BODFORSS

Så kan bankbedrägerierna minska

Analytiker: Rikard Bodforss
QA: Erik Orrsjö
Datum:2022-06-07
Version: 1.1
Uppdragsgivare: Ulf Stenberg,

Villaägarnas Riksförbund Produktgranskning

1 INNEHÅLL

2 INLEDNING

2.1 BAKGRUND

Bankbedrägerierna gentemot privatpersoner i Sverige ökar trots högre säkerhet för banker och betaltjänster. Det vanligaste tillvägagångssättet är att de drabbade privatpersonerna får sina bankkonton kapade och länsade av kriminella genom telefonbedrägerier (vishingbedrägerier), där bedragaren påstår sig ringa från en bank, ett försäkringsbolag eller något annat och därvid förmår brottsoffret att genomföra transaktioner från sitt bankkonto. Bedragaren kan till exempel påstå att brottsoffret behöver logga in på sitt bankkonto och godkänna att pengar betalas ut till brottsoffret, men i själva verket godkänner brottsoffret överföringar från sitt bankkonto till bedragaren eller bedragarens kumpaner. Det kan röra sig om mycket pengar, till exempel sparade pengar till en renovering eller en kontantinsats för husköp. Mot bakgrund av detta har Villaägarna Produktgranskning uppdragit till Bodforss Consulting att ta fram rekommendationer till både banker och privatpersoner för att minska risken/förlusten för privatpersoner när dessa väl har fallit offer för en bedragare.

Målet med rekommendationerna är även att minska bedragares incitament att komma över privatpersoners bankkonton och betaltjänster, då det ekonomiska utbytet blir mindre. Rekommendationerna är uppdelade på en del som avhandlar åtgärder som kan vidtas av bankerna, samt en del som belyser åtgärder som bankkunder kan vidta.

2.2 AVGRÄNSNINGAR

Denna rapport avhandlar rekommendationer för banker och betaltjänstkunder som ska leda till att minimera skadan vid ett fullbordat bedrägeri. Rekommendationer för att undvika bedrägeri finns att läsa i rapporten ”Granskning av säkerheten och skyddet mot bedrägerier för privatkunders bankkonton”, som Bodforss Consulting tog fram åt Villaägarnas Riksförbund förra året[1].

2.3 BEGREPP OCH FÖRKORTNINGAR

- **PSD2 – Payment Services Directive 2**, direktiv (EU) 2015/2366 ersatte det gamla betaltjänstedirektivet från 2007 och trädde i kraft 13 januari 2018 och omsattes i svensk lagstiftning genom den nya betaltjänstlagen. Direktivets syfte var bland annat att harmonisera konsumentskyddet och rättigheter och skyldigheter för betalningsleverantörer och användare.
- **PCI SSC – Payment Card Industry Security Standards Council** är en branschorganisation som består av banker och betaltjänsteleverantörer. De står bakom PCI DSS (Payment Card Industry Data Security Standards) som föreskriver regler för säkerhet kring korttransaktioner, kortutgivning och betalflöden.
- **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 synonyma, men i denna granskning utgör legitimeringen oftast autentiseringen mot internetbanken och vi använder därför här begreppen synonymt.

[1] https://www.villaagarna.se/debatt/press/pressmeddelanden/skyddet-mot-bedragerier-varierar-mellan-bankerna/

- **Signering –** I denna rapport handlar det uteslutande om elektronisk signering. Det kan likställas med att skriva under med sin namnteckning. 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:t och räknar ut en svarskod som kan verifieras av banken.

3 PROBLEM- OCH HOTANALYS

De senaste åren har det vidtagits ett antal åtgärder från lagstiftare för att göra betaltjänster säkrare ur ett konsumentperspektiv. Bland annat så har EU:s andra betaltjänstdirektiv (PSD2) medfört krav på stark kundautentisering, vilket har gjort att det blivit svårare för bedragare att komma åt bankkundernas pengar. Branschåtgärder inom betalkortsindustrins standardråd (PCI SSC) har också gjort att kredit- och betalkortsbedrägerier är svårare att lyckas med.

I den granskning av banksäkerhet som vi genomförde förra året på uppdrag av Villaägarnas Riksförbund konstaterade vi att bankernas säkerhet generellt är hög, vilket också visar sig i statistiken. Trots detta förekommer bedrägerier där brottslingar lyckas övertala offret att lämna ifrån sig autentiseringsuppgifter och på så sätt föra över pengar till sina egna konton.

