INTERNETRELATERADE BEDRÄGERIER

OCH

NÄRLIGGANDE ORGANISERAD EKONOMISK BROTTSLIGHET

RAPPORTEN AVSER PERIODEN 2003 - 2013

En rapport om Internetrelaterad organiserad ekonomisk seriebrottslighet i Sverige.

Skriven av Internet- och IT-brottspecialisten Peter Forsman
Stockholm i juni 2013

INNEHÅLLSFÖRTECKNING

AVSNITT		SIDA
1	SAMMANFATTNING	4
2	OM FÖRFATTAREN	5
3	OM RAPPORTEN	5
4	INLEDNING	6
5	HISTORIK – FÖRTROENDEBEDRÄGERIER	8
6	SVENSKA INTERNETABONNEMANG 2003 – 2012	9
7	SAMHÄLLSKOSTNADER – BEDRÄGERIER	10
8	ANMÄLDA INTERNETRELATERADE BEDRÄGERIER 2003 – 2012	11
9	PERSONUPPKLARINGSGRAD – BLUFFAKTUROR	12
10	RIKSKRIMINALPOLISENS IAKTTAGELSER (2003)	14
11	ÅKLAGARMYNDIGHETENS IAKTTAGELSER 2012	15
12	BESKRIVNING AV BEDRÄGERIERNA OCH BOLAGEN	16
12.1	BESKRIVNING AV BLUFFAKTUROR	16
12.2	BESKRIVNING AV ”BLUFFAKTURABOLAG”	16
12.2.1	EXEMPEL: KOMMANDITBOLAG	18
13	RELATION BOLAGENS SKULDSALDON OCH INTÄKTER	20
14	BETALNINGSGRAD AV BLUFFAKTUROR	22
15	TILLVÄGAGÅNGSSÄTT BLUFFAKTUROR	23
15.1	BLUFFAKTUROR TILL FÖLJD AV BEDRÄGLIGT TELESÄLJ	23
15.1.1	TELEFONINFÖRSÄLJNING VARIANT 1	23
15.1.2	TELEFONINFÖRSÄLJNING VARIANT 2	24
15.1.3	TELEFONINFÖRSÄLJNING VARIANT 3	24
15.1.4	TELEFONINFÖRSÄLJNING VARIANT 4	25
15.2	MASSUTSKICK AV BLUFFAKTUROR, UTAN TIDIGARE KONTAKT	26
16	BEDRÄGERIER - TRENDER OCH FÖRÄNDRINGAR	28
16.1	MODEMKAPNING	29
16.2	ANNONSSKOJARE / BLUFFAKTUROR	29
16.3	BANTNINGSBLUFFAR	29
16.4	DOMÄNSKOJARE	29
16.4.1	DOMÄNSKOJARE – ”VI HAR EN KUND” – TELEFON	30
16.4.2	DOMÄNSKOJARE – ”VI HAR EN KUND” – E-POST	30
16.4.3	DOMÄNSKOJARE – ”DOMÄNFÖRNYELSE” – E-POST	30
16.5	VARUMÄRKESSKOJARE	32
16.6	SPAM / PHISHING / NIGERIABREV	32
16.7	NIGERIABREV GENOM SOCIAL MEDIA (ROMANSBEDRÄGERIER)	33
16.8	INTERNETKATALOGER / BLUFFAKTUROR	33
16.9	RANSOMWARE	33
16.10	HACKADE KONTON BER VÄNNER OM EKONOMISK HJÄLP	34
16.11	SMS-PHISHING / BETALTJÄNSTABONNEMANG	34
16.12	SMART-MOBIL-KAPNING / PORRFAKTUROR	35
16.13	FALSKA VÄRDERINGSSIDOR / BLUFFAKTUROR	35
16.14	SKRIVARTONER / LYSRÖRSSKOJARE / KONTORSMTRL	36

16.15	SEO-SKOJARE / BLUFFAKTUROR	36
16.16	FALSKA VARNININGS- OCH SPÄRRTÄNSTER	37
16.17	TROJANSPRIDNING VIA SOCIALA MEDIER FÖR BANKINTRÅNG	37
16.18	ID-STÖLDER / ID-KAPNINGAR / FALSKA ID-HANDLINGAR	38
17	NYA TRENDER OCH NYA HOT	40
17.1	ID-SKYDD	42
17.2	STÖLDER AV SMARTA MOBILTELEFONER	42
17.3	KUNGÖRELSER AV BOLAGSNAMN	42
17.4	KLONER AV SERIÖSA WEBBSIDOR	43
18	REVISORER	45
19	LAGERBOLAG OCH KONKURSHOTADE BOLAG	45
20	BARTERAFFÄRER AV INAKTIVA BOLAG	45
21	FÖRÄDLING AV PENNINGFLÖDEN TILL FÖLJD AV BEDRÄGERIER	46
22	LEASINGBOLAG	46
23	PUMP N DUMP-VERKSAMHETER	46
24	SVENSKA BOLAG VERKSAMMA MOT NORGE	47
25	SVENSKA BLUFFVERKSAMHETER I UTLANDET	47
26	ANONYMA BREVBOXAR	47
27	SKATTEBROTTSENHETER	48
28	DATAINSPEKTIONEN – INKASSOTILLSTÅND	48
29	TELEFONBEDRAGARES LJUDINSPELNINGAR	48
30	ARBETSFÖRMEDLINGEN – PLATSBANKEN	49
31	LOTTERIINSPEKTIONEN	49
32	BOLAGSVERKET, BRISTANDE KONTROLL	50
33	KRONOFOGDEMYNDIGHETEN, BRISTANDE KONTROLL	50
34	BRANSCHORGANISATIONER OCH PRIVATA INITIATIV	51
34.1	SVENSK HANDELS VARNINGSLISTA	51
34.2	FÖRETAGARORGANISATIONEN FÖRETAGARNA	51
34.3	VARNINGSINFO I SVERIGE AB	51
34.4	FÖRENADE BOLAG AB	52
34.5	KNYT.SE	52
34.6	VARNINGSKOLLEN.SE OCH INTERNETSWEDEN.SE	52
34.7	10-15 AKTIVA OSERIÖSA VARNINGSTJÄNSTER	52
34.8	NATIONELL VARNINGSLISTA	52
35	POLISENS PROAKTIVA OCH BROTTSFÖREBYGGANDE VERKSAMHET	53
35.1	NBC, NATIONELLT BEDRÄGERICENTER	53
36	FÖRSLAG TILL ÅTGÄRDER	54
36.1	GENERELLT UTBILDNING	54
36.2	GENERELLT INFORMATION	54
36.3	GENERELL SAMVERKAN	54
36.4	OPERATIVA FÖRSLAG	54
37	AVSLUTNING	55

1 SAMMANFATTNING

Internet är det största som hänt vår generation och är en fantastisk tillgång på många sätt, men det är också en spegelbild av vårt samhälle i övrigt på gott och ont. Samhällets integrering med Internets olika tjänster innebär då också att brottsbekämpningen måste finnas och verka förtroendeingivande där medborgarna finns och utsätts för brott.
Bedrägerier är den brottstyp som ökar mest i Sverige, sedan flera år tillbaka. Internetrelaterade bedrägerier (brottstyperna: Bluffaktura, Datorbedrägeri och Internetbedrägeri) har tillsammans ökat med **1 200%** mellan 2003-2012 (ref. avsnitt 8). Och det finns inte någon brottsutredande myndighet med ett övergripande ansvar för den ekonomiska seriebrottsligheten i Sverige.

Bristen på helhetsperspektiv och samordning är nedslående, så även att uppfattningen om vad som är ekonomisk brottslighet skiljer sig mellan brottsbekämpande myndigheter. EBM särskiljer exempelvis bedrägeri från den ekonomiska brottsligheten och utreder endast i undantagsfall bedrägerier kopplade till annan ekonomisk brottslighet. Och bluffakturor är **inte** en egen företeelse inom den ekonomiska seriebrottsligheten, då någon klar avgränsning inte finns mellan bluffakturor och annan ekobrottslighet, vilket tydliggörs genom de kopplingar till ekonomisk seriebrottslighet och förgreningar som finns mellan grupperingar, personer, konton och bolag.
Som en lösning, går Rikspolischefen i januari 2013 ut i media och lovar rekrytering av 5-6 stycken civila bedrägeriexperter till en ny planerad satsning ***NBC, Nationellt Bedrägericenter***, med start hösten 2013 i Stockholm. När dimman lättat är 3-4 analytiker anställda med en lönenivå motsvarande 2/3 av medellönen för en analytikertjänst i Stockholm. En signal av **total oförståelse** från polisledningens håll, för den mest ökande brottsligheten i Sverige, när Rikspolischefen allokerar 3 miljoner till denna verksamhet, av polisens totala anslag på 20, 536 miljarder för 2013.

NBC ska verka som nationell uppsamlande enhet för bedrägerianmälningar med tre fokus: ***Brottsförebyggande insatser, Metodutveckling*** och ***Polisoperativt arbete***. Efter uppsamlandet ska anmälningarna ”skyfflas” ut för brottsutredning, sk brottsforum, lokalt ute i landet.

Källor: http://www.svt.se/nyheter/sverige/polisen-sluta-betala-bluffakturor
http://www.lonestatistik.se/loner.asp/yrke/Analytiker-1055/lan/Stockholm-21
http://www.regeringen.se/sb/d/1912/a/70938

NBC:s 3 fokusområden leder **inte** till att bromsa antalet bedrägerianmälningar, som ökat med 28% under första kvartalet 2013. De leder **inte** heller till en högre uppklaringsgrad.

Poliskåren saknar, mer än i undantagsfall, den förståelse, kompetens och de resurser som krävs för att bekämpa den Internetrelaterade organiserade ekobrottsligheten.
Personuppklaringsgraden för bluffakturaanmälningar ligger de senaste åren på 1-2%

Det krävs ett nytt sätt att arbeta för att kartlägga och utreda vilka personer som döljer sig **bakom** fasaden av brott, organiserar och tillägnar sig alla "brottspengar". ***Denna typ av brottslighet anmäls inte utan måste spanas fram och kartläggas.***

Det fjärde fokusområdet som NBC, eller annan myndighetsinstans behöver inrätta, är nödvändig och helt avgörande för att lyckas bromsa och vända trenden för den eskalerande ekonomiska seriebrottsligheten. Och det är ”**Spaning och kartläggning**”.

Det är helt avgörande att kompetens för denna resurs sker genom rekrytering av erfarna och målinriktade bedrägeriexperter, från privat sektor och från andra myndigheter.

2 OM FÖRFATTAREN

Domänspecialisten Peter Forsman är Partner- och Abuseansvarig på .SE, Stiftelsen för Internetinfrastruktur som är registerhållare för Sveriges landstoppdomän .se, där han ansvarar för .se-zonen (ca 1,3 miljoner .se-domännamn). Han har varit verksam inom IT-sektorn sedan mitten av 90-talet, främst inom datautbildningsbranschen och har erfarenheter från flera olika roller i domän- och webbhotellbranschen.

Han arbetar också aktivt för att informera och utbilda om oetiska verksamheter med koppling till Internet, som han bevakat sedan 2002, ofta i samarbete med andra organisationer, privata brottsbekämpare och myndigheter som exempelvis Svensk Handel, Varningsinfo i Sverige, Förenade Bolag och Polisen.

Peters engagemang fortsätter i ett privat initiativ utanför hans anställning på .SE genom att han ideellt driver bloggen internetsweden.se, som synliggör bedragare och informationssidan varningskollen.se och är delaktig i Polisens samverkansgrupp mot bluffakturor [http://www.bestrid.nu]

Peter har i åratal anlitats som föreläsare och utbildar bland annat kring spårning och kartläggning på Internet. Privat så är Peter Skatteverket, Polisen, Ekobrottsmyndigheten och Åklagarmyndigheten behjälplig i utredningar och kartläggningar och har föreläst om organiserad ekobrottslighet på Internet för Skatteverkets kompetensnätverk, Polismyndigheters olika bedrägerienheter och så även på Rosenbad och vid Polishögskolan.

Han har kallats som sakkunnig vid större Internetrelaterade ekomål och varit bidragande till informationsinhämtning för den stora bluffakturahärvan ”Företagslansering Sverige AB” i Helsingborg och större polisoperationer som Selma, Alfred, Draupner mfl. Och även bidragit till ett antal strategiska rapporter kring den organiserade ekobrottsligheten.

Peter har daglig kontakt med utredare inom privat och myndighetsutövande brottsbekämpning.

3 OM RAPPORTEN

Rapporten är skriven med avsikt av att ge en neutral, objektiv och pragmatisk nulägesbild.
En rapport som omfattar tidsaxlar kring trender och modusförändringar, likväl som att ge indikationer på nutida och framtida problemområden. Och i utvalda delar även utbilda läsaren.

Rapporten är framtagen efter rekommendation av ett flertal personer från ovan namngivna myndigheter.

4 INLEDNING

Den ekonomiska seriebrottsligheten i Sverige som är relaterad till Internet, omsätter stora pengar, men det finns inga siffror eller statistik att tillgå på området, då Sverige saknar ansvarig instans. I en direkt jämförelse med Storbritannien, så kostar bedrägerier Sverige över 81 miljarder kronor bara under 2013 (se uppskattning i avsnitt 7) och det behöver understrykas att *bluffakturor* endast är en av många metoder i hur de kriminella grupperingarna begår ekonomiska brott, men *bluffakturor* är bra exempel på hur Internet på olika sätt används på ett *bedrägeriförstärkande* vis.

