarperspektiv

7.1 SWEDBANK

Det är möjligt att spärra bankkort via mobilappen, i internetbanken eller genom att ringa till kundtjänst. Det är också möjligt att inaktivera automatuttag, internetköp samt inaktivera kortet tillfälligt.

Om kunden glömt sin PIN-kod går den att se i internetbanken eller mobilappen, det krävs dock en autentisering med till exempel Mobilt BankID innan PIN-koden visas.

Kontaktlös betalning (”blipp”) kan användas utan att behöva ange PIN-kod när beloppet är under 400 kronor, denna gräns kan dock variera mellan olika länder. För kundens säkerhet kräver kortutgivare att PIN-kod ändå skrivs in ibland även vid små belopp. Det kan vara efter att ett visst antal köp gjorts eller när summan av de kontaktlösa köpen har kommit upp i en viss totalsumma.

Om kunden skulle vilja avaktivera kontaktlös betalning görs detta via Spärrservice.

7.1.1 Omdöme — betyg 3 av 5

Swedbank har hög säkerhet när det gäller kortköp. Bankens kunder har generellt sett inte stora möjligheter att själva justera sina bankkorts inställningar. De flesta inställningar är antingen av eller på. Banken ger kunderna möjlighet att tillfälligt inaktivera bankkortet vilket är bra.
Ett minus är att kunder inte kan justera inställningarna för utlandsköp för specifika länder eller regioner, dessa är alltid på.

7.2 SEB

Det går att spärra kort och visa PIN-kod via mobilappen. För att visa PIN-koden krävs identifiering med BankID. Byte av PIN-kod kan endast göras i en uttagsautomat.

De köpinställningar för bankkort som kan göras i mobilappen är tryggare handel på nätet – Kundens bankkort är alltid öppet för köp på webbplatser med säkra kortköp över internet och för prenumerationer på till exempel olika streaming siter, alla köp på nätet under en timme – Kundens bankkort är öppet för alla nätköp under en timme, alla köp på nätet tills vidare – Kundens bankkort är alltid öppet för alla nätköp tills inställningen ändras eller endast köp i fysisk butik.

Kontaktlös betalning (”blipp”) kan användas utan att behöva ange PIN-kod när beloppet är under 400 kronor men om beloppet är större måste kunden alltid slå sin PIN-kod. Som en extra säkerhetsåtgärd behöver kunden slå sin PIN-kod vid slumpvist utvalda tillfällen vid kontaktlös betalning.

Kontaktlös betalning aktiveras automatiskt när kunden aktiverar bankkortet, det vill säga när kunden handlar eller tar ut pengar och använder PIN-kod. För att inaktivera kontaktlös betalning behöver kunden ringa till kundservice.

7.2.1 Omdöme – betyg 3 av 5

SEB har hög säkerhet när det gäller kortköp. Bankens kunder har bra möjligheter att själva justera sina inställningar för säkerheten gällande kortköp. Banken har försökt ta hänsyn till olika kunders köpvanor och köpbeteende.

7.3 HANDELSBANKEN

Kunden kan spärra bankkort via mobilappen, internetbanken eller genom att ringa till kundtjänst. Utlandsbetalning och internetköp aktiveras och inaktiveras i mobilappen och i internetbanken.

Det går inte att se PIN-koden i mobilappen eller internetbanken.

Vid köp med bankkort får kunden en notifiering via mobilappen på beloppet samt var köpet gjorts.

Kontaktlös betalning (”blipp”) kan användas tills att det sammanlagda beloppet uppnår 1200 kronor utan att behöva ange PIN-kod. Kunder som vill avaktivera kontaktlös betalning måste göra det via kundservice.

7.3.1 Omdöme – betyg 2 av 5

Handelsbanken har generellt sätt hög kortsäkerhet. Kunderna har relativt få möjligheter att själv påverka sina bankkorts inställningar. De inställningar som finns kan kunder endast slå av eller på.

7.4 NORDEA

Kunder kan tillfälligt inaktivera bankkorten eller spärra det helt, både i internetbanken och i mobilappen. Kunderna kan bestämma inom vilka regioner bankkortet får användas och om det får användas för säkra eller osäkra kortköp över internet. Alla dessa inställningar går att göra utan extra autentisering.

För att visa PIN-koden i mobilappen eller internetbanken krävs ingen extra identifiering med BankID.

