DEN STORA GUIDEN OM ID-KAPNINGAR OCH NÄTBEDRÄGERIER

En handbok i hur du undviker att bli ID-kapad

FÖRSÄKRINGAR FÖR EN DIGITAL VÄRLD

VARFÖR EN GUIDE OM ID-KAPNINGAR OCH NÄTBEDRÄGERIER?

Under de senaste året har över två miljoner personer blivit utsatta för ett försök till ID-kapning i Sverige. Av alla de här försöken är det runt 200 000 som fastnar i fällan och drabbas årligen vilket gör ID-kapningar till ett av våra absolut vanligaste brott. Så gott som alla ID-kapningsförsök genomförs idag över nätet och är ofta en del, eller slutmålet, med någon annan form av nätbedrägeri.

mySafety Försäkringar såg tidigt utmaningarna kring ID-kapningar och var även det första företaget att erbjuda en försäkring specifikt på området.
Det gjorde vi redan 2008, långt innan de flesta andra försäkringsbolag insåg problematiken och kom med på banan. Det har tyvärr gett oss en unik inblick i hur de här brotten fungerar och hur de utvecklats över tid.

Vår erfarenhet säger oss också att det bästa skyddet mot en ID-kapning är kunskap. Ju mer vaksam du är, särskilt när du använder internet och sociala medier, desto mindre risk för att du blir såväl utsatt för försök som faktiskt går i fällan. Den här guiden har som målsättning att allt fler ska förstå när de är på väg att bli utsatta för en ID-kapning och att få allt fler att polisanmäla när de drabbas. Vi vill också reda ut en del vanliga frågor kring vad en ID-kapningsförsäkring faktiskt är.

VAD ÄR EN ID-KAPNING?

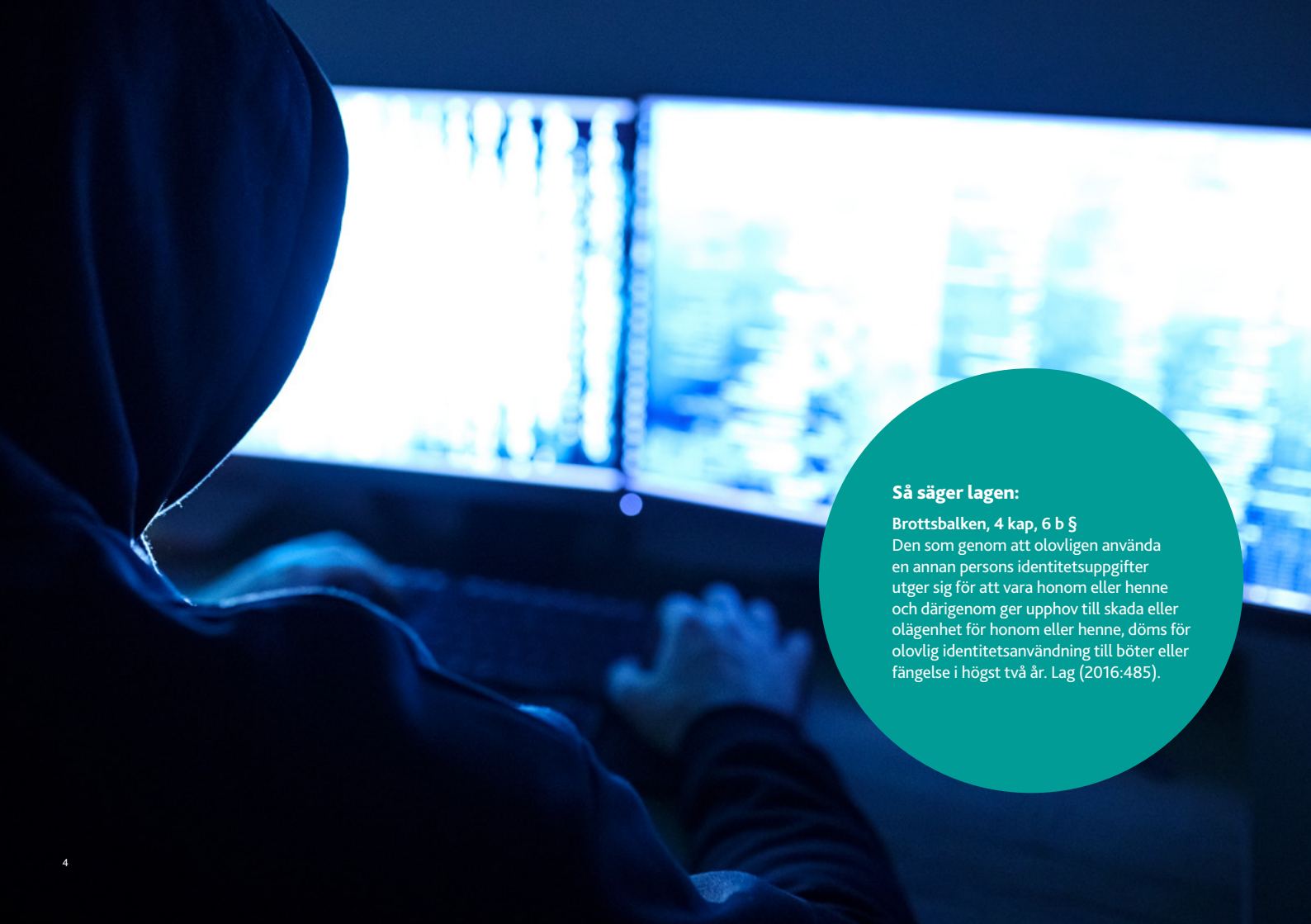
En ID-kapning är, enkelt förklarat, när någon använder dina personuppgifter utan din vetskap eller ditt godkännande. Det kan handla om allt från att någon handlar något över nätet i ditt namn och med dina kortuppgifter till att någon använder sig av dina personuppgifter för att komma över ditt bankkonto eller ta lån där du själv inte ser röken av pengarna.