Idag är samma personer och grupperingar verksamma med ett flertal olika samtidiga typer av bedrägerier med allt från falska **konsumentinriktade** Tradera- och Blocket-annonser, förskottsbetalningar för produkter på falska hemsidor, trojanspridningar och ID-kapningar till **företagsinriktade** bluffakturor, bolagsplundringar, bolagskapningar, skalbolag och *haussade* aktiekurser av börsnoterade ”Luftbolag”.

Den Svenska Internetrelaterade organiserade ekonomiska brottsligheten är hierarkiskt uppbyggd i flera nivåer och sfärer, där majoriteten av all ekobrottslighet styrs av till synes ett 10-tal huvudpersoner som har relation och påverkan på ett större antal grupperingar. Grupperingarna är ofta sammansatta av personer som endera förenas genom geografiskt ursprung/bostadsort eller efter specialiteter/kompetenser. Bolagsmålvakter (styrelseledamöter) i ansvariga bolag är ömsom betalda och medvetna, ömsom omedvetna/ID-kapade.

Man använder återkommande ”en-produkts-leverantörer” som bolagsbildare, domännamnsombud, webbhotell, webbsidetillverkare, tryckerier, boxadress-leverantörer och ”en-rolls-personer” som revisorer, innehavare av domännamn och abonnemang, bankkonto- och bolagsmålvakter mm.

Ofta involveras även personer ur-, eller hela våldskriminella miljöer, som är kända för sitt våldskapital, dels för att hålla konkurrenter borta, men även för att höja ”*betalningsmotivationen*” hos den drabbade.

Varje gruppering kan sedan omfatta 1-2 bolag med tillhörande 80-tal domännamnsadresser/sidor. Men kan lika gärna handla om ett 50-100 tal bolag och endast ett fåtal e-mailadresser. Verksamhetsområdet är helt avgörande.

Grupperingarna är även ofta involverade i en rad olika bedrägerityper som grupperingen kan växla emellan. Konsumenter som målgrupp byts ofta till verksamheter som är inriktade mot näringsidkare och vice versa, beroende på aktivitet och hur mycket myndigheter och massmedia varnar för bluffverksamheterna.

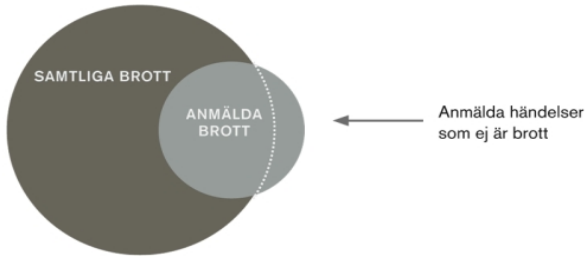
Uppfinningsrikedomen hos bedragarna är dessutom stor, då oseriösa telefonsäljare kan växla till att sälja falska spärrar mot telefonförsäljare, och bluffakturerande verksamheter växlar till att sälja medlemskap av varningstjänster mot bluffverksamheter, och ID-kapande verksamheter växlar till att sälja ID-skydd osv.

Svensk Handel gör uppskattningen att bara bluffakturor, årligen omsätter 1,2 miljarder kronor. Det är främst fåmans- och småföretagare som utsätts för bluffakturor, men offer kan hittas i alla verksamhetsstorlekar och hos kommuner och myndigheter, samt även privatkonsumenter.

BRÅ, Brottsförebyggande rådet skriver i sin sammanfattande text för bedrägerier och ekobrott att mörkertalet är stort för bedrägerier och att den faktiska brottsligheten antagligen är större, eftersom många bedrägerier inte kommer till myndigheternas kännedom.

BRÅ berättar att den vanligaste påföljden för bedrägeri är villkorlig dom och strafföreläggande.

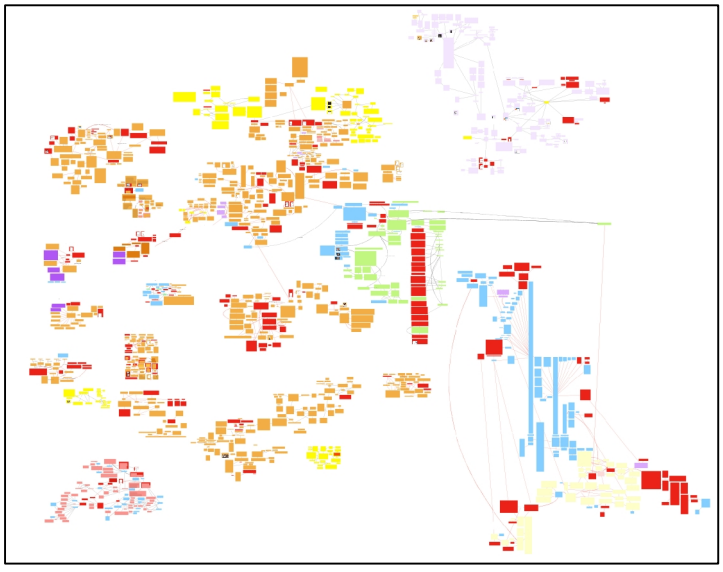
Mörkertal och dold brottslighet



Källa: http://bra.se/bra/brott--statistik/bedragerier-och-ekobrott.html

Trots att polisanmälda bluffakturor gått från 52 stycken (2004) till 16 068 (2012), så finns det inte möjlighet för en drabbad företagare att polisanmäla bedrägeribrott via polisens hemsida http://www.polisen.se. Detta faktum gör det omständigt och tidskrävande för en småföretagare att polisanmäla bedrägeribrott, så det är högst troligt att det bidrar till BRÅ:s uppskattade mörkertal.

Förutom att dessa grupperingar har svenska näringsidkare och konsumenter som målgrupp, så verkar de växelvis och dedikerat mot våra grannländer och övriga europeiska länder.
Förutom svenska juridiska personer, skapas även bolag i Estland, Cypern, Malta, Thailand, Hong Kong, USA och Storbritannien mfl. med svenska ”egentliga företrädare” och som utför brottsligheten mot Sverige och svenskar. Nedan visas en del av verksamma grupperingar under 2012.



5 HISTORIK - FÖRTROENDEBEDRÄGERIER

Det som genomsyrar samtliga tillvägagångssätt av bedrägerier på Internet, sk *modus operandi*, är att det i allra flesta fall handlar om någon form av ***förtroendebedrägeri***. Där gärningsmannen utnyttjar den bedragnes godtrohet eller okunskap för egen ekonomisk vinnings skull.

Eugène François Vidocq som 1811 grundade den franska underrättelsetjänsten ***Sûreté*** skrev redan i hans memoarer som publicerades i Sverige 1829 om en händelse från 1797 kring vad som *på tjufspråket kallades* ***jerusalemsbref***. Beskrivningen av innehållen i dessa ***jerusalemsbref*** är slående lika innehållen i det vi idag kallar för "***Nigeriabrev***" eller på engelska ***Advance fee fraud*** och syftar till att någon typ av lättillgänglig förmögenhet utlovas, i utbyte mot en lägre administrativ kostnad för mottagaren av brevet.
70 år senare, 1899 skriver en senare detektivchef för ***Sûreté*** vid namn ***Marie-François Goron*** att:

..detta klassiska bedrägeri, som härstammar från början af vårt århundrade och som tusentals tidningar ha afslöjat, men som ändå alltid lyckas..

.. Det märkligaste är, att dessa tiggarebref skickas ut på måfå och att addressaternas namn äro hämtade ur adresskalenden ..

Dessa operationer erfodra … ett visst rörelsekapital, ty det händer ibland, att flera tusen bref afsändas utan resultat, men tjuvarna drabbas sällan af denna otur, ty de dumma äro legio.

Fenomenet är alltså inte alls nytt, utan allmänheten har låtit sig luras av samma typ av förtroendebedrägerier i över 200 år, alltså långt långt före Internets födelse.
Idag skickas "Nigeriabrev" oftast i form av obeställd e-post (sk *SPAM*), men det är även vanligt med pappersbrev och faxmeddelanden. Det finns också otaliga varianter på dessa skojarbrev i form av allt från lotterivinster och arv från okända släktingar till undangömda skatter. De senaste 3-4 åren har även sk *romansbedrägerier* blivit allt vanligare, vilket beskrivs senare i rapporten.

På samma sätt känns också modus igen från dagens större bluffakturautskick, som skickas till adressater ur "*adresskalenden",* utan tidigare kontakt och kan skickas ut till tusentals näringsidkare, ofta under förespegling att det är en annuell avgift för ett befintligt avtal.

Ända sedan tidigt 70-tal har annonsbedrägerier förekommit i Sverige. De har oftast fungerat som något av en plantskola for tyngre ekonomisk brottslighet. Det finns aktiva "Huvudpersoner" som varit aktiva sedan 70-talet.

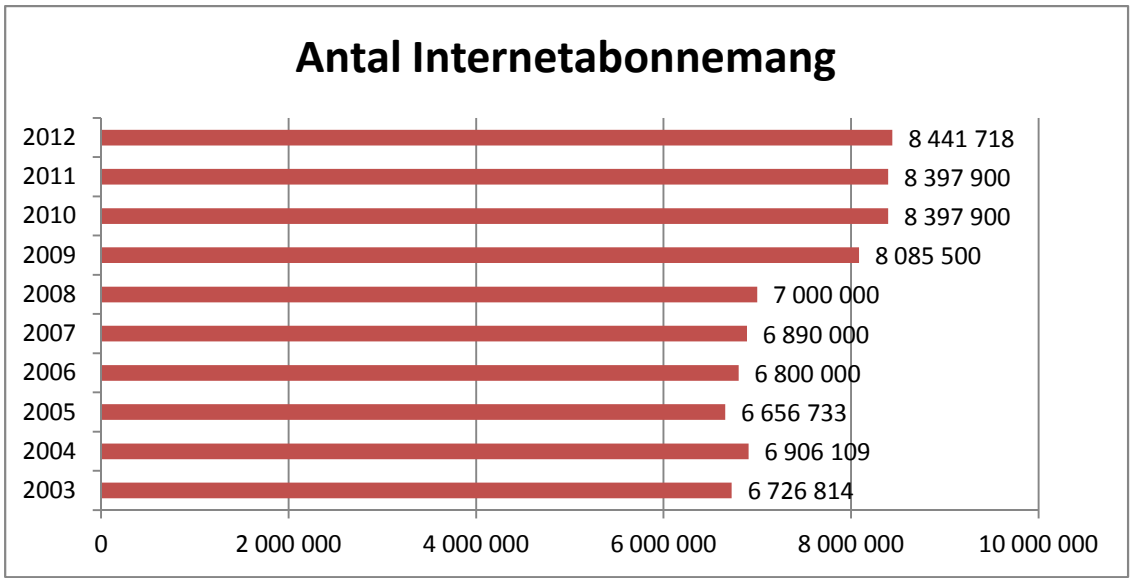
Sedan Internets intåg i svenska hem och företag under 90- och 00-talet och den ökande betydelsen i vårt samhälle, så har också Internet blivit den naturliga plattformen för majoriteten av alla bedrägeribrott, i Sverige såväl som övriga världen.

Källor:
Eugène François Vidocq http://www.internetsweden.se/som-pa-tjufspraket-kallades-jerusalemsbref
Marie-François Goron http://www.internetsweden.se/ty-de-dumma-aro-legio/

6 SVENSKA INTERNETABONNEMANG 2003 – 2012

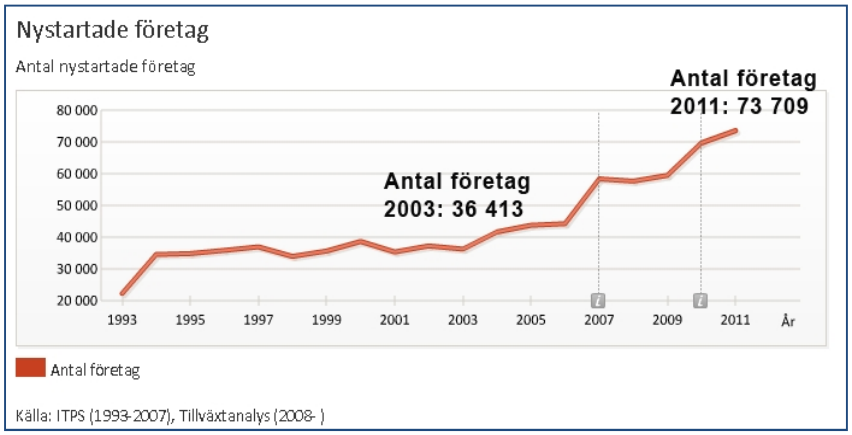
Från 1998 då Hem-PC reformen infördes, så hyr många anställda en PC för hemmabruk skattefritt och från att antal abonnemang börjar mätas 2002, då svenskarna har 4 048 000, så *exploderar* det till 6 726 814 året efter. Med Hem-PC paketen fanns kravet att det skulle finnas med en PC-utbildning, som i flesta fall skickades med i form av e-learning (interaktiv utbildning på CD-ROM och var förberedande till ECDL, European Computer Driving License).

Problemet var att det inte följdes upp av någon och det uppskattas senare att mellan 10-15% av utbildningarna överhuvudtaget öppnades från sin förpackning. Istället för att Hem-PC blev det kompetenslyft som det var avsett att vara, så användes Hem-PC istället företrädesvis att spela spel och koppla upp sig mot Internet. Sedan 2008/2009 tillhör Sverige de länder med högst Internetpenetration. **1 714 904 nya Internetabonnemang mellan 2003 – 2012 (nya användare)**



Källa: internetworldstats.com

Nystartade företag per år fördubblas mellan 2003 och 2011 (ca 36 500 nya företag)



Enligt SCB finns idag 1 137 028 svenska företag.