Kontaktlös betalning (”blipp”) kan användas utan att ange PIN-kod när beloppet är under 400 kronor men om beloppet är större måste kunden alltid slå sin PIN-kod. Som en extra säkerhetsåtgärd kan kunden ibland bli ombedd att slå in sin PIN-kod, även om beloppet understiger 400 kronor. Kunder som vill avaktivera kontaktlös betalning måste göra det via kundservice.

7.4.1 Omdöme – betyg 2 av 5

Banken har hög säkerhetsnivå. Banken har implementerat en rad säkerhetsmekanismer som är bra för kunderna vad det gällande regionsinställningar och för både säkra och osäkra köp över internet. Kunderna ges många inställningsmöjligheter, vilket är bra.

7.5 ICA-BANKEN

Det är möjligt att spärra bankkort via mobilappen, i internetbanken eller genom att ringa till kundtjänst.

I mobilappen går det att se PIN-koden. Det krävs en autentisering för att komma åt PIN-koden och det är bara möjligt att se en (1) siffra åt gången.

Det går även att styra inställningen för säkra och osäkra internetköp. Kunden kan välja om Mobilt BankID eller bankdosa krävs för att genomföra köpen. Dessa funktioner är inaktiverade som standard.

Kontaktlös betalning (”blipp”) kan användas på ICA affärer och Apotek Hjärtat upp till 500 kronor eller i andra butiker upp till 400 kronor utan att behöva ange sin PIN-kod. Kontaktlös betalning kan inte inaktiveras.

7.5.1 Omdöme – betyg 3 av 5

ICA Banken har hög säkerhetsnivå. Kunder har ett lite mer begränsat antal möjligheter att påverka sina bankkortinställningar själva. Tidigare hade kunder möjlighet att göra justeringar för utlandsköp på landsnivå. Vi ser det som ett minus att banken nu tagit bort den funktionen. Ett plus är att kunder kan styra över säkra och osäkra internetköp och vilken identifieringsmetod som ska användas.

7.6 LÄNSFÖRSÄKRINGAR BANK

Det är möjligt att spärra bankkort via mobilappen, i internetbanken eller genom att ringa till kundtjänst.

För att se PIN-koden till bankkort i mobilappen behöver kunden ange CVC-koden för det aktuella kortet.

I mobilappen eller i internetbanken kan kunden spärra bankkortet tillfälligt för alla typer av köp. Kunden kan även spärra köp på internet samt spärra för köp i olika regioner eller specifika länder.

Kunden kan ställa in att få ett SMS eller notis ifrån mobilappen om kortköp eller kontantuttag görs i annan valuta än i svenska kronor.

Kontaktlös betalning (”blipp”) kan användas utan att ange PIN-kod när beloppet är under 400 kronor men om beloppet är större måste kunden alltid ange PIN-kod. Som en extra säkerhet kommer kunden emellanåt bli ombedd att slå in sin PIN-kod eller göra ett vanligt köp med chip och din kod, även för köp under 400 kronor.

Kunder som vill avaktivera kontaktlös betalning gör det själva via mobilappen eller internetbanken.

7.6.1 Omdöme - betyg 4 av 5

Länsförsäkringars kortsäkerhet är generellt sett hög. Kunden har många inställningar att välja på för användningen av sina bankkort, exempelvis möjlighet att tidsätta och begränsa kortköp över internet.
Skulle kunden ha glömt sin PIN-kod till sitt bankkort, kan kunden se denna i sin mobilapp genom att ange CVC-koden till det aktuella kortet.

7.7 IKANO BANK

Det är möjligt att spärra bankkort i internetbanken eller genom att ringa till kundtjänst.

Det är inte möjligt att se PIN-kod via mobilapp eller internetbank.

Det går inte att på egen hand i mobilappen eller internetbanken ändra inställningar för internetköp. Det är dock möjligt att få hjälp att aktivera eller inaktivera internetköp samt välja regionsspärr, genom att ringa bankens kundtjänst.

Kontaktlös betalning (”blipp”) aktiveras genom ett vanligt köp där kunden slår sin PIN-kod. Banken uppger att kunden själv kan välja maxbeloppet på kontaktlösa betalningar. Beloppsgränsen är mellan 200–400 kronor. Om kunden överskrider beloppsgränsen blir kunden tvungen att ange PIN-kod i terminalen för att genomföra betalningen.

7.7.1 Omdöme – betyg 1 av 5

Ikano Banks kunder kan inte göra några inställningar på egen hand, annat än spärra kortet i internetbanken. Kunderna kan dock ringa kundtjänst för att ändra inställningar för kortköp, men vad

vi kan se presenteras inte någon information om detta på bankens hemsida och dessutom är det inte praktiskt att alltid behöva ringa till kundtjänst för att ändra sina inställningar.