Sedan 2016 är det förbjudet att ID-kapa någon i Sverige. Det låter kanske lite konstigt att det inte var det tidigare, men då resonerade rättsväsendet att det som gjordes med en stulen identitet i sig var det som skulle straffas, om det var olagligt. Till slut började dock problemet bli så stort att lagen om ”olovlig identitetsanvändning” togs fram. Tyvärr har den inte resulterat i något större antal domar, trots att antalet brott ökar konstant.

VAD ÄR ETT NÄTBEDRÄGERI?

Ett nätbedrägeri är i sin tur något mycket vidare. Men faktum är att vi i dag kan se att väldigt många nätbedrägerier syftar till att även komma åt dina identitetsuppgifter. Ett typexempel kan vara att du får ett meddelande via e-post eller SMS som säger att du måste betala en liten summa för att ditt paket (som du aldrig beställt) ska levereras. Eftersom det bara rör sig om några kronor och meddelandet ser helt ok ut betalar du. Bedrägeriet här handlar egentligen inte om att komma över några kronor, utan om att de nu har tillgång till alla dina personuppgifter.

Kort och gott är det svårt att dra en exakt gräns mellan olika typer av nätbedrägerier och ID-kapningar eftersom de är så tätt sammankopplade. Även om lagtexten är förhållandevis tydlig om vad som är en ID-kapning och inte, ser verkligheten ofta lite mer komplicerad ut.



Så säger lagen:

Brottsbalken, 4 kap, 6 b §
Den som genom att olovligen använda en annan persons identitetsuppgifter utger sig för att vara honom eller henne och därigenom ger upphov till skada eller olägenhet för honom eller henne, döms för olovlig identitetsanvändning till böter eller fängelse i högst två år. Lag (2016:485).

HUR GÅR EN ID-KAPNING TILL?

Tyvärr är bedragarna som sysslar med ID-kapning såväl duktiga på tekniken som uppfinningsrika. De hittar ständigt på nya sätt att lura till sig personuppgifter och inte sällan även nya sätt att använda sig av dem. Det är därför inte helt enkelt att svara på frågan hur en ID-kapning går till eftersom det finns så otroligt många sätt att kapa någons identitet på. Lite förenklat kan vi säga att det finns tre huvudtyper av ID-kapningar som du ska se upp för.

