KORTTRICKET

SÅ BLIR DU LURAD PÅ NÄTET

Björn Eriksson

FÖRORD

Visste du att kortbedrägerier numera är så vanliga att det finns en organiserad svart marknad för stulna kortuppgifter med standardiserade priser och kundsupport dygnet runt?

Det låter som fiktion men är alldeles sant. Vi hör inte så mycket om det bara. En anledning är att bankerna och kortföretagen helst inte vill prata så högt om problemen. De tjänar nämligen så mycket på varje kortbetalning att de pengar de förlorar på bedrägerierna är något de kalkylerar med. De ersätter hellre sina kunder snabbt och diskret, helst också utan att blanda in polisen.

Men vi tycker att problemet är för allvarligt för att tigas ihjäl. Bankerna kommer inte i evighet att ersätta sina kunder för de allt större förlusterna och det kan inte heller vara rätt att bankerna genom sitt förhållningssätt faktiskt stöder organiserad brottslighet.

Vad tycker du?

Björn Eriksson
Ordförande, Säkerhetsbranschen

KORTBEDRÄGERIER – ETT VÄXANDE SAMHÄLLSPROBLEM

Det är bekvämt att handla med kort. Vi trycker ner våra kort i dosan vid kassan och knappar in kontonummer och CVC-kod i nätbutiken, utan att bekymra oss speciellt mycket över vilka uppgifter vi samtidigt lämnar ut. Vi litar på att säkerheten fungerar.

Men faktum är att kortbedrägerierna ökar rekordartat. Varje år förlorar våra banker miljonbelopp till kortbedragare av olika slag. Samtidigt är intäkterna från kortbetalningar ett av bankernas mest lönsamma affärsområden. Så länge intäkterna för kortbetalningarna med råge överstiger kostnaderna för bedrägerierna väljer bankerna att se bedrägerierna som en kostnadspost bland andra, ungefär som ”utgifter för inkomsternas förvärvande”.

Omfattningen av bedrägerierna är något som bankerna inte gärna pratar om. Bankerna verkar i en förtroendebransch och de är medvetna om att förtroendet för deras säkerhetssystem skulle skadas rejält om det kom ut till kunderna hur utsatta de verkligen är. Bankerna lägger därför locket på, försöker så långt som möjligt att ersätta sina kunder utan omsvep, och om möjligt, utan att blanda in polisen.

Frågan är varför vi accepterar detta. Det är vi kunder som i slutändan får betala kalaset i form av ökade bankavgifter och förlorad integritet. Samtidigt tillåter vi bankerna att genom sin passiva hållning indirekt hålla kriminella verksamheter om ryggen.

Med den här skriften vill vi som värnar om kontanter öka medvetenheten om nätbedrägeriernas omfattning och konsekvenser. Vi diskuterar också bankernas hållning i frågan och hur vi kan förmå dem att ta ett större samhällsansvar.

Card present – vanligare förr

Vad är då kortbedrägerier? Grovt sett kan de idag delas in i två typer. Den traditionella typen kallas CP, Card Present, och är bedrägerier som kräver att man har tillgång till ett fysiskt kort för att kunna begå ett bedrägeri. Det kan handla om att någon ser över axeln hur en kund knappar in sin kod vid kassan och sedan helt enkelt stjäl kortet. Eller så kanske det handlar om så kallad skimning, det vill säga att någon manipulerar en bankomat eller en kortläsare för att kunna läsa av magnetremsan på kortet som offret använder.

Card Present-brott är lättast att lösa, men de är inte så vanliga längre eftersom banker gått över till säkrare lösningar med chipkort och koder.[1]

Card not present – ökar lavinartat

Den andra typen av bedrägerier brukar gå under begreppet CNP, Card Not Present. Det är bedrägerier som kan göras utan att man behöver ha tillgång till det fysiska kortet. Det räcker med att man har kommit över kortuppgifterna och CVC-koden. Koderna kan man komma åt på olika sätt. Nätfiske kallas det när bedragaren skickar ett mejl som ser ut att komma från någon seriös aktör som banken eller Skatteverket som uppmanar offret

1 Intervju med Konsumenternas bank och finansbyrå den 13 oktober 2016.

att lämna ut sina koder. Men de allra flesta CNP-brott sker genom it-intrång hos företag eftersom man på så sätt kan komma över en mängd id- och kortuppgifter i ett enda svep.