Enligt statistik från Brottsförebyggande rådet för år 2019 uppgick antalet anmälda befogenhetsbedrägerier till 3 600 stycken. En stor del av dessa bedrägerier utgörs av telefonbedrägerier (vishingbedrägerier). Motsvarande siffra för år 2020 är 4 676 stycken och 6 282 stycken för år 2021, vilket innebär att antalet befogenhetsbedrägerierna har ökat med hela 75 procent de senaste två åren. Samtidigt rapporterar polisen att brottsvinsterna från vishing-bedrägerier har ökat med 118 procent till 340 Mkr från år 2020 till år 2021[2].

Höjd banksäkerhet till trots, lyckas bedragarna likväl komma åt bankkundernas pengar. En kedja är dock som bekant aldrig starkare än sin svagaste länk. När det gäller säkerhet för bankkonton är bankkunderna i mångt och mycket den svagaste länken. Något som bedragarna förefaller utnyttja hämningslöst.

Dessa bedrägerier faller som sagt in under kategorin befogenhetsbedrägerier.

Andelen uppklarade bedrägeribrott[3] ligger stadigt på runt 6% vilket gör att det är fortsatt attraktivt för brottslingar att ägna sig åt bedrägerier. Anledningen till den låga siffran är sannolikt att utredningsinsatsen för att kunna lagföra någon för ett bedrägeribrott är stor och beloppen i de enskilda fallen relativt ringa, även om beloppen kan vara mycket kännbara för brottsoffret.

För att ett bedrägeri ska lyckas, så krävs ett stort mått av organisation. Bedragarna behöver bulvaner och konton genom vilka stulna medel kan slussas i upprepade transaktioner och slutligen behövs metoder för att tvätta pengarna. Detta gör att det sannolikt är organiserad brottslighet som står bakom lejonparten av bankbedrägerierna.

Precis som framgångsrika företag, så räknar även brottslingar på lönsamhet vägt mot risk. De två parametrar som skulle kunna avskräcka brottslingar från att genomföra ett brott är antingen;

- att sannolikheten för att lagföras och straffas för brottet är hög, eller
- att lönsamheten ställt mot arbetsinsatsen är låg.

En omprioritering av Polismyndighetens utredningsresurser till bedrägeribrott skulle kunna leda till att andra typer av brottslighet ökar. Det är fullt möjligt att en utökning av Polismyndighetens anslag skulle kunna leda till förbättrad statistik avseende uppklarade bedrägeribrott, men frågan är om det är rationellt. Troligen är det mera effektivt att slå mot brottslighetens lönsamhet i förhållande till

[2] https://www.stoldskyddsforeningen.se/bedragare-har-tjanat-over-300-miljoner-pa-bedragerier-via-telefon-under-2021/
[3] Avser samtliga typer av bedrägerier.

arbetsinsatsen. Detta kan göras genom att försvåra genomförandet och/eller minimera beloppen som stjäls.

Åtgärder för att försvåra genomförande/obehörig åtkomst till konton har vidtagits av flera banker de senaste åren. De flesta åtgärderna har rört starkare autentisering och tydligare koppling till att kunden är närvarande (QR koder för mobilt BankID, eller BankID på kort). Kravet på närvaro förhindrar möjligheten till inloggning på en enhet som inte finns på samma fysiska plats som den enhet som används för legitimeringen.

Väldigt lite har gjorts för att försvåra eller begränsa överföring av kapital från offer till bedragare, när bedragaren väl har lyckats ta sig in på kontot. Ansvaret för att försvåra genomförande och minimera bytet vid bedrägeribrott måste dock delas mellan bankerna och bankkunderna för att minska brottslingarnas incitament. I kapitel 4 beskrivs ett antal förslag som banker kan genomföra för att försvåra eller begränsa överföring av kapital från brottsoffren, medan det i kapitel 5 beskrivs vad kunderna kan göra för att begränsa skadan av ett fullbordat bedrägeri.

4 REKOMMENDATIONER TILL BANKER OCH BETALTJÄNSTER

I vår tidigare granskning avhandlade vi olika bankers säkerhetslösningar för autentisering och signering samt ytterligare säkerhetskontroller. Utöver de rekommendationer som framställdes där är det svårt att se ytterligare tekniska kontroller för autentisering och signering som inte skulle påverka användbarheten mycket negativt. Man kan däremot tänka sig andra kontroller som skulle göra bedrägeribrotten mindre lönsamma genom att försvåra överföring av större belopp.