DEN KLASSISKA ID-KAPNINGEN

En ”klassisk” ID-kapning är att någon beställt ett kreditkort eller söker ett lån i ditt namn. Tidigare bevakade bedragaren fysiskt någons brevlåda för att fånga upp kontrakt och kreditupplysningar, men i dag sker det mesta digitalt. Det kan röra sig om allt från digitala låneansökningar till mer analoga varianter där man beställer fysiska produkter som hämtas ut med en falsk legitimation.

DEN TEKNISKA ID-KAPAREN

Den tekniske ID-kaparen har insett att allt kan genomföras digitalt. Det kan exempelvis handla om att komma över dina personuppgifter som sedan kan användas för ytterligare bedrägerier och brott online. Eller så vill de lura av dig pengar direkt, kanske genom att få dig att logga in via ditt BankID på någon tjänst där de sedan kan ta kontroll, ta lån eller beställa digitala tjänster av olika slag.

DEN ORGANISERADE ID-KAPAREN

ID-kapning bedrivs i dag mer eller mindre på löpande band av olika internationella ligor. Ett typexempel är de mycket omtalade Facebook-annonser som förekommit i Sverige de senaste åren där falsk reklam med kändisar ska locka dig att investera i kryptovalutan Bitcoin. Bakom annonserna ligger en internationell liga som inte bara lurar av dig dina pengar, utan även tar lån och köper saker med hjälp av dina personuppgifter.

VAD HÄNDER OM JAG BLIR ID-KAPAD?

Det finns många sätt att genomföra en ID-kapning och det är inte ens säkert att du märker av att den har skett. För den som drabbas kan det dock få långtgående och dyrbara konsekvenser. Det vanligaste som händer när du blir ID-kapad är följande:

NÅGON TAR LÅN I DITT NAMN

Ofta handlar det om dyrbara lån från kreditinstitut som inte ställer höga krav på kreditvärdighet. På så sätt går det fort och lätt att få ut pengarna för bedragaren, men blir ofta ännu mer kostsamt för dig.

NÅGON KÖPER SAKER I DITT NAMN

Med hjälp av dina personuppgifter handlar någon online, från olika platser runt om i världen. Du får stå för betalningen men ser aldrig röken av produkterna eller tjänsterna. Enligt våra undersökningar är det den absolut vanligaste följden av en ID-kapning.

NÅGON RENSAR DITT BANKKONTO

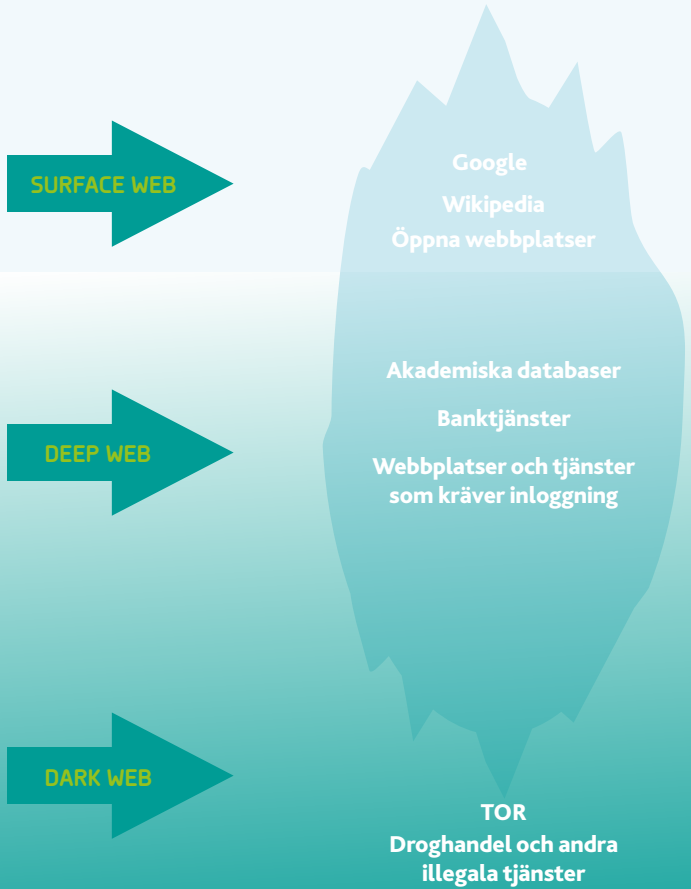
Genom att komma över person- och bankuppgifter, exempelvis genom inloggning via BankID, tömmer bedragarna ditt konto och pengarna är sedan svåra eller omöjliga att spåra.