CNP-brott är den typ av brott som är vanligast, som ökar snabbast och som är den största utmaningen inom en överskådlig framtid vad gäller bedrägerier. Det menar Nationellt bedrägericentrum, en organisation skapad 2012 för att specialisera sig på just kort- och internetbedrägerier.[2]

Trojaner vanliga i bedrägerier

Det vanligaste sättet att göra dataintrång på är att använda sig av så kallade trojaner. En trojan är ett litet program som installerar sig själv på användarens dator, oftast via ett mejl med en bifogad fil som bär trojanen. När användaren lurats att klicka på bilagan installeras trojanen, som då exempelvis kan börja samla in uppgifter som personnummer, kortuppgifter och lösenord som offret använder. Informationen skickas sedan till någon e-mejladress som gärningsmannen anger.

Det finns också speciella banktrojaner som är programmerade för att ta kontroll över kommunikationen mellan bankkunden och bankens servrar när kunden loggar in på sin internetbank. Trojanen kan manipulera de transaktioner som användaren själv genomför på kontot, genom att till exempel ändra beloppet vid en kontoöverföring eller omdirigera överföringar till andra mottagarkonton.[3]

2 Intervju Nationellt Bedrägericenter på Polismyndigheten oktober 2016.

3 Se t.ex. Buescher m.fl. 2011, Goldberg och Larssson 2013.

– Vi ser en trend att fler banktrojaner skräddarsys för svenska banker och användare. Dessutom kan finansiella trojaner attackera mer än bara banker, exempelvis system som Bitcoin och PayPal, säger säkerhetsforskare på Kapersky Lab.[4]

Behöver inte vara avancerat

Men att begå kortbedrägerier behöver inte vara så avancerat. Det går faktiskt bra även med en vanlig bankdosa. Trots att bankdosan räknas till ett av de absolut säkraste legitimeringssätten idag, kräver inte alla banker att vi personligen går in på kontoret och legitimerar oss för att få ett bank-ID, utan det kan göras direkt på internet. Det är alltså relativt lätt att komma över en annan persons bankdosa och kortuppgifter och därmed kan man begå en mängd bedrägerier med en mycket liten risk att bli upptäckt.[5]

Inte ens e-legitimationer är alltid säkra. 2015 upptäcktes en brist i Telias e-legitimationer som gjorde att bedragare kunde komma åt och länsa konton som hörde till några av topparna inom svenskt näringsliv. Exempelvis blev finansmännen Christer Gardell och Mats Arnhög av med sammanlagt över fem miljoner kronor i den vevan. Bedragarna hade hämtat de känsliga uppgifterna med vanlig post i en Ica-butik.[6]

Finns inga säkra sajter

Som konsument får man ofta höra rådet att enbart använda säkra sajter när man ger ut sina identitetsuppgifter. Men faktum

4 http://skyddosakerhet.se/nyheter/fler-banktrojaner-skraddarsys-for-sverige/

5 Brå rapport 2016:9.

6 http://www.dn.se/arkiv/nyheter/natbedragare-stal-miljoner-fran-naringslivstoppar/

är att det inte finns några helt säkra sajter. Även stora, välkända sajter med förmodad hög it-säkerhet blir hackade. 2014 blev exempelvis Yahoo bestulet på femhundra miljoner kortuppgifter, Adobe 152 miljoner och Ebay 145 miljoner kortuppgifter.[7]

Inte ens länders centralbanker går fria från bedrägerier och attacker. 2013 drabbades USA:s centralbank, FED, av dataintrång där bland annat inloggningsuppgifter för 4000 anställda läckte ut på nätet.[8] I mars 2016 drabbades Englands centralbank Bank of England av cyberattacker, ett brott som fortfarande är under utredning.[9]

Hur används de stulna uppgifterna?