Många säkerhetsåtgärder som bankernas säkerhetsavdelningar skulle vilja införa bromsas sannolikt av deras marknadsavdelningar som eftersträvar enkelhet och smidighet för kunderna. Riskarbetet inom betaltjänstesegmentet är en balansgång mellan att öka sina volymer och bibehålla en rimlig säkerhetsnivå som accepteras av kunderna. Misslyckas man åt något håll så kommer det uppstickare i form av tech-bolag som ser en affärsmöjlighet och kanske har en annan riskaptit. Det resulterar ofta i att marknadsandelen naggas i kanten, med minskande marginaler till följd.

Flera av våra förslag på åtgärder och kontroller är sådant som en del banker redan har infört i någon form. Skulle man införa alla åtgärderna så är det sannolikt att en stor kundgrupp skulle välja att byta bank, på grund av att säkerhetsåtgärderna upplevs som oproportionerliga. Detta skulle ge marknadsavdelningarna än mer tyngd åt sina argument. Ett förslag från vår sida är att kunden själv skulle kunna välja att slå på ytterligare säkerhetsfunktioner för att försvåra eller begränsa möjligheterna för bedragare att föra över medel från kontot.

Vad vi vill försvåra för bedragare, är att när de har lyckats logga in sig på offrets internetbank och signerat en transaktion, inte ska kunna föra över betydande belopp till sina egna konton. Vad som är betydande belopp skiljer sig avsevärt mellan olika bankkunder och därför bör nivåerna kunna anpassas i någon mån. Nedan följer ett antal åtgärder och kontroller som skulle försvåra och försämra lönsamheten i bankbedrägerier.

4.1 SIGNERING AV NYA MOTTAGARE

En ganska enkel åtgärd är att kräva signering när en ny betalningsmottagare läggs till. Detta är en kontroll som används av bland andra Swedbank och Handelsbanken. Fördelen är att det kräver ett ytterligare steg av signering innan en bedragare kan föra över pengar till ett nytt konto. Det ger offret ytterligare möjlighet att upptäcka att någonting skumt håller på att hända, under förutsättning att hen läser vad de signerar.

Den största nackdelen är att en kund kan uppleva det extra momentet som jobbigt och omständligt när de får en faktura från en ny betalningsmottagare. En kompromiss skulle kunna vara att man vid skickandet av betalningsuppdragen får signera alla nya mottagare i klump eller åtminstone uppmärksammas på att man håller på att betala till en ny mottagare.

4.2 BELOPPSGRÄNSER

Här kan man tänka sig olika lösningar som alla skulle försvåra för en bedragare. En variant är att som Handelsbanken ha dynamiska beloppsgränser där en ny mottagare anses utgöra en större risk och därmed har en snävare beloppsgräns. Ett annat alternativ är att ha dynamiska beloppsgränser för alla mottagare, som skulle kunna förfinas över tid. Ett tredje alternativ är att man kräver ytterligare autentisering om man ska skicka en betalning över ett visst belopp.

Beloppsgränser kan vara problematiska vid sällanköp av kapitalvaror eller större transaktioner och kan upplevas som väldigt inskränkande. Det är därför önskvärt att kunden genom någon form av

ytterligare autentisering kan lyfta beloppsgränsen vid exempelvis ett bilköp. Flera banker har beloppsgränser för kortköp, men inte för fakturabetalningar eller överföringar.

4.3 AUKTORISATION AV NYTT BANKID

För ett år sedan då vi granskade banksäkerheten var det endast SEB som hade krav på ytterligare auktorisation när ett nytt BankID användes för inloggning i Internetbanken. Detta är en mycket stark kontroll för att minimera skadan om en bedragare skulle lyckas utfärda ett nytt BankID till sin egen telefon. Genom att verifiera ett nytt BankID med Bankdosa eller SMS första gången det används uppnår man en högre assuransnivå och kunden behöver bara göra sig omaket en gång när de byter telefon.

4.4 YTTERLIGARE AUTENTISERING VID HÖG RISK

En enkel men effektiv kontroll skulle vara att införa en ytterligare autentisering vid transaktioner eller uppdrag som innebär en högre risk. Flera banker kräver detta exempelvis vid utfärdande av nytt BankID eller vid avtalssignering, men man skulle även kunna införa det för transaktioner över ett visst belopp.