7.8 DANSKE BANK

Kunden kan via mobilappen spärra bankkortet tillfälligt, ändra beloppsgränser för belopp per uttag, uttagsgräns per sju dagar och köpgräns per sju dagar. Kunden kan också spärra bankkortet för internetköp per region.
Det finns en fast uttagsgräns på 15 000 kronor per dag som inte går att ändra.

I internetbanken kan kunden endast se beloppsgränser, spärra bankkortet för internetköp per region, beställa nytt bankkort samt spärra bankkort.

För att visa PIN-koden i mobilappen krävs identifiering med BankID.

Kontaktlös betalning (”blipp”) kan användas för 20st kontaktlösa köp eller tills köpen uppnår totalsumman 1500 kronor. Efter det behöver kunden göra ett köp med chip och PIN-kod innan den kan göra köp med den kontaktlösa funktionen igen.

7.8.1 Omdöme - – betyg 4 av 5

Banken har hög säkerhet för kundernas bankkort. Kunderna har bra möjligheter att anpassa inställningarna för sina bankkort både för köp och uttag i automater. Kunderna har större möjligheter att göra anpassningar i mobilappen, jämfört med internetbanken. Det kan vara en nackdel för kunder som inte har tillgång till en mobilapp och i stället tvingas att kontakta kundtjänst för att få hjälp.

8 SLUTSATSER

8.1 TESTFALL 1-5

Vi kan konstatera att bankerna har en bra grundnivå gällande säkerhet mot bedrägeriförsök, men den skulle kunna bli ännu bättre. BankID inför nya krav för säker start av BankID. Senast 1 maj 2024 måste bankerna enbart använda Mobilt BankID med QR-kod där koden byts ofta eller Mobilt BankID på samma enhet som skall logga in. Start av BankID med personnummer kommer inte längre att tillåtas. BankID uppmanar bankerna att ”*Uppdatera så snart som möjligt”*, vilket vi instämmer i.

Inte helt oväntat, med tanke på kommande krav från BankID, ser vi att bankerna går mot att mer och mer använda Mobilt BankID med QR-kod som främsta alternativ för autentisering och signering av transaktioner. Det finns dock några banker som fortfarande har kvar den mer osäkra inloggningen med personnummer och Mobilt BankID utan QR-kod på annan enhet, som ur säkerhetssynpunkt är ett sämre alternativ för kunden. Vid användande av Mobilt BankID tillsammans med QR-kod som förnyas löpande säkerställs inte fysisk kontakt men ger ändå en ytterligare försäkran om att kunden som försöker logga in har autentiseringsenheten i närheten.

Giltighetstiden på QR-koden för Mobilt BankID är i samtliga fall också så kort att det måste anses osannolikt att en bedragare hinner skicka över den till bankkunden och lyckas övertala denna att godkänna inloggningen.

De flesta banker utfärdar BankID. Det är bara nischbankerna, Avanza och Ikano Bank, som inte gör det. Bankerna har snarlika säkerhetslösningar för att förnya eller skapa ett första nytt BankID.

Bankerna vidtar ständigt åtgärder för att försvåra bedrägerier mot sina kunder. I våra tester ser vi att bankerna främst har gjort justeringar av befintliga säkerhetsfunktioner sedan förra gången vi gjorde dessa tester. Samtidigt som bankerna gör detta vill man även möta kundens behov av smidighet och information. Vi ser att bankerna generellt sett är bra på att informera sina kunder om vem kunden identifierar mot samt vad som signeras gällande transaktioner.

Informationen som kunderna får upp i Mobilt BankID och BankID på datorn, är generellt sett informativ och tydlig, förutom vid inloggning där endast vissa av banker talar om anledningen till den identifiering som sker.

Bankerna gör hela tiden säkerhetsbedömningar baserat på hur tekniken utvecklas, hur hotbilden förändras och vad kunderna är villiga att acceptera. Det kan konstateras att mognadsgraden ökar och att den största utmaningen är att många äldre inte har anammat Mobilt BankID utan förlitar sig på bankdosor för att göra sina bankärenden. Det är också denna grupp som i många fall utgör målgruppen för bedragare. Detta gör att riskerna för att äldre blir lurade ökar.

Bankerna har mycket information på sina hemsidor som handlar om säkerhet och bedrägerier och det står varningar vid inloggning på nära nog alla internetbankerna. Problemet är att det inte blinkar några varningar när kunder knappar in sin PIN-kod i bankdosan. Det är där risken är som störst, inte när kunden själv loggar in på sin bank.