NÅGON FÖRSÖKER LURA ANDRA I DITT NAMN

Bedragarna är smarta nog att använda andras personuppgifter för att göra ytterligare bedrägerier. Det kan handla om att hyra lägenheter, lura ytterligare människor eller sprida näthat i ditt namn. Det finns exempelvis fall där någon använder en falsk identitet på dejtingsajter för att smutskasta personen i fråga.

NÅGON SÄLJER DINA PERSONUPPGIFTER TILL ANDRA

På ljusskygga sidor på internet, ofta kallat dark web, är det lätt att köpa någon annans personuppgifter. Många bedragare samlar här uppgifter på hög för att sälja vidare till andra.



Vad är egentligen dark web och deep web? Och behöver jag bry mig om det?

Att förklara termer som dark web och deep web skapar ofta mer diskussion än det är värt. Många har sin egen definition och gränserna är inte alltid glasklara. Ett vanligt sätt att försöka förklara skillnaderna är ett isberg där toppen, det du ser, utgörs av allt det du hittar via en sökmotor.

Deep web är nästa lager där det finns massvis med material som inte nödvändigtvis är tillgängligt för alla. Ett enkelt exempel är dina sjukvårdsjournaler. De finns på nätet, men det är få som har tillgång till dem.

Kvar har vi då dark web, eller darknet som det ibland betecknas här i Sverige. Här handlas det med vapen, droger och görs mest ljusskygga och olagliga affärer överlag. Här handlas det ofta med just identitetsuppgifter.

VARFÖR SKA JAG OROA MIG FÖR ID-KAPNINGAR?

”Det händer ju inte mig och skulle det hända har jag ändå inte så mycket pengar på banken. Eller så litar jag på att banken täcker upp förlusten om jag blir lurad.”

Tyvärr är det ett vanligt resonemang, men det riskerar att bli dyrköpt. Det finns några enkla anledningar varför det här är ett problem som rör oss alla i dag.

ID-KAPNINGAR HAR BLIVIT ETT MÄNGDBROTT

Om den klassiske ID-kaparen bevakade din brevlåda vecka ut och vecka in, och därmed inte hann med så många enskilda offer, går det i dag blixtsnabbt. Vi vet att det genomförs fyra försök till ID-kapning i minuten i Sverige. Det behövs knappast mer bevis än så på att det är just ett mängdbrott vi pratar om.

DET KAN KOSTA MYCKET OCH LÄNGE

Bedragarna nöjer sig sällan med att tömma ditt sparkonto – de är också blixtsnabba att ta lån hos en rad banker och låneinstitut. Pengarna får du självklart inte se röken av men däremot får du sköta avbetalningarna. Hanterar du inte dem, eller om du inte upptäcker dem i tid, riskerar du även att få dras med betalningsanmärkningar under många år.

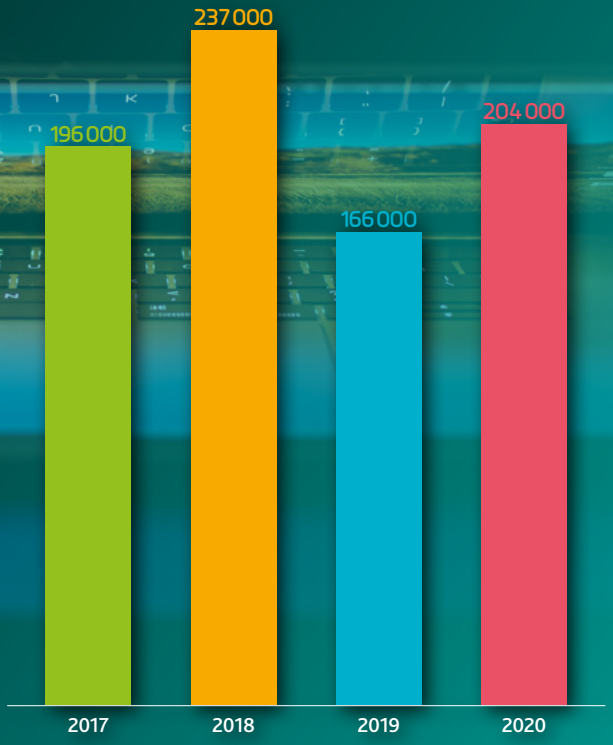
INGEN LÖSER PROBLEMET AUTOMATISKT LÄNGRE