4.5 FÖRDRÖJNING VID ÖVERFÖRING FRÅN SPARKONTO

En fördröjning av överföring från sparkonto kombinerat med en spärr för överföringar till andra konton än egna skulle ge kunderna en chans att upptäcka bedrägeriet innan alla pengarna försvunnit. En överföringsfördröjning på en bankdag hade gjort att chansen att stoppa pågående bedrägerier hade ökat avsevärt. Det hade också minskat incitamentet för kunderna att sprida sina innehav på flera banker för att uppnå samma funktion. Risken med att införa en fördröjning är att kunderna hade upplevt det som begränsande, men kontrollen skulle kunna vara frivillig.

4.6 SMS ELLER PUSH-NOTISER VID HÖG RISK

Detta är också en kontroll som används av en del banker idag. Möjligheten att uppmärksamma kunden på att ett stort belopp har dragits, eller att en transaktion har auktoriserats skulle också öka sannolikheten för att ett bedrägeriförsök stoppas i tid. Det finns egentligen inga nackdelar med att införa kontrollen, men det är viktigt att varningarna är relevanta för att kunderna ska uppmärksamma dem.

4.7 DETEKTION AV AVVIKELSER I TRANSAKTIONSMÖNSTER

Genom att analysera kundernas användarmönster och normala betalflöden skulle man kunna detektera avvikande transaktioner och lägga på en fördröjning eller ytterligare verifiering av att transaktionen är auktoriserad av kunden. Analys av betalflöden används idag för att upptäcka tecken på oegentligheter, samt för marknadsanalys och affärsutveckling. Det skulle gå att använda i större utsträckning för att begränsa skadan vid bedrägerier.

Metoder för avvikelsedetektion och dataanalys förbättras ständigt, men det finns risker förknippade med analys av köpmönster. Integritetsfrågan behöver hanteras och risken för falsklarm är uppenbar. Det skulle kunna leda till att kunder blir irriterade på funktionen och invänder mot personuppgiftsbehandlingen, men känsligare detektion av transaktionsmönster skulle kunna vara frivillig.

4.8 Förstärkt identitetskontroll vid hög risk

Detta är en metod som används för andra typer av tjänster (exempelvis AirBnB) där användaren får ta en bild på sitt ID kort och sedan filma sig själv med mobilkamera eller webbkamera. Det är en relativt integritetsinskränkande metod att identifiera en användare, men skulle kunna användas som ytterligare kontroll vid transaktioner eller uppdrag med mycket hög risk eller avvikelse. Det är stor risk att kunderna skulle kunna uppfatta det som oproportionerligt och det bör därför användas sparsamt.

En annan liknande metod är att i förväg spara biometriska data och sedan använda mobilkamera eller webkamera för att verifiera identiteten, men den metoden har utmaningar ur ett GDPR perspektiv och skulle kunna leda till dålig PR.

Funktionerna behöver dock inte vara obligatoriska utan kan vara påslagsbara för de kunder som så vill.

4.9 Tidsbaserade begränsningar i belopp och funktionalitet

En relativt drastisk åtgärd skulle vara att begränsa funktionalitet och beloppsgränser baserade på tid på dygnet, alternativt fördröja vissa transaktioner tills en banktjänsteman hunnit verifiera att uppdraget ser rimligt ut. På så sätt skulle bankens antibedrägeripersonal kunna agera om något inte ser legitimt ut. Det är dock en stor risk att detta skulle uppfattas som begränsande och inskränkande ur kundperspektivet, men skulle kunna göras frivilligt.

4.10 Användarutbildning

Likaväl som att kunderna med jämna mellanrum tvingas att fylla i ekonomisk information för att banken ska kunna följa penningtvättslagen, så skulle man kunna tänka sig korta utbildningar online som man måste gå. Utbildningarna skulle kunna röra säkerhet och hur man undviker bedrägeri, men också förklara bakgrunden till kundkännedomskraven.

4.11 Möjlighet för kunden att själv anpassa kontrollerna

En möjlig tanke som bank är att presentera ett smörgåsbord av tekniska och administrativa kontroller som kunden själv får välja att slå på eller av. Man kan då tänka sig att en kund med högt säkerhetstänk och låg riskaptit skulle kunna välja att stå ut med större inskränkningar i smidighet mot en högre nivå av assurans. Omvänt kan en kund som prioriterar smidighet och mobilitet välja att avstå från beloppsgränser och betalspärrar.