Denna gång utser vi Swedbank till Bäst i test. Motiveringen är att den totala sammanvägningen av bankens riskmedvetenhet, säkerhetsmekanismer och tydlighet mot sina kunder är något bättre än de andra bankerna i denna granskning. Swedbank kräver att kunden aktiverar utökad användning av Mobilt BankID innan nya mottagare kan signeras med Mobilt BankID. Banken är dessutom den enda

bank där kunden behöver signera både en ny mottagare och överföring. Det som drar ner betyget något är att det inte sker någon extra kontroll vid transaktioner av ovanligt höga belopp.

En kunds sparkapital är säkrare på en nischbank än på en fullservicebank eftersom de inte medger utbetalningar till andra konton än kundens egna. Det är dock inget alternativ att endast använda nischbanker eftersom de inte erbjuder möjlighet att betala räkningar.

8.2 TESTFALL 6

Bankerna har generellt sett hög säkerhet när det gäller bankkort och erbjuder en rad olika säkerhetsinställningar som kunden själv kan göra för bankkorten. I detta sammanhang är det upp till bankkunden att själv sätta sin prägel på säkerhetsnivån utifrån de funktioner som banken erbjuder och utifrån sitt köpbeteende och vanor på nätet. Hos en del av bankerna har kunden en stor frihet att själv avgöra vad som känns tryggast att aktivera eller inaktivera gällande de olika säkerhetsfunktionerna för sina bankkort. Hos några av bankerna är det dock mer begränsat vad som kan ställas in.

Hos alla bankerna har kunden, förutom via kundtjänst, möjlighet att själv spärra sitt bankkort via internetbanken alternativt mobilappen, detta är dock en spärr som är permanent och är till för när kunden förlorat sitt kort.

Några av bankerna har en funktion där kunderna själv tillfälligt kan spärra sitt kort och sedan aktivera det igen. Denna lösning borde vara tilltalande för fler banker. Ett tänkbart scenario är att en kund kanske inte hittar sitt bankkort och spärrar det utifall kortet skulle vara stulet eller borttappat. Några dagar senare hittar kunden kortet igen och om det är permanent spärrat, måste banken tillverka och skicka ut ett nytt kort till kunden. Är det däremot tillfälligt spärrat av kunden, kan den själv aktivera det igen och banken behöver inte ha några kostnader för ett nytt kort och kunden kan använda det direkt igen. Det höjer även säkerheten radikalt, om kunden själv kan välja att aktivera kortet enbart vid de tillfällen som det skall användas och däremellan ha det spärrat. Det finns dock en viss risk om kunden inte haft kontroll över kortet att någon kopierat data ifrån det och möjligtvis skulle kunna använda kortets data till ett bedrägeri när kortet blir aktiverat igen, men vi bedömer den risken som relativt liten i förhållande till vinsten i säkerhet att själv kunna spärra kortet tillfälligt.

På samma sätt är möjligheten att kunna se PIN-kod till bankkortet i internetbanken eller i mobilappen, något som borde bespara bankerna en del arbete samt underlätta för glömska kunder, förutsatt att visningen av PIN-koden skyddas på ett säkert sätt.

Att kunna styra i vilken del av världen eller i vilka länder bankkortet skall kunna användas, är en bra funktion som höjer säkerheten för de kunder som aktivt gör inställningar utifrån sina geografiska köpvanor.

Angående ”blipp” funktionen är den, kanske inte helt oväntat, ganska snarlik mellan de olika bankerna, det är relativt låga belopp som det kan handlas för innan PIN-kod krävs.

Vi har inte kunnat finna officiell statistik över kortbedrägerier där bedragare lyckats stjäla kortuppgifter via en trådlös avläsare eller med hjälp av en vanlig mobiltelefon och sedan utnyttjat informationen för att göra kortköp utan kod. Trots att det är något som är tekniskt möjligt för en bedragare att utföra, blir troligtvis arbetsinsatsen ganska omfattande i förhållande till den vinst det ger för bedragaren och i dagsläget bedömer vi därför risken som relativt liten att få sina kortuppgifter stulna av en bedragare på detta sätt.

För de bankkortskunder som aldrig använder ”blipp” funktionen, skulle det vara säkerhetshöjande att stänga av den. För de kunder som ofta använder ”blipp”-funktionen ihop med sina bankkort, skulle det inte vara speciellt praktiskt att slå av och på funktionen i samband med varje köp.

Det finns en mängd olika tekniska hjälpmedel att köpa, som skall förhindra läsning av bankkort med ”blipp”-funktion, vilket kan öka tryggheten för dem som inte vill stänga av funktionen.