En gång i tiden var de här brotten så pass få till antalet att de löstes mer eller mindre bakom kulisserna. I takt med att det blivit ett mängdbrott handlar det däremot om allt större summor och allt fler får även stå för återbetalningar på egen hand. Såväl banker som kortutgivare ska ha all ära för att de fortfarande är mycket alerta på om någon börjar handla från udda platser och för stora summor med ditt kreditkort. Då slår ofta automatiska larm och spärrar till. Men, tyvärr är det uppenbart att den typen av skydd inte längre räcker till.

ANTAL ID-KAPADE PERSONER I SVERIGE I ÅLDRARNA 16–79 ÅR

2017: 196 000 st.
2018: 237 000 st.
2019: 166 000 st.
2020: 204 000 st.

Över 2 miljoner människor i Sverige utsätts varje år för ett eller flera försök till ID-kapning.



NÅGRA VANLIGA BEDRÄGERI-FÖRSÖK ATT SE UPP FÖR:

SKIMMING

När någon kopierar informationen på ditt konto- eller kreditkort. Lämna aldrig ifrån dig ditt kontokort till någon okänd och kontrollera att maskiner du stoppar in kortet i inte har manipulerats.

PHISHING

När någon skickar förfalskade e-post eller andra meddelanden som ser ut att komma från ett riktigt företag. Skicka aldrig personlig och känslig information i e-post eller på andra sätt om du inte är helt säker på vem som finns på andra sidan skärmen.

FALSKA TÄVLINGAR PÅ NÄTET

Tävlingar där priserna ofta är för bra för att vara sanna. Inte sällan har det handlat om nästa eller till och med nästnästa generations iPhone. Är priset orealistiskt bra för din insats lär det vara en falsk tävling. Och måste du dela med dig av exempelvis bankkonton eller kort-nummer är det garanterat fuffens på gång.

AKUT PENGABEHOV / VD-BREV

När en vän hör av sig, ofta via sociala medier, och säger att han eller hon är i akut behov av pengar. Mot företag låtsas bedragarna ofta vara VD eller annan chef som ber om en snabb utbetalning. Kontrollera alltid att den som hör av sig verkligen är den de utger sig för att vara.

KRYPTOBEDRÄGERIER / FALSKA ANNONSER

Kryptovalutor som exempelvis Bitcoin har fått stor uppmärksamhet och det utnyttjar bedragarna. Genom falska annonser där de lovar enorma vinster lurar de dig att investera i ingenting. Ge aldrig bort personuppgifter eller investera i verksamheter du inte känner till, kan kontrollera noga eller som lovar och garanterar allt för stora vinster utan att prata om risker.

DEN FALSKA WEBBSIDAN / E-POSTADRESSEN

Felstavade domäner är ett klassiskt sätt att luras. Genom att byta en bokstav eller två, eller helt enkelt ta en annan toppdomän (exempelvis .com istället för .se) blir du lurad att du faktiskt pratar med banken, försäkringsbolaget eller vem det nu är som hör av sig. Dubbelkolla alltid adresser och liknande innan du fyller i personliga och känsliga uppgifter på nätet.

FRÅN SMÅBROTT TILL MÄNGDBROTT – VAD HÄNDE EGENTLIGEN?