Vad händer då med alla kortuppgifter och koder som stjäls vid dataintrången? Oftast säljs de vidare på olika forum på nätet. Ibland sker det helt öppet, men för det mesta sker det på den del av nätet som inte nås via de vanliga sökmotorerna, det som går under benämningen Darknet. Sedan början av millenniet har det växt fram en allt mer organiserad och sofistikerad svart marknad för stulna kortuppgifter på nätet, en marknad som till och med har kundsupport dygnet runt och standardiserade priser på sina tjänster. För närvarande ligger paketpriset på kontokortsuppgifter inklusive namn, giltighetstid och cvv-nummer på 250 kronor styck.[10]

Enkla jobb och låga straff

Varför ökar då kortbedrägerierna så mycket? En anledning är att de är så enkla att utföra. Man behöver inte utsätta sig själv

7 Uppgifter från Nationellt Bedrägericentrum, NBC, 2016.

8 http://computersweden.idg.se/2.2683/1.490745/usas-centralbank-erkanner-vi-hackades

9 http://www.di.se/artiklar/2016/3/15/allvarligt-cyberhot-mot-bank-of-england/

10 http://www.svd.se/kortbedragerier-okar-lavinartat--svart-att-skydda-sig

för någon fysisk fara utan kan begå brottet hemma i soffan med en laptop i knät. Många gärningsmän vittnar också om att de får ett slags distans till brotten de utför. Ett nätbedrägeri känns mer abstrakt än ett fysiskt rån eller stöld och bankerna brukar ju dessutom ersätta offren direkt. Därför är det bara storbankerna med sina redan välfyllda kassakistor som drabbas, resonerar de.[11]

Bedrägeribrott är dessutom ett oprioriterat område där straffvärdet är lågt i förhållande till den potentiella vinsten. Medan ett grovt bedrägeri bestraffas med sex månaders till sex års fängelse är straffskalan för grovt rån mellan fyra och tio års fängelse. Som grädde på moset är risken att åka fast minimal. Brotten är mycket svåra att utreda. Endast ca 10 procent av den här typen av brott blir lösta enligt Nationellt Bedrägericentrum, NBC.[12]

Och när någon grips är det ofta en målvakt som inte vet något om vilka som egentligen ligger bakom bedrägeriet. Dessa brott ingår ändå i statistiken som uppklarade.[13]

Bra förutsättningar för id-kapningar i Sverige

Något som gör det särskilt enkelt att begå bedrägerier i Sverige är att det är ovanligt lätt att få tag i personuppgifter i landet. Vi använder våra personnummer nästan dagligen när vi visar våra id-kort i olika sammanhang. Vi har dessutom ovanligt många typer av godkända ID-handlingar, något som underlättar för förfalskare. I dag finns det cirka 15 godkända id-handlingar i Sverige som utfärdas av Polisen, Skatteverket, Transportstyrelsen, vissa större banker, företag och myndigheter.

11 Goldberg Larsson, Korthuset.

12 https://polisen.se/PageFiles/471893/NBC_L%C3%A4gesbild_2014.pdf

13 Goldberg, Larsson, Korthuset.

Vi svenskar är dessutom unika när det gäller att utan reflektion lägga ut mängder av uppgifter om oss själva på nätet. När vi använder våra betalkort i kassan eller på e-handelssajten, när vi läser av våra månadskort på tunnelbanan, när vi lägger upp bilder i sociala medier eller när vi rör oss med våra telefoner i fickan så lämnar vi digitala spår som går att följa. Spåren berättar överraskande mycket om våra beteendemönster och identiteter, uppgifter som kan säljas vidare, lagligt eller olagligt. Vår svenska benägenhet att betala även småbelopp med kort gör dessutom att vi skapar fler tillfällen att analysera våra digitala spår än vad som är fallet i de flesta andra länder.

Vad kostar kortbedrägerierna?