7 SAMHÄLLSKOSTNADER - BEDRÄGERIER

Det finns idag ingen officiell statistik över vad bedrägerier kostar samhället i direkta och indirekta kostnader, då det saknas ansvarig organisation för uppdraget, men
Svensk Handel uppskattar att den avgränsade delen *Bluffakturor* omsätter 1,2 miljarder årligen och **Skatteverket** ger uttryck för att det årligen ”*saknas*” 100 miljarder kronor i statskassan och **Stockholmspolisen** bedömer att att ca 90% av anmälda bedrägeribrott är *relaterade till Internet*.

Och en mycket intressant jämförelse kan emellertid göras med Storbritannien som via deras ansvariga myndighet **NFA, *National Fraud Authority***, sedan 2010 årligen publicerat **Annual Fraud Indicator**. Annual Fraud Indicator uppskattar årligen kostnaderna till följd av bedrägerier i GB.

Storbritannien och Sverige är de mest jämförbara länderna i Europa, gällande faktorer som:
- **Internetpenetration**, GB = 83,6%, SE = 92,7% (internetworldstats.com 2012)
- **Internetmognad**, GB = 93.83, SE = 100 (thewebindex.org 2012)
- **Daglig Internetanvändning**, GB = 67%, SE = 71% (ons.gov.uk, internetstatistik.se 2012)
- **Betalningar över Internet**, GB = 71%, SE = 71% (Eurostat 2011)
- **BNP per capita**, GB = $36,900, SE = $40,900 (cia.gov uppskattning 2011)
- **Arbetslöshet**, GB = 8,2%, SE = 7,9% (Eurostat 2012)

Och då NFA nyligen (jun 2013) publicerade *Annual Fraud Indicator 2013*, så kan de för första gången uppvisa ett tydligt trendbrott, då de från **£73 miljarder**(2012), visar en kraftig sänkning på ca 30% till **£52 miljarder** (2013). Passus: NFA har sedan 2010 med kraft bekämpat bedrägerier, alltmedan motsvarande nationell insats i Sverige saknas, varför jämförelsen riskerar att vara felaktigt gynnsam för de svenska siffrorna.

ÅR	GBP	SEK
2010	30 000 000 000	307 800 000 000
2011	38 400 000 000	393 984 000 000
2012	73 000 000 000	748 980 000 000
2013	52 000 000 000	533 520 000 000

Om vi gör ovan jämförelse med svenska förhållanden, **baserat endast på befolkningsmängd** (Befolkning GB = 62 300 000, Befolkning SE = 9 555 893), så skulle den direkta och indirekta kostnaden till följd av bedrägerier i Sverige se ut på följande sätt:

ÅR	SEK	SEK PER PERSON
2010	47 211 940 055	4 941
2011	60 431 283 270	6 324
2012	114 882 387 466	12 022
2013	81 834 029 428	8 564

I jämförelsen blir kostnaden **81,8 miljarder kronor** eller **8 564 kronor per invånare i Sverige för 2013**.

Källor: https://www.gov.uk/government/publications/annual-fraud-indicator
https://www.gov.uk/government/publications/annual-fraud-indicator--2

8 ANMÄLDA INTERNETRELATERADE BEDRÄGERIER 2003 - 2012

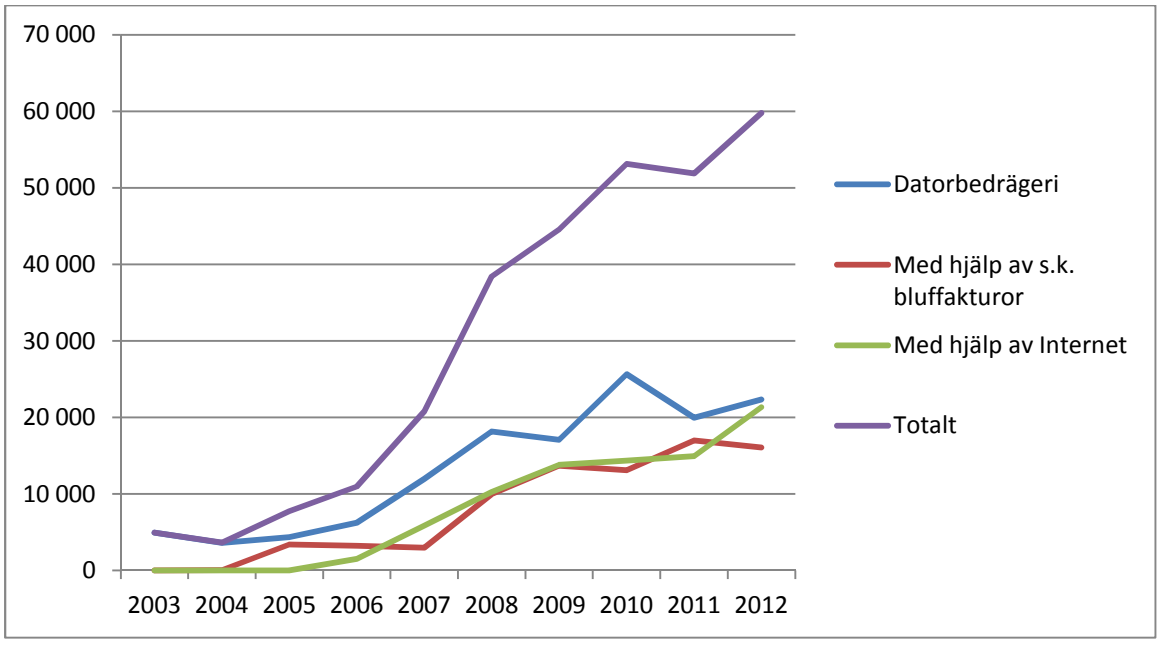
Polisanmälningarna för Dator- och Internetrelaterade bedrägerier har under de senaste 10 åren (2003 – 2012) **ökat med över 1 200%** totalt.

Anmälda bedrägerier med hjälp av *bluffakturor* började av BRÅ mätas först 2004 då 52 brott anmäldes, att jämföras med 2012 då 16 068 anmäldes.

Då ett *Datorbedrägeri* behöver ske mellan två parter, så behöver dessa kommunicera över Internet. Därför är det relevant att redovisa båda dessa brottskategorier (Datorbedrägeri och Mha Internet). Att så få bedrägerier kategoriseras som ”Mha Internet”, torde vara att det inte fanns valbart förrän 2006. Medan anmälningarna numera är jämnt fördelade mellan de två brottskoderna.

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Datorbedrägeri	4 939	3 588	4 361	6 236	11 956	18 173	17 092	25 668	19 960	22 359
Mha s.k. bluffakturor		52	3 390	3 220	2 963	9 976	13 667	13 121	16 973	16 068
Mha Internet				1 502	5 860	10 260	13 800	14 350	14 927	21 354
Totalt	**4 939**	**3 640**	**7 751**	**10 958**	**20 779**	**38 409**	**44 559**	**53 139**	**51 860**	**59 781**

Samma siffror som ovan för att grafiskt påvisa trendökning av Internetrelaterade bedrägerier.



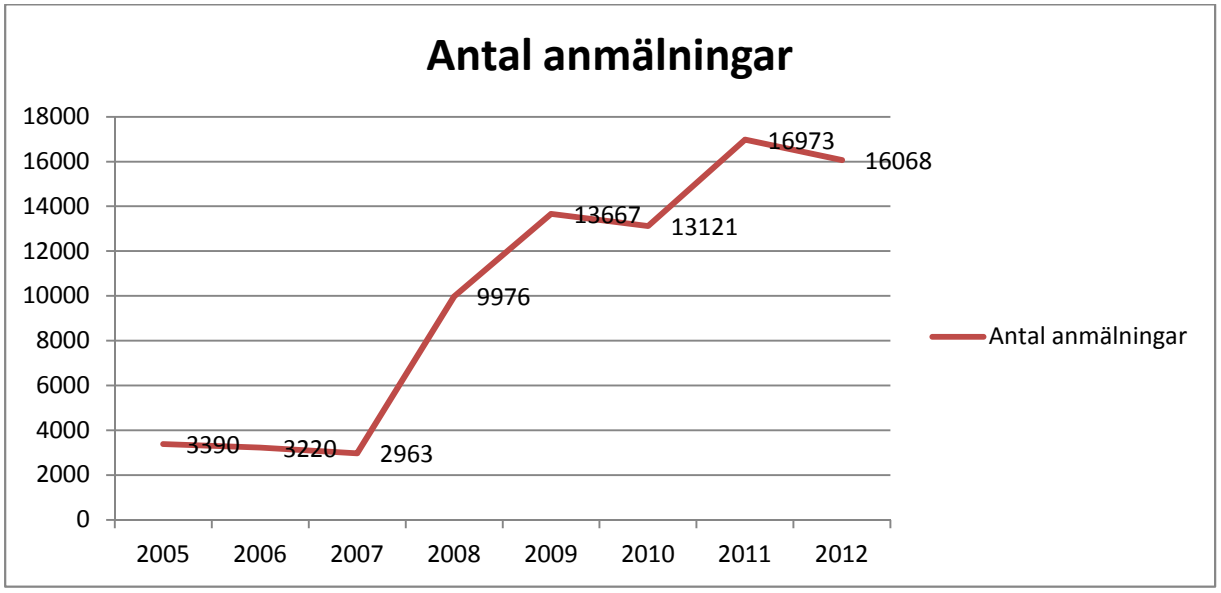
Källa: Brottsförebyggande rådet

Fördelning mellan Polismyndigheter, av inkomna polisanmälningar (Fördelningen avser 2011):

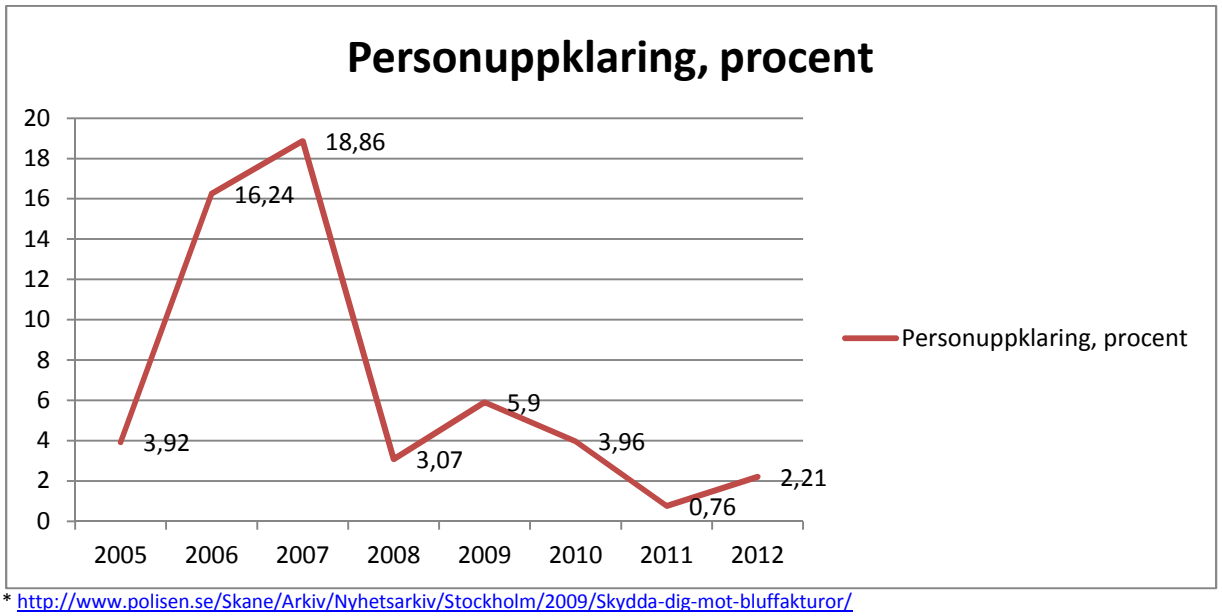
Stockholm	30% (jmfr. 40% år 2009)
Malmö	20%
Västra Götaland	16%
Övriga	34%

9 PERSONUPPKLARINGSGRAD – BLUFFAKTUROR

Jämförbar statistik (BRÅ) finns från 2005 och framåt. Tittar vi först på antalet anmälningar under perioden, så har den mångdubblats under perioden (mellan 2007 då den var lägst till 2011 då den var högst så ökar den med 574%).