Utvecklingen på området har varit extremt snabb. För bara några år sedan handlade de flesta ID-kapningarna fortfarande om vårt klassiska exempel – det vill säga att någon tog ett lån i ditt namn och bevakade din brevlåda. Det kunde vara såväl kostsamt som jobbigt för den som drabbades. Under de senaste åren har dock utveckling gått i rasande fart och bedrägerierna har blivit oerhört omfattande, framförallt sett till mängden försök. I många fall handlar det i dag om snabbare bedrägerier där det kanske är mindre summor i det enskilda fallet, men i totalen blir det mycket stora belopp och ett allt större samhällsproblem. Ökningen tycks bero på att organiserade internationella ligor på allvar fått upp ögonen för den här typen av bedrägerier. Det finns ett antal anledningar till att det har blivit så:

DET KOSTAR NÄSTAN INGET ATT FÖRSÖKA

Nätet innebär en nära på perfekt grund för den här typen av bedrägerier. Det kostar minimalt att försöka med samma bedrägeri till tio eller hundratusentals användare.

ETT NÄRA PÅ RISKFRITT BROTT

Det är i dagsläget mycket liten risk att åka fast, vare sig det rör sig om en fullbordad ID-kapning eller bara ett försök. Nästan inga lagförs och än färre får något straff.

ETT ENKELT SÄTT ATT FINANSIERA ANDRA BROTT

Vi vet att stulna ID-uppgifter är hårdvaluta i vissa kretsar för att exempelvis teckna hyreskontrakt till lokaler som sedan används i den brottsliga verksamheten. Det är alltså inte bara rena pengar som är målet för bedragarna.

DEN LOGISKA UPPFÖLJNINGEN PÅ ALLA KLASSISKA BEDRÄGERIER

ID-kapningar har blivit en naturlig följd, eller till och med slutmålet, med de flesta typer av bedrägerier. Om huvudmålet tidigare var att få dig att ge bort dina pengar ser bedragarna nu att de riktigt stora summorna finns att hitta när de väl kapat din identitet.

FÖRSÄKRINGSSKYDD MOT ID-KAPNINGAR OCH BEDRÄGERIER – HUR FUNKAR DET EGENTLIGEN?

BEHÖVS DE?
Det finns vissa som menar att bankerna och kortutgivarna oftast täcker kostnaderna för den som drabbas. Det stämmer inte längre, i den mån det någonsin varit en sanning. I dagsläget görs det ofta en bedömning att den som drabbats har handskats ovarsamt med sina personuppgifter, oftast över nätet, med resultatet att varken banker, kortutgivare eller vanliga försäkringsbolag ger ut någon ersättning. Men problemet stannar heller inte riktigt där.

KAN DU LÖSA PROBLEMEN SJÄLV?
En av de vanligaste utmaningarna när du blir ID-kapad är att ta hand om alla olika krav som ställs på dig. Bedragarna maxar ofta ut en persons uppgifter så långt det går med resultatet att du har en stor mängd banklån samt ett stort antal köp på nätet och liknande att ta hand om. Ska du hantera det själv gäller det alltså att ligga i och bestrida alla fakturor, kontakta alla kreditgivare och även vara beredd att driva process mot dem alla. Gör du inte rätt sak i rätt tid leder det tyvärr ofta till en betalningsanmärkning som är mycket svår att bli av med om inte allt hanteras rätt. Det är här försäkringen mot ID-kapning kommer in.

RÄCKER DET INTE MED EN HEMFÖRSÄKRING?
De allra flesta har i dag någon form av försäkringsskydd mot ID-kapningar, men de vet troligen inte om det. De senaste åren har så gott som alla olika försäkringsbolag lagt in delar som hanterar ID-kapning i hemförsäkringen. Skyddet är dock ofta begränsat, dels vad gäller funktionalitet som exempelvis automatiserad bevakning av om dina personuppgifter finns till salu på nätet, men kanske framförallt vad gäller rättsskyddet och den personliga assistansen.

VAD ÄR VIKTIGT NÄR DU VÄLJER FÖRSÄKRING MOT ID-KAPNING?

PENGARNA TILLBAKA INKLUSIVE NOLL I SJÄLVRISK
Med en hög självrisk är det inte säkert att det är värt att använda försäkringsskyddet alls. Och oavsett vad så kommer det alltså att kosta dig pengar att få hjälp. En bra försäkring på det här området har noll i självrisk.