Digitaliseringen har gjort det möjligt att utföra bedrägerier i en helt annan skala än tidigare när beloppet begränsades av hur mycket kontanter man kunde få med sig i en flyktbil. Tyvärr redovisar inte bankerna sina förluster från kortbedrägerier och därför är det svårt att beräkna omfattningen av dem. Trots många propåer genom åren vill bankerna inte lämna ut någon öppen statistik över bedrägerierna och deras kostnader, varken till allmänheten eller till polisen. Det skulle undergräva förtroendet för dem om allmänheten fick veta hur mycket det rör sig om, är deras inställning.[14]

ECB, den europeiska centralbanken, har dock börjat sätta samman statistik på kortbedrägerier sedan några år tillbaka. Den senaste, från 2013, visar att bedrägerier omfattar 0,023 procent av värdet av kortbetalningarna i Sverige.[15] Eftersom svenskarna genomförde kortbetalningar för 500 miljarder

14 Goldberg, Larsson, Korthuset.

15 ECB, Forth report on card fraud, July 2015.

kronor[16] samma år, bör kortbedrägeriernas omfattning ha landat på cirka 110 miljoner kronor år 2013.

Detta är dock bara toppen på isberget enligt NBC, som bedömer att de allra flesta bedrägerier aldrig rapporteras eftersom bankerna systematiskt ersätter de flesta kunders förluster direkt, utan att blanda in polisen.[17]

Bankerna vill inte ha någon inblandning

Det sista bankerna vill är att omfattningen av kortbedrägerierna kommer upp till ytan. De vill i så stor utsträckning som möjligt ta hand om problemen själva. I sin interna kamp mot cyberbrottslingarna har bankerna byggt upp omfattande övervakningssystem som scannar av, samlar in och analyserar alla kunders korttransaktioner. Bankerna vet därför exakt vad vi brukar handla, för hur stora belopp, var vi brukar befinna oss när vi gör köpen och mycket mer, vilket gör att de snabbt kan fånga upp transaktioner som bryter mot våra konsumtionsmönster. Det kan handla om att beloppet verkar orimligt stort, att uttaget är gjort på en osannolik plats eller att själva köpet verkar osannolikt.

Kunden får inte se vad som hänt på kontot

Om systemet fångar upp en misstänkt transaktion brukar bankerna agera preventivt och spärra kortet i samråd med kunden. Kunden brukar få ett nytt kort och banken ersätter förlusten. Därmed vill banken att ärendet ska vara avklarat. För att det ska bli så lite uppståndelse som möjligt brukar kunden

16 Visa Annual Results 2014.

17 https://polisen.se/PageFiles/471893/NBC_L%C3%A4gesbild_2014.pdf

inte få se några spår på sitt konto av vad som hänt: banken sätter helt enkelt tillbaka pengarna utan att bedragarens uttag eller bankens kompensationsinsättning redovisas på kontot. Banken vill inte heller gärna informera om i vilket sammanhang kortuppgifter har läckt eller hur bedrägeriet gått till – om det skett i en butik, i en uttagsautomat eller via ett dataintrång. Inte heller hur många svenskar som varje år drabbas av detta brott vill man berätta.[18] [19] Det ligger inte i bankernas intresse att anmäla dem, och enligt NBC har de inte heller resurser för att göra det.[20]

Få bedrägerier polisanmäls

Bankernas princip är att det är kundens pengar som försvunnit när ett bedrägeri har begåtts. Banken anser sig alltså inte vara brottsoffret utan hänvisar kunderna till att själva anmäla bedrägerierna. Det gör polisens situation svår. Istället för att få en samlad anmälan från banken med alla bedrägerier från exempelvis en viss dator, tvingas polisen hantera mängder av enskilda anmälningar och utifrån dessa försöka hitta mönster bland dessa.[21]

Eftersom det är upp till kunden att anmäla är det enbart de bedrägerier där kunden är informerad eller själv sett att belopp dragits från kontot, som polisanmäls. Det betyder att den stora mängden kortbedrägerier som ännu inte upptäckts av kunden varken blir föremål för polisundersökningar eller fångas upp i statistiken.[22]

18 http://www.svd.se/banker-morkar-om-kapat-kort/om/naringsliv

19 Intervju Dick Malmlund.

20 Intervju med Jan Olsson, NBC den 13 oktober 2016.

21 Korthuset, Goldberg, Larsson.

22 Bedrägeribrottsligheten i Sverige, Brå 2016:9.

Kortbetalningar är bankernas kassako

Varför är då bankerna så inställda på att vi ska betala med kort trots de omfattande bedrägerierna? Svaret är helt enkelt att kortbetalningar är en oerhört lönsam affärsverksamhet för bankerna.