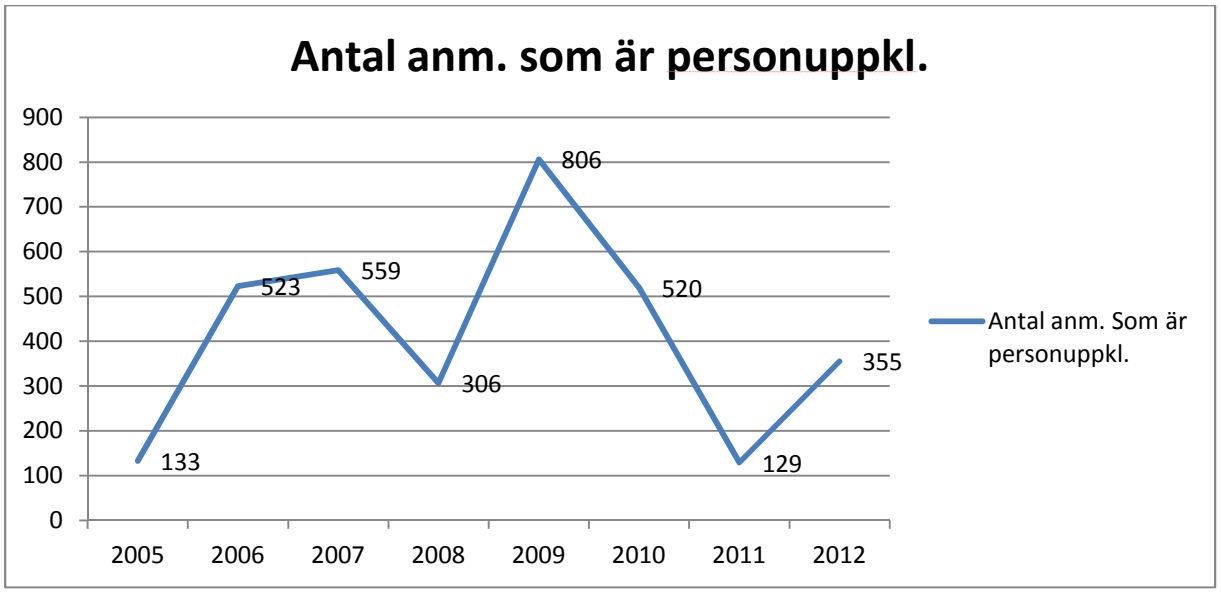
Under samma period har personuppklaringsgraden sjunkit i takt med att fler anmälningar skett. Stockholmspolisen som emottog 40% av bluffakturaanmälningarna 2009 (5499 av 13667) hade 2009 tre brottsförebyggare som aktivt informerade om att näringsidkare behövde driva bluffakturor civilrättsligt. * Något som Helsingborgs Tingsrätt istället konstaterade var ”Grovt Bedrägeri” i maj 2012 i den stora rättegången mot företrädare ur ”Företagslansering Sverige AB”.



* http://www.polisen.se/Skane/Arkiv/Nyhetsarkiv/Stockholm/2009/Skydda-dig-mot-bluffakturor/

* http://www.polisen.se/PageFiles/229125/Fakturabedr%C3%A4gerier_1.pdf

Tittar vi istället på **antal** personuppklarade anmälningar, så ser kurvan ut på annat sätt.



Trenden är väldigt bekymrande, då det tydligt visar att brottsbekämpningen i de allra flesta fall inte lyckas fastställa gärningsman, medan BRÅ berättar att den vanligaste påföljden för bedrägeri är **villkorlig dom** och **strafföreläggande**. Samhället ger tydliga signaler om en ***"riskfri brottslighet"***!

År	Antal	Anmäln.	%
2005	133	3 390	3,92%
2006	523	3 220	16,24%
2007	559	2 963	18,87%
2008	306	9 976	3,07%
2009	806	13 667	5,90%
2010	520	13 121	3,96%
2011	129	16 973	0,76%
2012	355	16 068	2,21%

Och eftersom det vanligtvis skickas ut 500 – 10 000 bluffakturor per bluffakturautskick och varje enskild bluffaktureanmälan räknas separat i statistiken. Så innebär det att det kan vara så lite som **en** (**1) individ per år** som lyckas personuppklaras. Personuppklaring innebär **inte** att det väcks åtal och det innebär **inte** att den **egentliga** verksamhetsföreträdaren fastställts.

10 RIKSKRIMINALPOLISENS IAKTTAGELSER (2003)

Rikskriminalpolisen genomförde under knappt 2 år tid (2001-2003) ett projekt kring ”Annons- och fakturabedrägerier”, som i slutrapporten december 2003 ger en nedslående läsning, då deras iakttagelser och analyser i många fall är identiska med läget nu 10 år senare. Ur rapporten:

Den grova brottsligheten har förändrats genom att brottslingarna har blivit rörligare och ***utför flera olika typer av grov brottslighet samtidigt****. Brottslingarna är mera anonyma och svårfångade, då de kan hålla ständig kontakt med varandra via mobiltelefon var de än befinner sig. Det är dessutom möjligt att snabbt flytta pengar mellan olika postgirokonton med transaktioner via Internet. Detta gör det mycket svårt att finna brottsplats och fysiskt ansvarig person.*

Annonsbedrägeribrottsligheten anses vara kvalificerad och svårutredd. Trots att det enskilda bedrägeriet synes vara enkelt att utreda, så är det i själva verket inkörsporten till grov ekonomisk brottslighet, eftersom de misstänkta efter bedrägeribrottet vidtar ett antal åtgärder för att ta ut inkomna pengar. Dessa åtgärder ***genererar ett antal andra brott som penninghäleri, skattebrott, urkundsförfalskning och osant intygande osv.*** *För att utreda och slutföra den typen av förundersökning krävs hög kompetens hos alla medverkande. Det är dessutom nödvändigt att flera myndigheter samverkar i ett tidigt skede.*

Det krävs ett nytt sätt att arbeta för att utreda vilka personer som döljer sig bakom fasaden av brott och tillägnar sig alla "brottspengar". *Det kan ske genom att samma polispersonal som arbetat med spanings- och underrättelseverksamheten även deltar aktivt i förundersökningen. Detta arbetssätt gör det möjligt att i ett tidigt skede och steg för steg bygga upp den samverkan mellan berörda myndigheter som krävs.* ***Denna typ av brottslighet anmäls inte utan måste spanas fram och kartläggas.***

Brottsbekämpning av annons- och fakturabedrägeribrottsligheten bör ske på central nivå *av en särskilt avdelad kartläggningsgrupp vid Rikskriminalpolisen.*

Kartläggningsgruppens arbete måste sedan följas av operativa åtgärder *och då inte bara i form av förundersökningar utan även av skatterättsliga och andra åtgärder. För att uppnå detta måste det finnas direkt operativa resurser som omedelbart kan följa upp den information som ges genom den kartläggning som sker. En sådan operativ resurs kräver utredningspersonal (polis, polisekonomer och skattebrottsutredare) och åklagare, alla med erfarenhet av ekonomisk brottslighet.*

Den centrala utredningsenheten *kan skapas av ekoutredare som tillhandahålls och bekostas av landets ekorotlar. De utredare, som önskar arbeta med förundersökning under begränsad tid även utanfor sitt eget hemdistrikt, bör vara frivilligt anmälda. De tas i anspråk då en förundersökning startar och arbetar tills den slutförts. Förundersökning förläggas till den plats där det brottsmisstänkta annons- och fakturabolaget har sitt säte.*

De föreslagna åtgärderna till operativ verksamhet gör det möjligt att arbeta med fokusering på att driva förundersökning, som är en förutsättning för att åklagare skall kunna väcka åtal och gärningsmän bli lagförda.

Källor:
http://internetsweden.se/112/Annons-%20och%20fakturabedr%C3%A4gerier%202003.pdf
http://internetsweden.se/112/Bilaga.pdf

11 ÅKLAGARMYNDIGHETENS IAKTTAGELSER 2012

I Åklagarmyndighetens tillsynsrapport för ”***Fakturabedrägeri - Kvaliteten i den brottsutredande verksamheten***” 2012:7, 2012-11-21 (dnr ÅM-A 2012/0764) så påtalar myndigheten en lång rad brister i polisens hantering av fakturabedrägerier och vitsordar ett flertal insatser, som:

Vid granskningen har särskilt uppmärksammats polismyndigheternas bristande möjligheter till samordning av ärenden och behovet av att göra något åt detta problem. ***Det måste skapas bättre förutsättningar för samordning av ärenden över länsgränserna****.*

Ytterligare åtgärder kan vidtas för att öka samordningsansvaret avseende brottslighet av aktuellt slag. Det skulle t.ex. kunna övervägas om ***det bör införas någon form av enhet inom Polisen och/eller Åklagarmyndigheten som har samordningsansvarför länsöverskridande brottslighet****.*

Dessutom skulle ***en nationell databas kunna tillskapas där alla uppgifter om bluffakturaföretagen, dess företrädare och konton samlas.*** *Även Rikspolisstyrelsen har i sin förstudierapport pekat på* ***behovet av ett särskilt register som är anpassat för just bedrägeriutredningar****.*

Inom Åklagarmyndigheten kan samordningen förbättras både inom myndigheten och gentemot Ekobrottsmyndigheten *om det aktuella ”misstänkta” bolaget registreras i Cåbra som misstänkt juridisk person. I denna fråga bör förändrade diarieföringsföreskrifter övervägas.*

Förundersökningsledaren bör regelmässigt och fortlöpande under brottsutredningen överväga om andra brottsrubriceringar än bedrägeri kan vara aktuella. *Det bör också beaktas att Ekobrottsmyndigheten har värdefulla kunskaper om ekobrottsrelaterad brottslighet som kan komma till nytta i en brottsutredning om fakturabedrägeri.*

Granskningen visar också på ***behovet av att åtgärder vidtas för att se till att rätt brottskoder anges*** *i ärendehanteringssystemet Cåbra.*

Vid granskningen ***har också uppmärksammats att en ökad kompetens inom Polisen skulle kunna bidra till en förbättrad kvalitet i handläggningen av fakturabedrägerier****. Utbildningen skulle bl.a. kunna ta upp frågor kring* ***brottstypen bedrägeri i allmänhet och utredningsmetodik gällande fakturabedrägeri i synnerhet****.*

Bedrägeribrottslighet förekommer ofta tillsammans med annan ekonomisk brottslighet. Mot denna bakgrund och med hänsyn till den framtida förändrade organisationen för ekobrottsbekämpningen är det viktigt att också Åklagarmyndigheten ser över behovet av utbildningsinsatser. *Även iakttagelserna och slutsatserna i denna rapport bör ligga till grund för översynen av utbildningsinsatserna.*

Källa: http://www.aklagare.se/PageFiles/10113/Rapport%20kvalitetsprojektet%20inkl%20bilagor%20130402.pdf

12 BESKRIVNING AV BEDRÄGERIERNA OCH BOLAGEN

12.1 BESKRIVNING AV BLUFFAKTUROR

Bluffakturor är ett samlingsbegrepp för fakturor och räkningar som uppkommit genom bedrägliga former eller utan tidigare kontakt med avsändaren.

Begreppet inbegriper även sk ***erbjudanden*** som utformats för att av mottagaren uppfattas som en faktura eller räkning. Ofta är texten ”*Detta är ett erbjudande, betalningsplikt föreligger ej*” skrivet i mycket finstil text på dessa fakturaliknande erbjudanden.

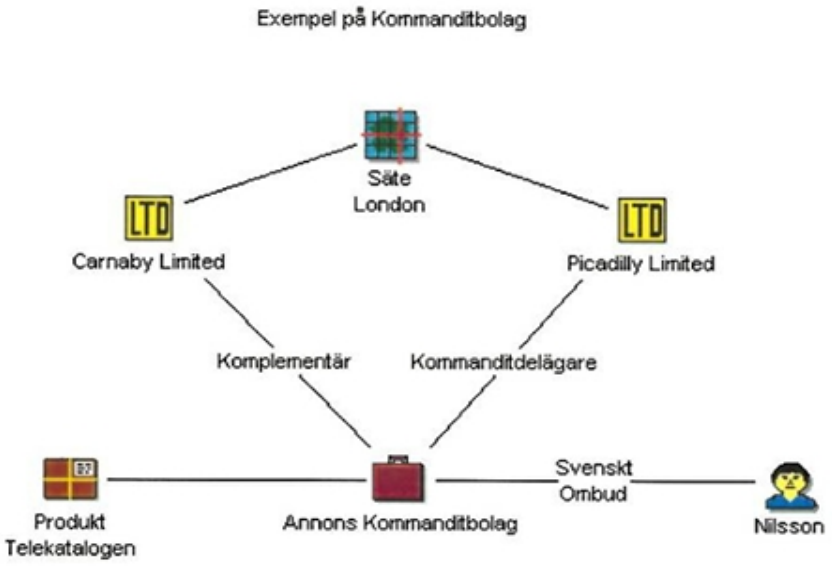
12.2 BESKRIVNING AV ”BLUFFAKTURABOLAG”

Ett bluffakturabolag är ett bolag som ställer ut fakturor enligt beskrivning under punkt 12.1. Fakturorna är inte beställda och ibland finns det ej någon tjänst eller produkt eller så det finns en produkt som är av undermålig kvalitet. Nedan visas ett par exempel på hur bolagen är uppbyggda.

Bluffakturaverksamheten är grov organiserad ekonomisk brottslighet. Den är riksomfattande och drabbar främst företag, myndigheter och kommuner men även privatpersoner, som luras att betala utsända fakturor.

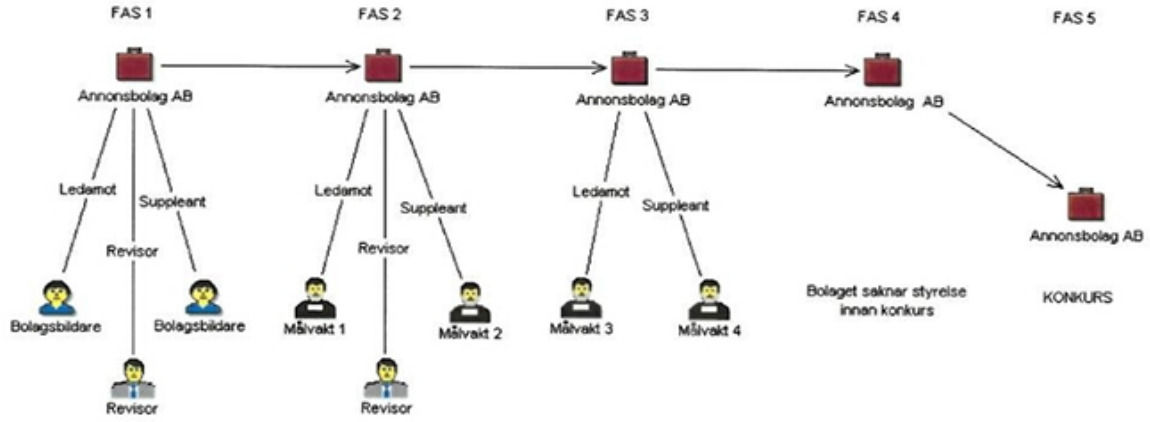
Följande bolagsexempel är generellt för samtliga bolagsstrukturer inom ekobrottsligheten.