RÄTTSSKYDD
Går det illa behöver du gå till domstol och det kostar pengar. Handlar det om komplicerade ärenden med många olika motparter kan det snabbt kosta summor som är högre än de rättskydd som ingår i många försäkringar. En bra ID-skydds-försäkring har därför ett rejält tilltaget rättsskydd och låg eller ingen självrisk för rättshjälpen.

PERSONLIG ASSISTANS
Att få snabb och professionell hjälp är en självklarhet i alla försäkringar, men en bra försäkring ser även till att du får en personlig handläggare som vet allt om ditt ärende och ser till att du själv behöver göra så lite som möjligt.

DARK WEB-BEVAKNING
Dark web kan enklast förklaras som den mörka sidan av internet. Här finns allt du inte vill veta mer om. Inklusive dina personuppgifter. En bra försäkring eller skydd bör även innehålla lösningar som söker igenom de här delarna av internet och varnar om just dina personuppgifter dyker upp på handelsplatserna.

HELTÄCKANDE SKYDD OCH HJÄLP DYGNET RUNT
Ett bra ID-skydd täcker självklart allt du behöver hjälp med. Du ska bara behöva ringa ett nummer och sedan få hjälp med alla delar. Och det ska gå att få hjälp dygnet runt oavsett var i världen du befinner dig.

Även företag drabbas hårt av ID-kapningar

Våra små och medelstora företag är också i skottgluggen för bedragarna. De senaste åren har vi sett en snabb utveckling där allt fler företag blir utsatta. Det handlar då om allt från att använda ett företags organisationsnummer för att göra affärer till att ID-kapa någon anställd eller någon i ledningen.

Det vanligaste tillvägagångssättet är de så kallade ”VD-breven” där någon låtsas vara en chef eller annan högt uppsatt person på företaget som behöver en snabb utbetalning av pengar. Meddelandena är ofta smart utformade och det är lätt att de slinker igenom betalningssystemen om alla inte är på sin vakt.

Enligt vår undersökning har 51 procent av de svenska små och medelstora företagen med upp till 250 anställda varit utsatta för ett försök till eller en fullbordad ID-kapning under 2020. Runt 11 procent av företagen har blivit ID-kapade.

HUR SKYDDAR JAG MIG BÄST MOT EN ID-KAPNING?

Förutom att ha ett försäkringsskydd, som även scannar av nätet för att se om dina personuppgifter är till salu, är det bästa sättet att skydda sig vaksamhet och försiktighet. Det finns en gammal sanning som gäller mer än någonsin när det kommer till internet – om ett erbjudande känns för bra för att vara sant är det ofta det. Ser du annonser eller hör av säljare som garanterar att du ska tjäna jättemycket pengar ljuger dom troligen. Erbjuder någon dig den senaste versionen av en mobiltelefon bara du lämnar lite uppgifter om dig själv är det troligtvis ett bedrägeri. Det är svårt att värja sig mot alla typer av bedragare, för de är ofta ruskigt skickliga på det de gör. Men här är några smarta tips som minimerar riskerna:

BE ATT FÅ RINGA TILLBAKA

Om någon ringer från din bank, ditt försäkringsbolag, från skattemyndigheten eller liknande och ber dig logga in på exempelvis banken eller någon annan tjänst på nätet – gör det inte. Be istället om namn och säg att du ringer tillbaka. Det brukar vara ett bra sätt att få bedragarna att visa sitt rätta jag och ger dig möjligheten att kontrollera att du verkligen pratar med rätt person.

UNDVIK ATT GE UT ALLT FÖR PERSONLIG INFORMATION PÅ NÄTET

De flesta vet nog att de aldrig ska lägga ut exempelvis kortuppgifter öppet, men det är lätt att bli lurad att lämna ut saker som inte, vid en första anblick, känns så känsliga. Men om du exempelvis deltar i allt för många ”kedjebrev” på sociala medier och där berättar vad ditt första husdjur hette, vad din mamma hade för efternamn innan hon var gift och i vilken stad du föddes – ja då har du väldigt snabbt avslöjat ett antal frågor som brukar användas för att återställa lösenord. Var försiktig helt enkelt.