År 2012 gjorde riksbanken en uppskattning av bankernas intäkter från kort, som då landade på omkring 8,5 miljarder kronor exklusive ränteintäkter på kreditkort.[23] Av intäkterna kom 60 procent från de avgifter som handlaren betalar till banker och kortföretag för att kunna ta emot kort. Resten står kortbetalarna, det vill säga vi konsumenter, för i form av transaktionsavgifter. Runt 2014 gjordes närmare två miljarder kortbetalningar i Sverige och andelen kortköp ökar stadigt.

År 2015 införde EU ett maxtak för hur mycket bankerna får ta ut i så kallade mellanbankavgifter från handeln. Taket ligger nu på 0,2 procent för bankkort (debetkort) och 0,3 procent för kreditkort. De minskade intäkterna från handeln tar bankerna nu igen på oss konsumenter i form av ökade kortkostnader.[24] Enligt Handelns utredningsinstitut lägger hushållen ned runt 1 500 kronor per år bara på kortkostnader.[25] Denna siffra har med största sannolikhet ökat efter införandet av maxtaket.

Kriminaliteten – en kostnadspost bland andra

Det är alltså av största vikt för bankerna att kunderna fortsätter att handla med kort. Därför gör bankerna ständiga avvägningar

23 Riksbankens rapport kontanter eller kort, hur bör vi betala, 2012.

24 https://www.svd.se/dyrare-kort-for-svenska-bankkunder/om/debatten-om-kontanterna

25 https://www.compricer.se/nyheter/artikel/nu-blir-det-hogre-avgifter-pa-bankkorten

mellan säkerhet och enkelhet för användaren. Högre säkerhet betyder ofta mer krångel i form av fler säkerhetskoder eller längre väntetider och riskerar att kunderna väljer smidigare betalsätt. Att stoppa fler, eller för all del alla bedrägerier, kanske vore möjligt för bankerna, men är inget självändamål. Så länge kundernas kortbetalningar genererar de intäkter de ska, accepteras kostnaderna för kriminaliteten och betraktas helt enkelt som en kostnadspost bland andra.[26]

Vi betalar för bankernas förluster

Vi har tidigare konstaterat att bankerna har som policy att så långt som möjligt ersätta oss kunder för att vi ska vara nöjda och inte väcka en debatt i onödan. Men bankernas kostnader för de generösa ersättningarna måste ju plockas ut någonstans. Det gör bankerna genom att höja avgifterna för sina tjänster eller att införa nya kreativa avgifter, allt från höjda årsavgifter, transaktionsavgifter, uttagsavgifter, insättningsavgifter, valutaväxlingsavgifter, till höjda räntor på krediter – avgifter som vi konsumenter i slutändan står för.[27]

Att det finns gränser för generositeten även från bankernas sida får vi nog räkna med i framtiden. Om bankerna får som de vill och kontanterna försvinner till förmån för kortbetalning eller andra digitala betalsätt, kommer också incitamenten för bankerna att ersätta kunderna som blivit bedragna att försvinna. Då finns det nämligen inte längre några konkurrerande alternativ till digitala pengar.[28]

26 Korthuset, Goldberg, Larsson.

27 Information från intervju med Nationellt Bedrägericentrum 2016.

28 Dick Malmlund intervju 2017.

Bankernas hållning stöder kriminalitet

Men det är inte bara kunderna som får betala för bankernas förluster. Även samhället i stort drabbas av bankernas agerande. Det faktum att bankerna betalar sig ur bedrägerierna genom att göra upp direkt med kunden utan att blanda in polisen innebär faktiskt indirekt att de håller en omfattande kriminalitet om ryggen.