Utställarbolaget av bluffakturan anger sällan valida kontaktmöjligheter på faktura och ev. hemsida, för att på så sätt göra sig onåbar för klaganden och bestridning.



Bildkälla: Rikskriminalpolisen 2003

Utställarbolaget av bluffakturan är sällan samma juridiska eller fysiska person som **betalningsmottagaren** av bluffakturan. I exemplet ovan är Annons Kommanditbolag utställarbolaget av bluffakturor medan betalningsmottagaren är ett annat (exempel nedan Annonsbolag AB).



Bildkälla: Rikskriminalpolisen 2003

I exemplet ovan är Annonsbolag AB endast aktivt i FAS 2 (då de är betalningsmottagare), i FAS 3 tar utredande polis vid pga av inkomna anmälningar. Polisen som mycket sällan når framgång i dessa utredningar pga av komplexiteten (se nedan), så lämnas ärendet i FAS 4 över till en Skattebrottsenhet med avsikt att göra en ”*Al Capone*”, (vilket innebär att polis misslyckas med att beivra brott och SKV eller EBM istället utreder skattebrott. Det är betydligt mer vanligt att SKV/EBM är framgångsrika, än att bluffaktureringen beivras).
Perioden mellan FAS 2 till FAS 5 understiger sällan 9 månader och det sker ”aldrig” att tidigare ledamöter döms för brott.

Bildkälla: Rikskriminalpolisen 2003

Utöver ovan exempel kan nämnas att telefonnummer kan använda riktnummer från Uppsala och domännamnsinnehavare kan har uppgett adress i Umeå vid registreringen av domännamnet.*

* Not. Från juni 2013 har domännamnsregistret .SE, för domännamn med ändelsen .se, efter påtryckningar från Datainspektionen behövt anonymisera alla domännamnsinnehavare som är privatpersoner eller enskilda firmor, med hänvisning till Personuppgiftslagen.

Det händer även att Annonsbolag AB (i exemplet) i nästa steg anlitar ett inkassobolag, **med** Datainspektionens tillstånd att bedriva inkasso i Sverige.
Idag finns *ett antal* utfärdade tillstånd för bolag som är bluffakturerande bolags ”**egna**” inkassobolag.

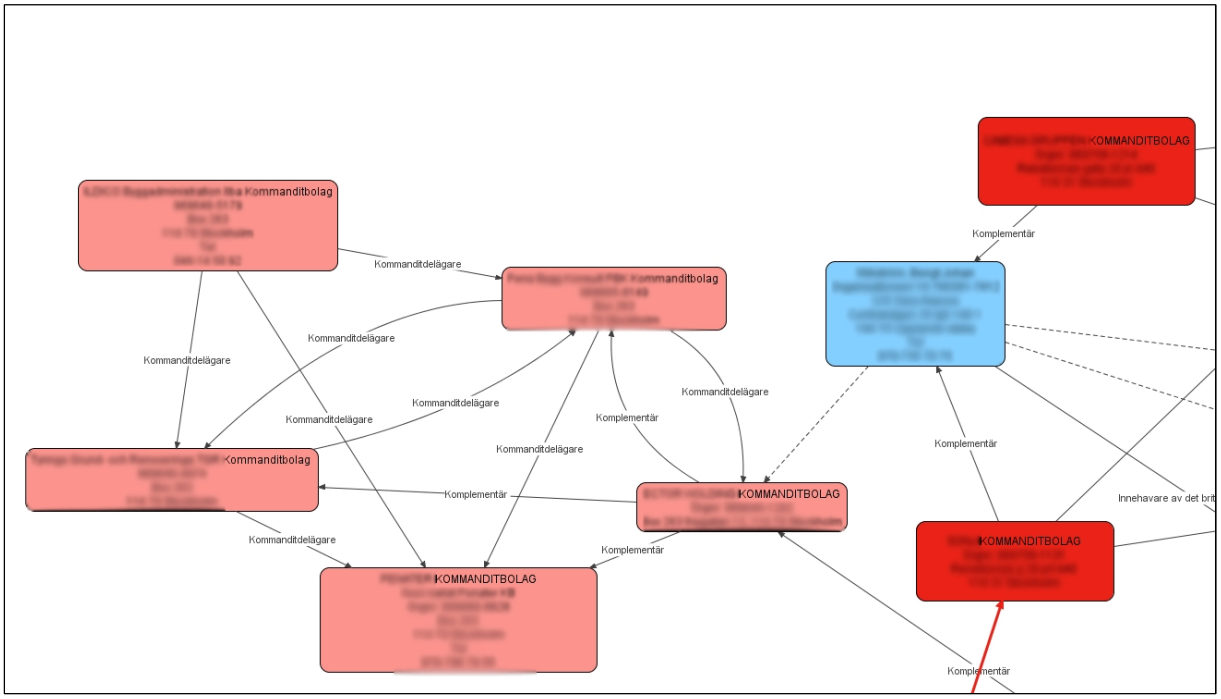
Även seriösa inkassobolag används för att driva in dessa fordringar, då Datainspektionen sällan utför noggrann kontroll av nya klienter. Mer om denna problematik under *Datainspektionen.*

12.2.1 Exempel: Kommanditbolag

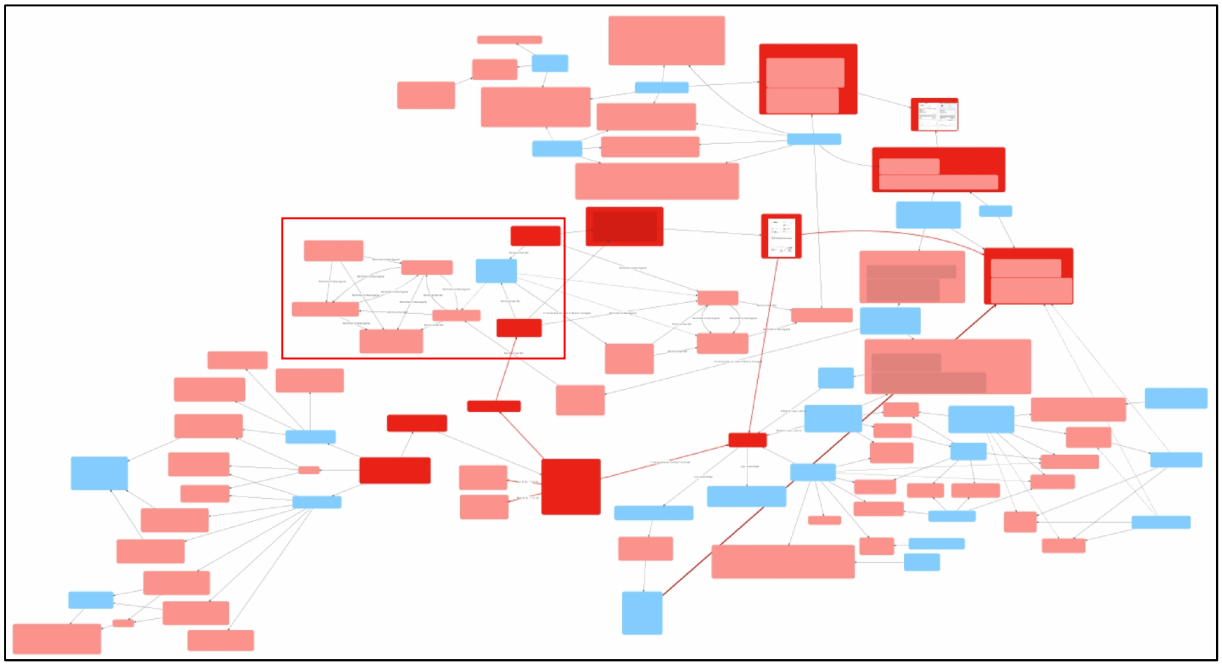
(Registreringskostnad: från 900 kronor)

I nedan exempel skickades ett större antal bluffakturor ut i flera omgångar för ett flertal olika söktjänster på Internet (4 olika falsk- eller målvaktsregistrerade domännamn användes och hemsidorna gav uttryck för att vara sökregister över bolag, något som inte var verkligheten, utan dessa var statiska sidor utan bakomliggande register, dvs fasader).

I just denna del av denna ”sfär” användes 7 stycken kommanditbolag.
De rosa bolag är ”byggbolag” som alla är komplementärer eller kommanditdelägare till varandra.
Den blå rektangeln visar individen som bildat kommanditbolagen, men efter att girokonton skapats, lämnat bolagskopplingen. De röda rektanglarna är avsändare av bluffakurorna, respektive initial betalningsmottagare. Betalningsmottagare har successivt bytts ut till de rosa rektanglarna, som är 4 byggbolag och ett holdingbolag.



För att visa hur denna typ av billig och ”anonym” bolagskonstellation nyttjas för att penninghäleri och är en del i betydligt större grupperingar, så är ovan bild tagen ur följande **större sammanhang**:



På samma sätt som innan så motsvarar blå färg individer, röd färg motsvarar bluffakturerande verksamheter och rosa färg motsvarar ett bolag (kommanditbolag, aktiebolag eller UK Limited-bolag. Värt att nämnas är att 21 av 26 individer ur denna ”gruppering” har namn som tyder på baltiskt ursprung, flertalet är utan svensk personnummer och skrivna endera på en boxadress eller en c/o-adress.

Bluffakturorna har företrädelsevis avsett falska sökregister och SEO-tjänster på Internet.

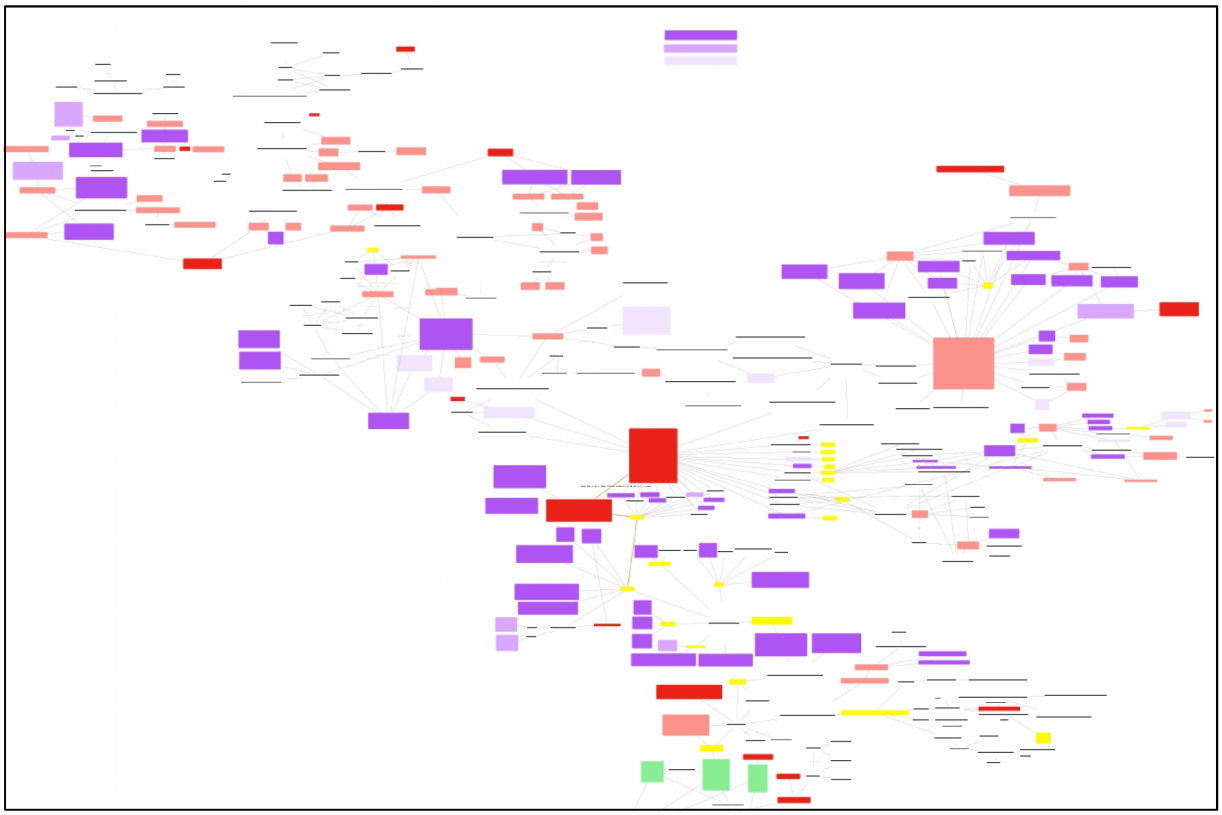
Trots att ovan kartläggning är skapad 2012, så är endast 5 konkurser inledda eller avslutade för de rosa och röda bolagen, med synliga skulder från ca tjugo tusen kronor till några hundra tusen kronor ända upp till 32 miljoner kronor för ett av byggbolagen, som haft direkt koppling till bluffakturautskicken. (som enligt uppgift från SKV även är central i en ekoutredning rörande systematiskt fusk med ROT-avdrag och grovt skattebrott).