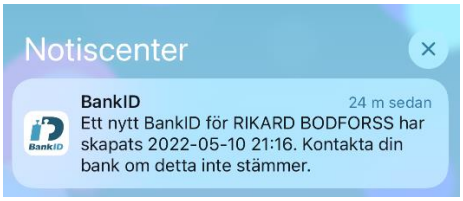
För att öka incitamentet att slå på fler säkerhetsfunktioner kan man införa rabattsatser eller andra ekonomiska incitament baserat på hur många säkerhetsfunktioner som kunden valt att aktivera. Alternativt kan man använda sig av spelliknande utmärkelser (gamification) och visa kundens ”riskpoäng” i internetbanken.

Fördelen med att kunna kundanpassa säkerhetsfunktionerna, baserat på bankens riskbedömningar, är att kunderna inte skulle behöva välja bank för att få eller slippa vissa säkerhetskontroller. Man kan tänka sig att vissa säkerhetsfunktioner skulle kunna kosta extra (till exempel mänsklig verifiering av transaktioner) och att andra skulle kunna medföra rabatter eller andra incitament för att öka användningen. Säkerhet bör ses som en affärsfördel och ett konkurrensmedel snarare än något onödigt ont som skrämmer bort kunder och kostar marknadsandelar.

5 REKOMMENDATIONER TILL BANKKUNDER

Som bankkund har man långtgående krav på sig att skydda sina autentiseringsuppgifter enligt betaltjänstlagen. I några fall[4] som tagits upp i Allmänna reklamationsnämnden (ARN) har bankkundernas agerande befunnits vara ”särskilt klandervärt och de har då tvingats stå för hela beloppet som de lurats på. Det har rört sig om fall då bedragare lurat offren att identifiera sig med BankID eller bankdosa och sedan signera transaktioner, där offren har agerat på ett rejält riskfyllt sätt. När kunderna har varit grovt vårdslösa, men inte handlat särskilt klandervärt, får de enligt betaltjänstlagen stå för 12 000 kr, vilket kan ses som en form av självrisk då man agerat rejält slarvigt med sin bankdosa eller BankID. Beroende på hur ekonomin ser ut kan 12 000 kr vara en betydande del av ens tillgångar. Vid lägre grad av vårdslöshet än ovan, begränsas kundens ansvar till 400 kr.

I vår förra rapport för Villaägarna avhandlade vi sätt att minska risken att bli bedragen, men här är vårt syfte i stället att minska bytet för bedragarna om de skulle lyckas. Det värsta scenariot skulle vara om en bedragare lyckas utfärda ett nytt mobilt BankID till sin egen telefon. Då skulle bedragaren kunna agera självständigt mot en stor del av svenska banker och finansinstitut och systematiskt tömma alla konton i alla banker som offret har engagemang i. Det är därför otroligt viktigt att avbryta en pågående ID-kapning så fort man får en notis om att ett nytt BankID håller på att skapas, oavsett vilka förevändningar bedragaren kommit med. När ett nytt BankID utfärdas kommer det ofta ett SMS från utfärdande bank om att ett nytt ID håller på att skapas och när det har skapats så får man en push-notis till de enheter där man har Mobilt BankID installerat (se Figur 2).



Figur 1 Bild på push-notis från BankID

Skulle detta ske utan att man själv skapat ett nytt BankID för en ny enhet så ska man ringa sin banks spärrservice omedelbart.

Om vi nu antar att bedragaren inte lyckats utfärda ett nytt Mobilt BankID, men ändå lyckats lura bankkunden att autentisera bedragaren och signera en transaktion, så vill vi minimera skadan så mycket som möjligt. Som privatperson är det oftast bäst att vara ”otrogen” mot sin bank och sprida sina tillgångar. Bankerna strävar oftast efter att vara helhetsleverantör för att bättre ha fullständig kontroll på kundernas inkomster och utgifter och lockar med bättre hypoteksräntor och andra villkor om man samlar sina affärer hos dem. Att sprida sina tillgångar kan också vara bra ur privatekonomiskt perspektiv då pengarna inte är lika tillgängliga för impulskonsumtion.