LÄMNA ALDRIG UT KREDITKORTSUPPGIFTER

Dina kreditkortsuppgifter är bland det känsligaste du har. Hamnar de i orätta händer kan det snabbt gå väldigt illa. Dela aldrig med dig av uppgifterna annat än på säkra sajter när du köper något.

SÄKRA BETALNINGAR PÅ NÄTET

När du köper saker på nätet ska du vara extra noga med var du handlar. Dubbelkolla alltid att webbadressen börjar med https:// (alltså med ett ”s” på slutet) vilket innebär att din uppkoppling är krypterad.

INSTALLERA ALDRIG OKÄNDA PROGRAM PÅ DATORN

Installera aldrig program på uppmaning av andra, om du inte är säker på vad det är för program. Låt aldrig någon du inte känner och litar på till fullo få fjärrstyra din dator. Risken är annars stor att någon får kontroll över den och därmed även dina personuppgifter.

SPÄRRA ADRESSÄNDRING

Av någon underlig anledning kräver inte Skatteverket någon legitimation för att göra en adressändring. Du kan dock själv enkelt spärra obehöriga från att adressändra, men det kräver att du själv gör det här: *https://skatteverket.se/privat/folkbokforing/flyttanmalan/sparraobehorigadressandring*.

SE UPP FÖR SOCIAL MANIPULERING

Social engineering är en engelsk term som lite förenklat beskriver bedragare som är duktiga på att lura till sig olika typer av uppgifter. Det här handlar om allt från smarta säljare som ringer, till den typen av sociala medie-undersökningar som samlar in dina personuppgifter.
Var helt enkelt vaksam när människor du inte känner kontaktar dig och ber om råd, tjänster, information eller något annat. Be gärna att få ringa tillbaka för att kontrollera att de verkligen ringer därifrån de säger.

VAD GÖR JAG OM JAG DRABBAS?

Om du drabbats av en ID-kapning gäller följande:

1

Har du en ID-skyddsförsäkring kontaktar du ditt försäkringsbolag och får hjälp av dem. Förutsatt att det är en bra försäkring bör du även få hjälp med följande punkter.

2

Spärra kreditkort – antingen via en spärrtjänst eller bank och kortutgivare.

3

Spärra personnummer, ring din bank och avaktivera ditt BankID. Här måste du agera för att täppa till alla möjliga sätt för bedragarna att utnyttja dina personuppgifter och dina personliga konton.

4

Polisanmäl – även om det inte leder till vare sig utredning eller att någon åker fast för brottet är det viktigt och ibland nödvändigt för att få rätt mot eventuella fordringsägare. Dessutom kan det hjälpa till att lösa upp andra brott då bedragaren kan ha ett mönster. Ju mer statistik som finns desto bättre.

5

Var beredd på en process och kolla upp ditt rättsskydd. Har du otur kommer du att behöva försvara dig i rätten.

6

Hantera alla enskilda fordringsägare – beroende på vad som hänt måste du kontakta alla fordringsägare som bedragaren lånat pengar av eller köpt saker från. Det kan vara mycket tidskrävande och eftersom mycket görs med automatik i dag måste du hålla koll under lång tid för att minska risken att hamna hos kronofogden och få betalningsanmärkningar.

Om mysafety Försäkringar

mySafety Försäkringar har sedan 20 år utmanat försäkringsbranschen med innovativa lösningar för såväl nya som gamla problem och brott. Vi är ledande inom ID-skyddsförsäkring samt andra trygghetstjänster som förenklar i vardagen. Genom partners och våra egna kanaler erbjuder vi försäkringar till privatpersoner och företag i Norden. mySafety finns till för dig alla dagar, dygnet runt. mySafety Försäkringar är en del av mySafety Group. För mer information, vänligen besök www.mysafety.se.

FÖRSÄKRINGAR FÖR EN DIGITAL VÄRLD

HUVUDKONTOR Telefon: 08-408 380 00 Tegeluddsvägen 21, 115 41 Stockholm