Övriga bolag är alltjämnt verksamma, varav flera hunnit byta bolagsnamn samt ett flertal hunnit byta flera generationer av styrelseledamöter. De flesta bolagens verksamhet är beskrivna som byggbolag och entreprenadbolag men även betalningslösningar på Internet och söktjänster på Internet mm.

Motsvarande sätt att brottsövergripande kartlägga brottsliga grupperingar, sker idag inte hos någon utredande myndighet i Sverige. Endast i ett fåtal fall hos bla EBM/Polis/SKV (Operation Selma, Alfred och Draupner i Skåne-regionen) så har det varit frågan om speciella kraftsamlingar i form av informationsmässigt, myndighetsövergripande samarbeten mellan ett flertal myndigheter, för att begränsa ekonomiska flöden till enskilda grupperingar. **Problemet är att det handlat om tidsbegränsade projekt och direkt efter att projekten avslutats så har den brottsliga aktiviteten ökat markant igen.**

13 RELATIONEN MELLAN BOLAGENS SKULDSALDON OCH VERKLIGA INTÄKTER

För att visa systematiken och omfattningen från ett annat perspektiv, där en **helt annan gruppering** är kartlagd och färgerna istället symboliserar inledda/avslutade konkurser (mörklila), likviditationer (mellanlila) och avregistrerade bolag (ljuslila). Bland de mörklila **konkurserna** finns ett flertal aktiebolag som tillsammans har **redovisade skulder på 100,8 miljoner kronor**.



Dessa 100 miljoner, bör även kunna sättas i följande perspektiv:
Tittar vi på ”**Företagslansering Sverige AB**” som under 9 månaders verksamhet under 2011 bedrev verksamheten [***hittaforetagen.se***] och som Tingsrätten konstaterat sysslade med ”**Grovt bedrägeri**” när de med utpressningsliknande telefonförsäljning och efterföljande bluffaktura fick svenska företagare att betala **55 miljoner kronor*** (Detta bolag är ett av de lila bolagen ovan).

Konkursen inleddes i augusti 2012 och har idag (juni 2013) ett skuldsaldo på **8,5 miljoner kronor**. Dessa 8,5 miljoner är allstå vad som syns när en anmärkningskontroll sker mot bolaget, men är helt andra siffror än vad deras bluffverksamhet omsatt, då den motsvarar ca 15% av de 55 miljonerna.

Om vi då utgår från att Företaglansering Sverige AB:s relation mellan skuldsaldo och Intäkter (SKV) är genomgående för de kursade bolagen i kartläggningen ovan, så motsvarar deras verksamheter inte mindre än **652 miljoner kronor**, vilket i så fall skulle motsvara drygt hälften av Svensk Handels uppskattade årliga siffra för Bluffakturor (1,2 miljarder).
Problemet är att kartläggningen ovan endast avser en tunn tårtbit av den svenska organiserade ekobrottsligheten.

* Skatteverkets skatterevision: http://sverigesradio.se/sida/artikel.aspx?programid=96&artikel=5344943

Allmänt kan förmodas att bluffakturabolagen har en fördel av fakturamottagarnas höga betalningsmoral samt att företagarnas betalning sker i en blandning av godtro, rädsla, misstag eller slarv.

Det handlar om mycket stora pengar i dessa verksamheter. Enligt Svensk Handels uppskattning så omsätter bara bluffakturor årligen i Sverige 1,2 miljarder kronor från svenska näringsidkare.

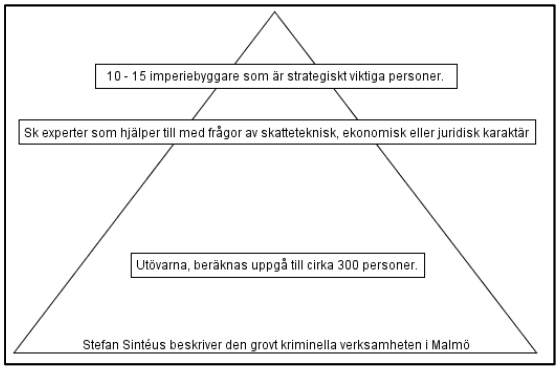
Det skattemässiga bortfallet enbart för moms beräknas till 300 miljoner kronor; därtill kommer arbetsgivaravgifter, bolagsskatter samt källskatter. Bolagen verkar helt utanför systemet.
Inga skatter eller avgifter betalas och inga deklarationer görs och arbetskraften är oftast "svart".
Styrelseledamöter, firmatecknare och kontoinnehavare är betalda målvakter eller ID-kapade ovetande personer.

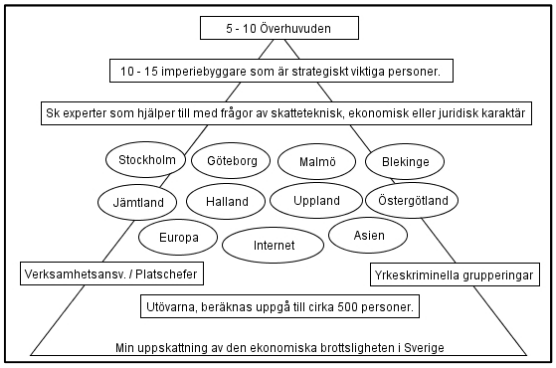
Bluffakturabolagen är endast en länk ur en kedja i bolagssfärer som är verksamma inom den organiserade ekonomiska brottsligheten. All tänkbar brottslighet förekommer i dessa grupperingar.

Delar av intäkterna från den ekonomiska brottsligheten investeras även i utländska partier av amfetamin, som smugglas in till Sverige för, något som inte minst 4 större tillslag visar i nordvästra skåne under det senaste året till ett värde av hundratals miljoner kronor.*

*– Under vårt arbete med **mord**utredningarna såg vi tidigt **kopplingar till bedrägeriverksamheten**, säger **Stefan Sintéus, chef för länskriminalpolisen i Skåne**. I de här kretsarna [den organiserade brottsligheten] var man tidigt ute med **kortkapningar**. Nu ser vi hur **strategiskt viktiga kriminella** finns med kring **bluffakturorna**.*

Vid en jämförelse av de nivåer / hierarki som Polisen i Malmö analyserat fram under de senaste åren, så skiljer den sig inte nämnvärt från den uppdelning jag själv ser för den organiserade ekonomiska brottsligheten i Sverige, sedan ca 5 års tid tillbaka, då bla tidigare ”krig” mellan yrkeskriminella grupperingar bytts till att de är verksamma ”sida vid sida” eller ”rygg mot rygg” i till synes konkurrerande verksamheter. Det är uppenbart organiserat från högre nivå.





* *Källa:* http://hd.se/skane/2013/02/22/ligornas-kapacitet-oroar-polisen/
* *Källa*: http://www.polisen.se/Skane/Aktuellt/Nyheter/Gemensam/okt-dec/Organiserad-brottslighet-bekampas-pa-flera-nivaer-samtidigt/

14 BETALNINGSGRAD AV BLUFFAKTUROR

Det är svårt att ge ett enkelt svar på hur stor betalningsgraden är för bluffakturor, då flera olika faktorer verkar spela in, som tidigare kontakt, förväntad faktura, påtryckningsmedel (hot om indrivning, kronofogdemyndigheten mm), belopp osv.

När Visma SPCS i maj/juni genomförde en undersökning kring bluffakturor* visade resultaten bland annat att av de tillfrågade så hade 54% fått en bluffaktura, **12% lurats att betala bluffakturor**, 65 % ansåg att straffen borde skärpas och 32 % ansåg att polisen inte tar ärendena på tillräckligt stort allvar. Endast 17 % menar att polisen gör så gott den kan.

Dock bör man läsa undersökningar som ovan, medveten om att tillfrågade företagare behöver ha kommit till insikt om att han verkligen har blivit drabbad och lurad. Detta är långt ifrån alla som är, utöver det så är det påfallande många som bestrider bluffakturor, utan att göra en polisanmälan.

Det tyder även Polisens egna uttalanden för, då de menar att de flesta anmälningar som sker, avser försök till bedrägeri (med bluffaktura), alltså utan genomförd betalning. Därmed är mörkertalet fortfarande stort vad gäller den ekonomiska omsättningen för denna brottslighet.

Som enda kända exempel från mars 2012 och som en del av Operation Selma i Skåne, så genomförde bland annat Skatteverkets specialrevisorer ett tidigt tillslag mot två bolag i Malmö och kunde för första gången jämföra den egna bokföringen över utgående bluffakturor mot transaktionerna hos Bankgirocentralen *. De två bolagen delade förutom på gemensamma bolagsmålvakter, även gemensam anonym boxadress och oregistrerat kontantkorts telefonnummer.

Det ena företaget hade endast skickat ut 1300 fakturor. Av dessa var 280 stycken betalda.
Snittvärdet per faktura var 6 000 kronor (280 * 6 000 = 1 680 000 kronor)
280 betalda av 1300 utskickade bluffakturor = **21,5%**

Det andra bolaget hade skickat ut 3 965 stycken bluffakturor, men till ett snittbelopp på ca 5 000 kronor. Här hade 1 490 betalat av de 3 965 utskickade bluffakturorna = **37,6%**
1 490 betalda * a pris 5 000 = 7 450 000 kronor.

Slår vi ihop dessa två bolags bluffakturor, så skickades det ut 5 265 bluffakturor och 1 770 stycken betalades, vilket innebär att var tredje; **33,6% av alla utsända fakturor betalades**, till ett värde av 9 130 000 kronor. Det innebär likaså att av de totalt 5 265 bluffakturorna så fick bedragarna **1 734 kronor per utskickad faktura!**

Stefan Sintéus, chefen för länskriminalpolisen i Skåne säger i artikeln nedan: **”Var tredje person som blir utsatt för bluffakturor betalar faktiskt.”***

Källor:
* http://www.mynewsdesk.com/se/pressroom/visma/pressrelease/view/hoejd-beredskap-mot-bluffakturor-infoer-sommaren-875447
* http://www.sydsvenskan.se/malmo/kravs-pa-moms-for-bluffakturor/
* http://www.sydsvenskan.se/ekonomi/brottsligt-skicka-bluffakturor/

15 TILLVÄGAGÅNGSSÄTT BLUFFAKTUROR

15.1 BLUFFAKTUROR TILL FÖLJD AV BEDRÄGLIG TELEFONFÖRSÄLJNING

För att ge en mer förklarande bild av den typ av bedrägliga telefonsamtal som sker, så presenteras 4 varianter av vanligt förekommande säljsamtal.

15.1.1 TELEFONINFÖRSÄLJNING VARIANT 1

Försäljning via telefon där säljaren påstår att det finns ett befintligt gällande avtal för någon typ av tjänst och säljaren bara ringer upp för att kontrollera adressuppgifter inför att förnyelsefakturan nu skall skickas ut, ofta till en kostnad runt 20 000 kronor, när den uppringde opponerar sig eller vägrar, så hotas ärendet gå till inkasso och Kronofogdemyndigheten. Men säljaren ber sedan kunden vänta lite för att denne ska prata med sin chef, för att sedan komma tillbaka och erbjuda den uppringde att ingå ett ”avslutande avtal” som då endast kostar **6 - 8 000 kronor**, men som spelas in digitalt (ljudupptagning).

Naturligtvis fanns det inte något gällande avtal i botten, utan den uppringde har nu ingått ett **nytt** avtal under falska och bedrägliga former och förespeglingar. Beloppet faktureras och avtalet är ofta ett annuellt löpande avtal, som är dessutom är omöjligt för den drabbade företagaren att säga upp. Bluffbolaget (”avtalsparten”) hinner ofta överlåta kundavtalen (ljudfilerna) till nya bluffbolag innan det gamla bolaget försätts i konkurs, dessa nya ”avtalsägare” fortsätter sedan att fakturera den drabbade från år 2.

Faktureringen
Ofta faktureras beloppet av annan juridisk person, som den falska fordran påstås ha överlåtits till (ett sk factoringbolag). Och på detta sätt lyckas bedragarna försvåra ytterligare för den drabbade.

Detta då det införsäljande bolaget meddelar att:
- Vi har sålt vår fordran till *factoringbolaget*, det är dem du behöver vända dig till med invändningar.

Factoringbolaget å sin sida menar att:
- Vi har bara köpt denna fordran och om du har klagomål kring avtalet, så behöver du vända dig till *säljbolaget* som du ingått avtalet med.

I verkligheten sitter ofta samma personer i styrelsen för båda bolagen, använder samma adress och endast olika telefonnummer.

15.1.2 TELEFONINFÖRSÄLJNING VARIANT 2

- Försäljning via telefon där säljaren påstår att han har noteringar från sist de talades vid för ett halvår sedan att han skulle återkomma nu, för att de kommit överens om att de skulle trappa ner på annonseringen och han nu ringer för att stämma av att det fortfarande stämmer.
Om ja, vad bra då skickar jag över en orderbekräftelse som du skriver under och skickar tillbaka, så löper er annonsering ut efter kommande tremånadersperiod, ni kommer alltså att avsluta er annonsering efter det och ni får själv ta kontakt med oss om ni vill återuppta annonsering.

När den förtryckta bekräftelsen kommer fram så står det att läsa 2 995:- vilket den uppringde tycker är en acceptabel peng för att slippa eländet som han inte känner till sedan innan, han skriver under och skickar tillbaka, men missar detaljen att det står ”**No. of exposures: 8**”
(Syftar till att annonsen skall visas under 8 olika kategorier)
Det som sedan faktureras: 2 995 (belopp) x 8 (antal kategorier) x 1,25 (moms) = **29 950 kronor**

Naturligtvis fanns det inte något avtal i botten, utan den uppringde har förmåtts att ingå ett nytt avtal under falska och bedrägliga former. De påstådda katalogerna där annonseringen skulle ske lyser med sin frånvaro och när det gäller annonsering i webbaserade kataloger, så handlar det om stulna texter och bilder från seriösa webbsidor på undermåliga sidor som tillverkats med gratis (Open Source) publiceringsverktyg som *Wordpress* eller *Joomla*.