Att se mellan fingrarna med stölderna göder kriminaliteten och skapar en inkörsport till grövre brottslighet. Polisen ser kopplingar mellan storskaliga kortstölder, våldsbrott och narkotikahandel. De ser hur pengar strömmar ut ur betalsystemen och landar hos kriminella ligor. De ser också hur människor utnyttjas som målvakter och dras in i en kriminell värld, där de inte sällan går över till grövre brott.[29]

Vad gör polisen?

Sedan 2008 har polisen satsat allt mer på att utreda bedrägeribrottsligheten. I och med bildandet av Nationellt Bedrägericentrum 2012, kan nu polisen samordna sina resurser så att de kan upptäcka bedrägerier som hänger ihop, oavsett om bedrägerierna handlar om bluffakturor, banktrojaner, skimning eller bidragsbedrägerier.[30]

Organisationen är ett värdefullt tillskott till brottsbekämpningen, men obalansen mellan brottsvolymen och de tillgängliga utredningsresurserna är stor. Förutsättningarna för att utreda kort- och kreditbedrägerier är också mycket svåra. Det finns

29 Larsson, Goldberg, Korthuset.

30 https://polisen.se/Arkiv/Nyhetsarkiv/Gemensam/Polisen-startar-nationellt-bedragericenter/

sällan möjlighet att följa pengarna genom hela transaktionskedjan, och många anmälningar läggs ner, antingen för att de anses vara icke utredningsbara eller för att det inte varit möjligt att identifiera någon misstänkt person.

Den enskilt vanligaste orsaken till nedläggning av anmälning av kortbedrägeri är att brottet inte går att utreda. Beslutet fattas i regel direkt efter att anmälningen registrerats.[31]

31 Bedrägeribrottsligheten i Sverige, BRÅ 2016:9.

STÄLL KRAV PÅ BANKERNA

Nu har vi sett hur bankerna hanterar kortbedrägerier. Vi kan konstatera att bankerna inte är intresserade av att stävja någon brottslighet – i alla fall inte om det innebär sämre vinst för dem själva. Det är i sig naturligt. Även om de flesta av oss ser dem som något slags förmedlare av samhällsservice, är storbankerna privata bolag och i första hand lojala mot sina aktieägare.

Därför måste vi själva väcka och driva frågan om bankernas samhällsansvar. Att bankernas agerande, det vill säga ”blunda och betala”, innebär ökade kostnader för oss kunder är allvarligt i sig. Men ska samhället även acceptera att bankerna genom sitt passiva förhållningssätt indirekt håller kriminell verksamhet om ryggen?

Tvingande lagstiftning krävs

Som bankkunder är det rimligt att vi kunder får veta vilka risker vi utsätter oss för i en betalsituation. Vi måste kunna känna oss trygga med att den bank vi väljer är säker. Därför måste vi ställa krav på att bankerna klart och tydligt redovisar omfattningen av bedrägerierna och vad de kostar i sina resultat- och balansräkningar.

Självklart bör också bankerna redovisa de uttag som sker på våra konton vid bedrägerier. Att det inte görs är en fullständig gåta. Har köp gjorts kopplat till ett konto måste det rimligen redovisas och inte som nu, ersättas utan att vi ser ett enda spår av vad som skett.

Bankerna har sedan länge en överenskommelse, ett slags ”gentlemen’s agreement” med varandra som innebär att de aldrig inbördes konkurrerar med säkerhet. En enskild bank skulle kunna bryta mot regeln och vinna på det kortsiktigt, men långsiktigt skulle förtroendet för hela bankvärlden äventyras om den typen av diskussioner kom upp till ytan. Därför är det viktigt att vi får till en tvingande lagstiftning som kan bryta upp sådana överenskommelser.

Bankerna bör också förmås att polisanmäla alla bedrägerier som kommer till bankens kännedom. Att lägga anmälningsskyldigheten i händerna på kunderna genom att hävda att de är målsägande är att göra det för lättvindigt för sig. Här måste bankernas samhällsansvar tydliggöras.