Det man vinner i säkerhet får man ofta offra i smidighet och våra rekommendationer kräver att man behöver ha lite framförhållning när det gäller stora utgifter. I gengäld riskerar man bara sitt månatliga transaktionskapital om man skulle falla offer för ett bedrägeri och bedragaren kommer åt transaktionskontot. För att upplägget ska fungera behöver man ha koll på ungefär hur mycket pengar man omsätter en normal månad, hur mycket pengar man behöver ha i likviditetsbuffert för oförutsedda händelser och större utgifter, samt vilken sparhorisont man har på övrigt kapital.

[4] https://www.arn.se/arn---testsidor/pressmeddelanden/kapning-av-mobila-BankIDn-och-liknande-bedragerier--vad-hander-om-man-blivit-lurad/

Idén är att utnyttja nischbanker där överföringar endast kan ske till egna konton i andra banker för sitt sparkapital och på så sätt skaffa sig extra tid för att hinna kontakta bankerna och stoppa bedrägliga transaktioner. Överföringar mellan olika banker tar mellan några timmar upp till en bankdag att genomföra och denna fördröjning gör att man får mer tid på sig att stoppa bedragarna.

Att vara helhetskund i en bank med betalservice, kontokort, kreditkort, hypotekslån och så vidare kostar en slant varje år. Det kan därför bli dyrt att likt en ekorre ha flera sådana engagemang, men nischbankerna tar oftast inte betalt för att öppna sparkonto hos dem. I det enklaste upplägget som ändå är väsentligt säkrare än att samla alla ägg i en korg så kan det se ut så här:

1. Huvudbank (lämplig storbank) – Används som transaktionsbank. Här går lönen in och räkningar betalas varje månad. Här ska bara så mycket pengar finnas så att det täcker räkningar, lånebetalningar och konsumtion en vanlig månad med lite marginal. Överskjutande belopp förs över till långsiktigt sparande och likviditetsbuffert. Om det är fördelaktigt kan man även ha sitt hypotekslån i denna bank.
2. Likviditetsbuffert (lämpligen nischbank) – Här sparar man på ett sparkonto, där det bara går att göra överföringar till transaktionskontot hos huvudbanken. Sparkontot ska inte ha några utbetalningsbegränsningar, men borde ändå kunna ge en positiv sparränta. Detta konto ska användas för oförutsedda utgifter eller större konsumtionsutgifter som går utöver budget för en normal månad. Det kan vara en semesterresa, renovering, byte av bil, eller andra större kostnader. När man ser att räkningarna en månad överstiger vad som finns på transaktionskontot för man över pengar från detta konto för att täcka underskottet.
3. Långsiktigt sparande (lämpligen nischbank eller nätmäklare) – Här sparar man på längre sikt än ett år. Beroende på sparhorisont så kan man antingen spara i låsta sparkonton, räntefonder, aktiefonder, derivat eller andra finansiella instrument beroende på kunskap och risknivå. Uttag från detta sparande kräver ofta planering så att man inte behöver sälja med förlust eller att pengarna är låsta då de behövs. Även här ska bara överföringar kunna göras till det egna kontot i Huvudbanken.

Detta upplägg kräver framförhållning när det gäller större utgifter och man offrar smidigheten att ha överblick på alla sina tillgångar. Vill man ta det ytterligare ett steg kan man dela på transaktionskontot för räkningar och det konto som är anslutet till Swish. Helst ska man då ha dem på olika banker så att det är en fördröjning på överföringar till och från Swishkontot. I inställningarna för Swish ska man också ställa in beloppsgränser som motsvarar den normala användningen. Om man vid något tillfälle behöver höja beloppsgränsen för att göra ett större inköp (till exempel en båt eller en bil) så går det att lyfta beloppsgränsen temporärt. På så vis begränsar man de belopp som en bedragare kan komma över snabbt. Att dela upp transaktionskontot och Swish på olika banker kan medföra ytterligare avgifter till banker.

En ytterligare åtgärd som man kan vidta är att skaffa ett kreditkort som inte är kopplat till något bankkonto för alla korttransaktioner. Det förutsätter dock att man kan hantera en kredit och inte lever över sina tillgångar. På så sätt kan en bedragare inte tömma transaktionskontot om man skulle bli av med sina kreditkortsuppgifter. Man får oftast betala en årlig avgift för kreditkortet som måste tas med i beräkningen och om man inte betalar av sina kreditköp varje månad kan det lätt bli väldigt dyrt.