Bluffbolaget (”avtalsparten”) hinner även här överlåta kundavtalen till nya bluffbolag innan de försätts i konkurs, dessa nya avtalsägare fortsätter sedan att fakturera den drabbade från år 2 osv.

15.1.3 TELEFONINFÖRSÄLJNING VARIANT 3

Försäljning via telefon där säljaren egentligen är ”återförsäljare” till seriösa etablerade leverantörer såsom Telebolag, Försäkringsbolag, Pensionfondsbolag mfl. och använder följande upplägg (från autentiskt föräljningsmanus):

- Säljaren: Hej, jag heter ***påhittat namn*** och ringer ifrån ***Telefonverket***
- Kund: Hej
- Säljaren: Hej, jo du använder ju ***Telefonbolag1*** idag, eller hur?
- Kunden Nej: Jag använder ju ***Telefonbolag2***
- Säljaren: Oj ja ursäkta, ***Telefonbolag2*** var det ju, jag som såg fel på listan här.
- Säljaren: Fortsättning/Om Ja: När vi la in dig där senast så fick du ju automatisk vår ***prisgaranti*** som gör att vi alltid kontaktar dig när vi hittat ett billigare alternativ, och det är därför vi ringer dig idag. Allt är som vanligt, du är fortfarande kvar hos oss, men det kommer stå ***Telefonbolag1***på fakturorna i framtiden istället för ***Telefonbolag2***, så det är väl inte fel med lite lägre priser?
Kund: - Nej, det är det väl inte.
- Säljaren: - Precis, så det enda vi behöver göra för att det ska bli korrekt här är att vi gör ett litet kort

muntligt avtal, och så börjar de nya billigare priserna gälla inom någon vecka, du får ett brev i posten också så du vet att allting blivit korrekt. Då startar jag inspelningen och du heter....osv.

Detta tillvägagångssätt drabbas ofta äldre näringsidkare eller speciella yrkesgrupper som åkerier, innehavare av skogsskiften och frisörer, som är en extra sårbara, då de sällan är införstådd i skillnaderna eller ens att det är möjligt att ingå avtal över telefon.

15.1.4 TELEFONINFÖRSÄLJNING VARIANT 4

Försäljning via telefon där säljaren påstår att denne ringer från *Svenska domänregistret/IT-verket* eller liknande (försöker ge ett intryck att företräda myndighet) och anledningen till samtalet är pga av att den uppringde står som innehavare av ett domännamn (ex. janssonsbil.se).

Säljaren: - Och nu är det så att vi precis fått in en beställning från en kund som tänker registrera janssonsbil under com, net, biz, info och nu. Men eftersom du redan har janssonsbil.se så är vi tvungna att kontakta dig för att ge dig förtur innan vi registrerar domänerna på vår kund.
Vill du utnyttja din förtur eller kan jag registrera domänerna på vår kund?

I flera fall brukar övertalningen kryddas med att den andra kunden kommer att lägga upp porr på domänerna.

Prisbilden som anges varierar också från att presenteras som ***”engångskostnad” och varumärkesskydd på Internetpå 1995:- för alla .com, .net, .biz, .info och .nu*** till att presenteras som ***”Det kostar bara 199,50 om året för alla .com, .net, .biz, .info och .nu”***

Även här tas en ljudupptagning upp som avtalsbindning.

Och när fakturan dimper ner så är den på **12 468,75:-**

För det kostar då 1 995 x 5 domäner x 1,25 (moms) = 12 468,75 alt.
199,5 x 10 år x 5 domäner x 1,25 (moms) = 12 468,75

Naturligtvis finns det inte någon annan kund, då det vore affärsmässigt oklokt att riskera den kundens beställning och såklart finns ingen ”förtur” i detta förfarande (utan samtliga dessa toppdomäner tillämpar först-till-kvarn-tilldelning). Dessutom varierar det mellan de domänbluffande bolagen från att INTE alls registrera de domäner den drabbade betalat för, till att domänerna blir registrerade, men med bluffbolaget som innehavare (för att kunna utöva en typ av utpressningsliknande relation till den drabbade, kallas även ”inlåsningseffekt”).

Ovan scenario är under perioder fullt utbytbart med ”varumärkesregistreringar” där det är en rysk eller polsk kund i andra luren som skickat in en beställning för ”Janssons Bil”, men förtur erbjuds såklart eftersom bolaget heter så. Kostnaden för detta är en ”engångskostnad så länge bolaget finns” på 10 000 kronor

15.2 MASSUTSKICK AV BLUFFAKTUROR, UTAN TIDIGARE KONTAKT

Med jämna mellanrum skickas tusentals obeställda fakturor ut till näringsidkare runt om landet. Oftast anger fakturan snarlika namn som seriösa tjänster. Det händer också att seriösa verksamheters namn och logotyper ”kapas” och fakturorna är identiska som orginalet, med undantag av Bank- eller Plusgironummer dit betalningen skall ske. Dessa girokonton hanteras sedan av den bedragarna, oftast genom bolag med bolagsmålvakter i styrelsen.
Två exempel på detta förfarande i nutid:

Exempel1:
118200.se och Nummerupplysningen.se (Mellanhand Media AB)

Under våren och sommaren 2012 skickar bolaget Mellanhand Media AB ut två omgångar av påminnelsefakturor till tiotusentals svenska företagare.

Det första utskicket avser verksamheten 118200.se, som tidigare skickat ut bluffakturor med annan betalningsmottagare: Malmöbaserade Åro AB (byggbolag).

Det andra utskicket av påminnelsefakturor avser Nummerupplysningen.se, som drivs av ett Estniskt bolag (med svenska bolagsföreträdare). Tidigare har Nummerupplysningen.se skickat ut fakturor med annan betalningsmottagare: Alfa fakturaservice AB (som även bedriver snabblånsverksamheten ”Lite Cash”).

Istället är det nu Mellanhand Media AB (Telemarketingbolag) som står som betalningsmottagare för alla påminnelsefakturor. I styrelsen hittas två bolagsmålvakter (19 och 21 år) utan tidigare bolagsengagemang.

Samarbete mellan Polis, EBM och civila experter analyserar och kartlägger kopplingar och grupperingar och samtliga är helt överens om att verksamheten bedrivs från Malmö av för polisen kända personer.

Trots detta tvingas Malmö lämna över hela ärendet till Stockholm.

För bolagsmålvakterna är skrivna i Solna och då bolagsadressen är den enes bostadsadress, så skickas alla **drygt tusen polisanmälningar** till Stockholm Norr.

Stockholmspolisen har naturligtvis ingen som helst förutsättning att klara upp denna utredning, utan hjälp från Polismyndigheten i Malmö.

Såhär ett år senare bolagsmålvakter bytts ut, misslyckade utmätningsförsök för skulder på 135 000 kronor har registrerats, men polisutredningen i Stockholm har inte kommit längre.

Det andra exemplet är högaktuellt från juni 2013, varför detaljer om bolag och personkopplingar ej kan lämnas.

Exempel2: Lokaldelen Sverige AB
(Nordic Support Finans KB & Skand – Gruppen Finans AB)

I början av juni 2013 kapades det seriösa bolaget Lokaldelen Sverige AB:s fakturor och bedragare skickade i Lokaldelen Sveriges AB:s namn ut påminnelsefakturor, där den enda skillnaden från orginalfakturorna var angivet telefonnummer och gironummer, dit betalningen skulle ske.

Då såväl kundnummer, kundens vanliga fakturabelopp och kundadresser var valida, så får det anses som troligt att bedragare på något sätt kommit över Lokaldelens kunddatabas.

De skickades ut ca 2 500 påminnelsefakturor, men tack vare rådigt ingripande av Posten Sverige, så stoppades ca 37 500 påminnelsefakturor från att skickas ut till drabbade.

Fakturabeloppen på påminnelsefakturorna varierade mellan 800 – 40 000 kronor, med ett totalt fakturavärde på ***åtminstone* 200 miljoner kronor**.

Betalningsmottagare för bluffakturorna var 2 stycken svenska bolag, ett aktiebolag (Byggbolag) och ett kommanditbolag (Byggbolag/Personaluthyrning) som till synes inte hade någon koppling till varandra.

Först efter mycket omfattande kartläggning av civila experter kunde utredande polismyndighet konstatera att det finns kopplingar mellan såväl dessa två bolag, som till ett kommanditbolag som utförde en identisk bluffakturakapning mot Lokaldelen Sverige AB i början av 2011.

Dessutom kopplingar till en större gruppering, kända för bedrägerier sedan mitten av 90-talet.

Utredning pågår.

16 BEDRÄGERIER - TRENDER OCH FÖRÄNDRINGAR

Tidsaxel över bedrägeritrender mellan 2003 - 2012. Den röda streckade linjen ovanför modus motsvarar ungefärlig period då de är som mest frekventa. Beskrivningar på kommande sidor.

16.1 MODEMKAPNING

Modemkapning som drabbade Internetanslutna användare gick till så att skadlig kod laddades ner i bakgrunden, när Internetanvändare besökte vissa sidor eller klickade på annonser, speciellt spelforum och mötesplatser var särsklit mycket smittospridare.
Den nedladdade koden installerade sig själv på klient-PC:n och ringde själv upp dyra porrbetalnummer, som fakturerades separat eller adderades på klientens telefonräkning.
Detta förekom under många olika verksamhets- och bolagsnamn som ScanBill, Internet-B, DateRegon, HarrysExpo mfl. men där samma gruppering låg bakom och där mycket stora betalningar gick till ”Svenska Let To Phone AB” som under verksamhetsåren 2004-2005 redovisade en omsättning på 1,7 miljarder kronor. (http://www.allabolag.se/5565601092/Svenska_Let_To_Phone_AB)
Flera av bolagen och även tillhörande indrivningsbolag representerades av personer med gängtillhörighet i Hells Angels. Även personkopplingar till flera andra senare bedrägerier som Hus- och bilvärderingar, Snabblån, Falska SMS-krav för falska lotterier och Falska porrfakturor till följd av kapning av webbläsare i smarta mobiltelefoner.

Dessa modemkapningar skedde i synnerhet mot svenska användare, men även utländska och var aktiva mellan 1996 till 2005, men rapporter finns så sent som 2011 över det speciellt utvecklade ”dialerprogrammet DateRegon” som användes vid samtliga modemkapningar.

16.2 ANNONSSKOJARE / BLUFFAKTUROR

Annonsskojare av typen där det handlar om telefonskojare som bedrägligt lurar företagare kring annonsinförande i icke-existerande papperskataloger/magasin har förekommit sedan mitten av 70-talet och är konstant, med enda skillnad att verksamheterna emellanåt kan ”byta land” och under perioder helt dedikera sig mot exempelvis Norge, vilket är aktuellt just nu, då ett 40-tal svenska verksamhetsnamn/bolag bedrar norska näringsidkare parallellt med grupperingarnas verksamheter i Sverige.

16.3 BANTNINGSBLUFFAR

Även detta fenomen härstammar sedan 70-talet, då verkningslösa sockerpiller såldes via kuponghäften och veckotidningar. Bantningsbluffar har funnits på Internet sedan starten, men har kraftigt ökat för Skandinaviskt vidkommande sedan ca 2005, då flera svenska och dansk/estniska grupperingar satsar stort på detta i många olika verksamhetsnamn och närliggande bedrägerier och försäljning av förbjudna narkotikaklassade preparat och läkemedel.
Ofta marknadsförs gratis proverbjudande genom stora annonser på större seriösa webbplatser och i sökmotorer och genom högprofilsnamn (kändisbloggare mfl.). Gratisproverna övergår genast till dyra flerårsprenumerationer som inte är möjliga för konsumenten att avsluta.

Verksamheterna har ofta kopplingar till våldskriminella grupperingar som Original Gangsters, Hells Angels och Black Cobra och närliggande bedrägerier.

16.4 DOMÄNSKOJARE

16.4.1 Domänskojare – ”Vi har en kund” - Telefon

Domänskojare blir egentligen synliga i slutet av 90-talet genom ”Gröna Verket” (som senare har sålts till VeriSign Sweden AB). Gröna Verket pysslade med telefonförsäljning mot företag och ringde upp och påstod att det funnits en tidigare kontakt och att de nu följde upp denna kontakt och sålde då in en rad verksamhetsbeskrivande domännamn till kraftiga överpriser.

Runt i slutet av 2003, modifieras försäljningstekniken, då flera bedrägliga verkamheter som IT-verket, Domänregistreringar Europa och EUWEB börjar kontakta svenska domäninnehavare med samtal om att ”..vi har en kund som lagt en beställning på ditt domännamn, fast med ändelserna .com, .net, .biz, .info och .nu och vi kontaktar dig för att erbjuda dig en förtur, som gäller NU..”. Den uppringde ovetandes om att domännamn registreras av vem som helst, utan förprövning gick ofta på denna falska introduktion av samtalet, eftersom det inte fanns något intresse från annan kund, utan telefonsäljaren lyckades oftast helt dölja kostnaden i samtalet och vid den inspelade avtalsbindningen och som vanligtvis låg på 10 faldigt gängse kostnad per domännamn. Så istället för några hundralappar så debiterades kunden för flera tusenlappar per domännamn.