VÄG RISKERNA – ANVÄND KONTANTER SOM ALTERNATIV

De viktigaste insatserna för att minska bedrägeribrottsligheten är våra egna förebyggande åtgärder. Innan vi slentrianmässigt ger ut våra konfidentiella uppgifter på internet bör vi ställa oss ett antal frågor:

Vilket betalsätt är bäst i just detta sammanhang, kontant eller kort? Om jag ska betala digitalt, litar jag på sajten? Vilka digitala spår lämnar jag? Hur kan de komma att användas?

Tänk på att:

- Med kortköp lämnar du ut data om dig som du inte har någon kontroll över. Kontanter lämnar inga digitala spår som kan komma i orätta händer.
- Kontanter har ingen kredit. Det går inte att bli av med mer än den mängd kontanter man förfogar över.
- Kontanter är ett robust betalmedel som går att använda även vid strömavbrott eller datastopp.
- Det är lättare att göra impulsköp med kort.
- Om kontanterna försvinner och alla betalningar blir digitala, försvinner också din konsumentmakt gentemot banken när du inte längre kan ta ut dina egna pengar från banken.

CHECKLISTA – VAD KAN DU GÖRA SOM KONSUMENT?

Som enskild konsument kan du själv tänka på en hel del saker för att undgå bedrägerier:

- Fyll inte i Googles autospara i formulär och uppgifter när du uppger dina kortuppgifter på nätet.
- Var uppmärksam på folk som tittar över axeln när du tar ut pengar från en bankomat.
- Kontakta din bank och lås ditt kort geografiskt (geoblocking).
- Inse att ditt kort är en värdehandling. Tänk på att alltid ha det under uppsikt.
- Lämna aldrig från dig kort eller kortnummer i annat syfte än att betala.
- Använd ett kort som genererar en faktura. Undvik att använda kort som direkt belastar ditt huvudsakliga bankkonto.
- Använd bara kortet för onlineköp om du litar på säljaren.
- Se till att alltid hålla din PIN-kod dold för andra.
- Kontrollera bankomater innan du använder dem. Dölj PIN-koden med handen medan du slår in den.
- Kontrollera alltid att beloppen på en faktura stämmer överens med dina egna kvitton.
- Var försiktig med att använda ditt bank-ID i situationer där du själv inte tagit initiativ till relationen, exempelvis om du blir uppringd och ombedd att identifiera dig med ditt bank-ID.

- Betrakta din mobiltelefon som en värdehandling, speciellt om du har ett bank-ID installerat på den.
- Lämna inte ut för detaljerad information om dig själv på Facebook eller i andra sociala medier. Om någon som påstår sig vara en kompis ber om hjälp via chatt: ring upp eller ställ kontrollfrågor!
- Spärra ditt stulna ID. Om du tappat bort en identitetshandling, polisanmäl och spärra den hos utfärdaren. Du kan även försvåra för bedragarna genom att aktivera notiser på mobilt bank-ID. Det går även via din internetbank att kontrollera vilka bank-ID:n som finns utgivna på ditt personnummer.
- Använd lösenord med specialtecken, versaler och siffror. Använd inte samma lösenord till dina viktigaste tjänster som exempelvis din e-post, eller något annat du har medlemskap i. Passa även på att byta lösenord med jämna mellanrum.
- Var uppmärksam på vilken post du får, till exempel bekräftelser och besked om adressändring. Byt till en låsbar brevlåda eller postfack.
- Det finns inga seriösa företag, myndigheter eller organisationer som ber om dina kortuppgifter via mejl. Radera sådana mejl eller ring och kontrollera vad det handlar om.
- Ge inte ut konfidentiell information i onödan. Fundera på om kortbetalning är det bästa alternativet.

ANTECKNINGAR

Kortbedrägerier är något vi allt oftare hör talas om. Men hur vanliga är de egentligen? Vilka drabbas? Och vilka kan man ställa till svars för att miljonbelopp varje år göder kriminell verksamhet?

Det är frågor som den skrift du nu håller i handen vill försöka besvara.

Stockholm 2017