> Hur man ska fördela medel mellan olika sparformer och vilka kostnader för banktjänster man tycker är rimliga, varierar individuellt. Vi ger därför inga rekommendationer på belopp eller sparformer. Det bistår däremot bankerna gärna med.

Det bästa sättet att minska risken för bedrägerier är förstås att inte låta sig luras alls. Grundregeln för att undvika bankbedrägerier är som alltid: Banken ringer aldrig upp och ber att du ska legitimera dig! Aldrig! Om någon utger sig för att vara banken och vill att du ska legitimera dig, lägg på luren och ring upp bankens kundtjänst själv. Det är bara när du ringer banken som de vill att du identifierar dig med BankID eller dosa. Detsamma gäller epost med länkar till banken. Det är bättre att själv starta en webbläsare och logga in på sin internetbank än att klicka på länken.

Ett generellt tips är att aktivera push-notiser i din bank-app på mobilen. Detsamma gäller om man har kreditkort med en app kopplad till kortet. Då kan man få en notifiering så fort en kortdragning har gjorts eller stor utgift har dragits från kontot. Det ger en bra möjlighet att snabbt kunna agera om olyckan skulle vara framme och dina kortuppgifter hamnar i orätta händer. En snabb åtgärd vid misstänkt bedrägeri kan många gånger minimera skadan och förhindra att bedragarna tömmer kontot.

6 SLUTSATS

Ansvaret för att minska volymen av bankbedrägerier vilar både hos bankerna och hos deras kunder. Det är naivt att tro att det går att lagstifta bort bedrägeribrotten. Fler regleringar kommer inte att leda till några väsentliga minskningar i brottslighet. Om man både från kundernas och bankernas sida lyckas göra bankbedrägerier svåra att genomföra och olönsamma ställt i förhållande till arbetsinsatsen, så kommer antalet lyckade bedrägerier att minska. Det behöver dock inte innebära att brottsligheten totalt sett minskar, utan att gärningspersonerna inriktar sig på annan brottslighet.

Metoder som fördröjer eller minimerar beloppen som brottslingarna kommer över, leder till att fler bedrägerier stoppas och att skadorna för den enskilde minskar. Som konsument har man ett ansvar att minimera sin exponering och att skydda sina tillgångar, men bankerna skulle kunna erbjuda fler metoder för att minska bedragarnas möjligheter att tömma kundernas konton. Framför allt skulle valbara spärrar minska behovet för kunderna att själva sprida riskerna.

Fördröjning av överföringar från sparkonton skulle dessutom kunna förbättra kundernas privatekonomi genom att minska risken för impulskonsumtion. Detta skulle kosta lite i minskade transaktionsintäkter, men skulle minska incitamentet att använda flera banker och på så sätt öka möjligheten att behålla kunderna som helhetskunder.

Balansgången mellan smidighet och säkerhet behöver inte vara en kamp mellan säkerhetsavdelningen och marknadsavdelningen. I stället kan säkerhetsfunktionerna – precis som när det gäller bilar – utnyttjas som en marknadsfördel och ett konkurrensmedel. Speciellt om man kan erbjuda dem som frivilliga valbara kontroller. Säkerhetsfunktioner som man vill att kunderna ska använda kan marknadsföras med olika incitament, medan mer kostsamma kontroller skulle kunna erbjudas mot en extra kostnad för kunden.

Som privatperson kan man vidta åtgärder redan idag för att minska konsekvenserna om man skulle falla offer för ett bedrägeri. Framför allt ska man utgå ifrån sin privatekonomiska situation och göra en riskbedömning baserat på hur mycket man skulle klara av att förlora utan att privatekonomin går omkull. Baserat på detta bör man sprida sina risker och minimera skadan om någon obehörig skulle få tillgång till ens konto. Att sprida sina tillgångar på olika banker är ett bra alternativ som gör att man inte står barskrapad om olyckan är framme.

Slutligen tror vi på att användarutbildning inte bara är något som bör ske internt utan att bankerna bör ta ett ansvar för att medvetandegöra kunderna om hot och risker. Det skulle öka förståelsen för varför vissa transaktioner behöver fler kontroller. Modern teknik innebär också större möjligheter att upptäcka oegentligheter utan att för den skull inverka negativt på användarnas upplevelse av smidighet.