Generellt sett angående kortbedrägerier, har de minskat de senaste åren, men en ökning har skett sedan början av 2023, enligt statistik ifrån SSF-säkerhetskollen[5] och det är främst bedrägerifall gällande kortköp utan tillgång till kort som står för den största delen.

Oftast kommer kortuppgifterna, i denna typ av bedrägerier, från intrång i ett kundregister på nätet och säljs därefter vidare till bedragarna som använder dem vid köp i utlandet hos handlare som har låga säkerhetskrav för internetköp.

När det gäller bankernas kortsäkerhet är det Länsförsäkringar som vi utser till Bäst i test. Motiveringen är att banken har en tydlig balans mellan säkerhet och funktionalitet för sina kunders kortfunktioner och kortköp. Kunderna erbjudes flexibilitet och frihet samtidigt som banken har en hög riskmedvetenhet.

[5] https://sakerhetskollen.se/brottsstatistik/statistik-bedragerier-februari-2023

9 REKOMMENDATIONER TILL BANKKUNDER

De viktigaste råden till bankkunderna gällande deras säkerhet för digitala tjänster mot banken, är i stort sett samma som vid förra undersökningen. Kunderna kan förbättra sin säkerhetsnivå genom att undvika att använda sig av de mindre säkra autentiseringsmetoderna och om möjligt inaktivera funktioner de inte använder sig av.

Var alltid vara noga med att kontrollera vem du identifierar dig mot eller vad du signerar. Lämna aldrig ut autentiseringsinformation, inloggningsuppgifter eller koder, till någon annan. Bankkunder som blir lurade vid bankbedrägerier läser ofta inte igenom vad de godkänner med sitt BankID.

Lägg på luren om någon som uppger sig ringa från din bank vill att du ska identifiera dig med BankID eller vill fjärrstyra din dator. Är du osäker och vill kontrollera om det var banken som ville dig något, ring i stället upp din bank själv. Använd alltid det telefonnummer som finns till kundtjänst på bankens egen hemsida.

Tänk också på att aldrig klicka på några länkar som kommer via epost eller SMS, det kan vara en bedragare som döljer sig bakom länken som skickats till dig.

Bankkunderna kan precis som vi nämnt i 2022 års rapport begränsa sin skada om de skulle falla offer för en bedragare genom att inte lägga alla ägg i samma korg och binda upp sig som helkund hos en bank. Det går att ta säkerheten ytterligare ett steg längre, genom att utnyttja att det idag är i stort sett omöjligt för en bedragare att komma åt en bankkunds bankmedel på nischbankerna Ikano Bank och Avanza Bank, då dessa banker helt enkelt inte tillåter överföringar till annat än bankkundens konton i den egna banken eller bankkundens konton på annan bank. Att ha sina huvudsakliga bankmedel på en bank som inte tillåter annat än överföring till kundens egna konton och endast ha mindre bankmedel för den dagliga livsföringen i en bank med möjlighet till överföring till andra via Swish med mera, blir mycket bedrägerisäkert. En bedragare har då enkom möjlighet att komma åt beloppen som finns på banken med överföringsmöjligheter till andra personer. Nischbankerna erbjuder dessutom oftast väsentligt bättre sparränta än fullservicebankerna.

Ett gott råd för att minimera risken gällande kortbedrägerier är att spärra bankkortet för internetköp och köp i utlandet och tillfälligt ta bort spärren vid behov, samt att inte spara några av dina kortuppgifter i kundregister på nätet eller i webbläsaren.

Granska kritiskt de sidor du besöker på nätet när du skall handla något, det kan i värsta fall vara en bedragare som satt upp en egen sida där du skriver in dina kortuppgifter. Skulle du upptäcka köp gjorda med ditt kort som du inte känner igen, spärra kortet omgående hos din bank. Efter att kortet spärrats skall du göra en polisanmälan.

När det gäller inställningar för kortköp varierar inställningsmöjligheterna hos bankerna. Om du har möjlighet att välja, skaffa bankkort i den bank vars inställningar för kortköp passar dig bäst. Har du redan ett bankkort, se till att utnyttja de inställningar din bank erbjuder för kortköp och välj att spärra det du inte behöver i din vardag och aktivera endast funktioner när du behöver dem.

Den största risken gällande bedrägerier hos svenska bankkunder är fortfarande att falla offer för kortbedrägerier i samband med internetköp eller förskottsbetalningar vid köp på Blocket, Facebook eller andra handelsplatser för privatpersoner.