Detta var mycket omfattande fram till slutet av 2007, då det nästan upphörde i Sverige över en natt. Istället startade samma personer utländskregistrerade bolag och verksamheter i Finland, Baltikum, Polen, Spanien, Schweiz och Österrike.
Samma säljare som innan satt i Stockholm, men ringde utländska kunder via IP-telefoni kopplade till utländska telefonnummer och ”exporterade bedrägeriupplägget” till olika europeiska länder.
Bara i Sverige, baserat på kundernas kartlagda registrerade domännamn så omsatte denna typ av Domänskojarverksamhet mellan 250 – 300 miljoner årligen. Ovisst hur mycket den svenska verksamheten omsatt globalt.

Med endast minimala manusförändringar har ovan bedrägeri även fungerat för att sälja in varumärkesregistreringar för 10 000 kronor styck.

16.4.2 Domänskojare – ”Vi har en kund” – E-post

Sedan ungefär 2005/2006 så har kinesiska domännamnsskojare systematiskt bearbetat domännamnsinnehavare enligt ovan upplägg, med enda skillnaden att de använder e-post för att kontakta innehavare. Där utger de sig för att vara en myndighet eller auktoritet på området.

16.4.3 Domänskojare – ”domänförnyelse” – E-post

Ett annat domänskojarupplägg är att utifrån sk whois-uppgifter (innehavaruppgifter) av generiska toppdomäner (.com, .net, .biz, .info och .org) ta reda på dels kontaktuppgifter och även förfallodatum för domännamnet, listor för detta finns publikt att tillgå ca 90 dagar innan förfallodatum och den administrerande registraren brukar vanligtvis skicka ut erbjudande om förnyelse mellan 30-60 dagar innan domänen förfaller.

Bedrägeriet ligger således i att under perioden 60-90 dagar innan domänen förfaller, skicka ut ett förnyelsemeddelande (e-post) om att den enda möjligheten om att försäkra sig om att domänen inte

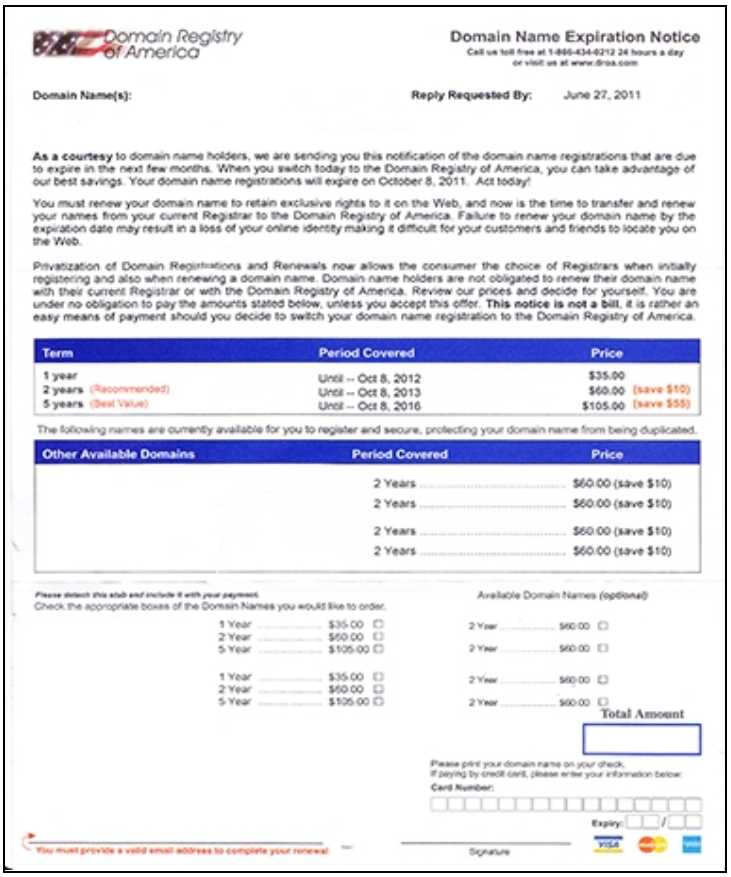
förfaller och hamnar i orätta händer, är genom att klicka på en länk för att betala en förnyelseavgift. (ca 80 dollar). Enligt andrahandsuppgift omsatte denna verksamhet drygt 50 000 kronor per dag.

För de kunder som väljer att att göra en kortbetalning via länken är pengarna endera helt bortblåsta eller så krävs att kunden byter registrar till denna bedrägliga registrar, då endast administrerande registrarer har möjlighet att förnya redan registrerade domäner.

Av de kunder som valt det sistnämnda alternativet, så har de hamnat i en stygg inlåsningseffekt, då domänerna bytt innehavare till registraren (ombudet självt), vilket gör det omöjligt för den egentliga innehavaren att byta registrar, utan får bruka domänen så länge årsavgiften betalas.
Vanligt pris för förnyelser av generiska domännamn brukar ligga på 10-15 dollar per år.

Våra svenska domänskojare låg bakom ovan bedrägeri i mycket stor skala, då det utan större kunskaper gick att skapa ett automatiskt flöde och kunde skickas ut genererade det frisläpps ca 50 000 generiska domäner varje dag.

Ett upplägg som sedan 2007 har adopterats av en internationell aktör som är mest känd som ”DROA”, Domain Registry Of America som når fram till fler, då de använder sig av ett förtroendeingivande tryckt formulär som skickas postledes och med ett pris på 30-35 dollar istället för 80 dollar..



Domain Registry of America

Domain Name Expiration Notice

Call us toll free at 1-866-434-0212 24 hours a day or visit us at www.droa.com

Domain Name(s):

Reply Requested By: June 27, 2011

As a courtesy to domain name holders, we are sending you this notification of the domain name registrations that are due to expire in the next few months. When you switch today to the Domain Registry of America, you can take advantage of our best savings. Your domain name registrations will expire on October 8, 2011. Act today!

You must renew your domain name to retain exclusive rights to it on the Web, and now is the time to transfer and renew your names from your current Registrar to the Domain Registry of America. Failure to renew your domain name by the expiration date may result in a loss of your online identity making it difficult for your customers and friends to locate you on the Web.

Privatization of Domain Registrations and Renewals now allows the consumer the choice of Registrars when initially registering and also when renewing a domain name. Domain name holders are not obligated to renew their domain name with their current Registrar or with the Domain Registry of America. Review our prices and decide for yourself. You are under no obligation to pay the amounts stated below, unless you accept this offer. **This notice is not a bill**, it is rather an easy means of payment should you decide to switch your domain name registration to the Domain Registry of America.

Term	Period Covered	Price
1 year	Until -- Oct 8, 2012	$35.00
2 years (Recommended)	Until -- Oct 8, 2013	$60.00 (save $10)
5 years (Best Value)	Until -- Oct 8, 2016	$105.00 (save $55)

The following names are currently available for you to register and secure, protecting your domain name from being duplicated.

Other Available Domains	Period Covered	Price
	2 Years	$60.00 (save $10)
	2 Years	$60.00 (save $10)
	2 Years	$60.00 (save $10)
	2 Years	$60.00 (save $10)

Please detach this stub and include it with your payment.
Check the appropriate boxes of the Domain Names you would like to order.

1 Year $35.00
2 Year $60.00
5 Year $105.00

1 Year $35.00
2 Year $60.00
5 Year $105.00

Available Domain Names (optional)

2 Year $60.00
2 Year $60.00
2 Year $60.00
2 Year $60.00

Total Amount

Please print your domain name on your check.
If paying by credit card, please enter your information below:
Card Number:
Expiry: /

You must provide a valid email address to complete your renewal

Signature

Sedan 2010 och än idag finns 4 nya svenska aktörer av domänskojare som använder telefon som redskap och som främst drabbar innehavare Sverige, Norge och Danmark.

Dessa aktörer kommer från två olika grupperingar i Sverige, som sysslar med en rad olika bedrägeriupplägg.

16.5 VARUMÄRKESSKOJARE

Se domänskojare.

Skedde genom att telefonsäljaren berättade att de hade en annan kund som var på gång att registrera den uppringdes företagsnamn som varumärke, men att de ringde för att erbjuda förtur..” En förtur som kostade 10 000 kronor ex moms.

16.6 SPAM / PHISHING / NIGERIABREV

SPAM eller oönskad e-postreklam brukar innehålla allt ifrån erbjudande om att skaffa ryska flickvänner till billigt potensmedel, men lika ofta innehåller de besked om att mottagaren vunnit en miljonvinst eller att någon avlägsen förmögen släkting gått bort och efterlämnat ett stort arv som nu erbjuds dig.

Det kan låta självklart att detta är bedrägeri och att om man inte köpt en lott, så kan man inte vinna, lika lite som att en okänd avlägsen släktings dödsbo skulle kontakta arvtagare och meddela arv, genom e-post.
Dock växer Internet med drygt 620 000 användare per dag. Nyanlända användare som inte förstår att vara vaksam och se igenom självklara bedrägeriförsök. Årligen drabbas ett okänt antal svenskar som låtit sig luras på mycket stora pengar, ofta hundratusentals kronor och i enstaka fall flermiljonsbelopp. Vanligtvis härstammar dessa ”Nigeriabrev” från länder i södra Afrika, England eller Spanien, men det förekommer även att svenska bedragare ägnar sig år detta, inte minst för investeringsbedrägerier.

Exempel:
* 2012 döms en Piteåbo till 4 års fängelse till följd av att han stulit 2,7 miljoner i en Nigeriabrevshärva.

* I mars 2013 häktas en 34-årig man från Trollhättan, misstänkt för att vara hjärnan i ett internationellt bedrägerinätverk. Han ska ha lurat företag i tolv länder och skickat sk Nigeriabrev till över 1,8 miljoner människor och även genomfört kontokortsbedrägerier, konstaterar polis och åklagare efter att ha granskat 40 konton som är kopplade till mannen.

* I juni 2013 döms en 75-årig fd politiker i Skellefteå för att ha lurat 6 personer, bland annat fd arbetsmarknadsminister Börje Hörnlund (C), på 900 000 kronor som skulle frigöra stora summor i ett klassiskt Nigeriabrevsupplägg där foton på kistor med dollarsedlar använts för att övertyga offren.

16.7 NIGERIABREV GENOM SOCIAL MEDIA (ROMANSBEDRÄGERIER)

Romansbedrägerier eller Romance Scams handlar i huvudsak om afrikanska bedragare som ”rippar” dvs stjäl information från andra personers Social Media-konton inklusive uppladdade bilder och skapar ett nytt konto, där de utger sig för att vara denna person (eller hittar på en ny identitet) och söka nya livskamrater. Extra utsatta är amerikanska soldater som tjänstgör i utlandstjänst, men även olika typer av affärsmän är vanligt. Bedrägeriet handlar om att tycke ska uppstå och att soldaten ska komma till kvinnan på besök, men det sker ALLTID upprepade kostsamma missöden, som kvinnan förväntas betala. Det finns ärenden där kvinnor lurats på hundratusentals kronor. Dessa bedrägerier blir mer och mer vanliga och offer hittas vanligtvis på dejtingsidor eller i Social mediakanaler som Facebook.

Ett närliggande bedrägeri är husdjur som är till salu på svenska köp&sälj-marknadsplatser, där djuret av outgrundlig anledning befinner sig i utlandet och där en serie av kostsamma transportkostnader, veterinärskostnader, tullkostnader mm tillkommer allt eftersom köparen lagt en handpenning för husdjuret. I verkligheten finns inget djur till salu, utan det handlar om stulna bilder från ett annat djur.

16.8 INTERNETKATALOGER / BLUFFAKTUROR

Bedrägeriet är i det närmaste identiskt med bluffakturor för annonsbedragare, men refererar nu istället till att avse införanden och företagspresentationer på en namngiven Internetkatalog, som lagts upp på en Internetadress och som vanligtvis finns klonade i 20-tal under olika webbadresser.

16.9 RANSOMWARE

Ransomware innebär att klienten utan att vara medveten om det laddar ner en skadlig kod som fryser PC:n och gör den obrukbar att använda, det enda som syns är en webbsida som påstår att PC:n utfört något olagligt som att ladda hem barnpornografiskt material och nu måste betala motsvarande 650-1050 kronor, detta tillsammans med Polisens och Regeringskansliets logotyper. Betalning skall ofta genomföras via Ukash, varför detta kommit att kallas bla ”Ukash-virus” eller ”polisvirus”. Ransomware innebär alltså att klienten behöver betala lösen (Ransom) till bedragare.

Detta virus är utomordentligt sofistikerat och en smittad laptop som flyttas till Danmark, slår om för att visa den webbsidan på danska och den danska polisens logotype istället, så den känner alltså av klientens IP-nummer och geografiskt placerar rätt språks utpressningssida för klienten.

Detta elände har drabbat hela västvärlden sedan sommaren 2010 och har kommit i minst 2 generationer av virus, varav den första var knepig, men gick att få bort. Den senaste är dock inte möjlig att få bort, då den har en rad försvarsmekanismer. Formatering av hårddisken är enda möjligheten att bli fri från den.
Något som gör att allt fler väljer att betala lösen, för att de har mängder med information på hårddisken som inte går att ersätta.

Denna kod finns via olika hackerforum tillgänglig att köpa för att själv anpassa efter egen verksamhet. Då den är så vanlig så är det ovisst om svenska bedragare använder koden. 2012 anhölls ett 20-tal spanjorer för inblandning.

En närliggande internationell plåga är bedragare från Pakistan och Indien som ringer upp användare och påstår sig ringa från Microsoft och att de ringer för att de fått rapport om att användarens PC är infekterad av skadlig kod och att de ringer för att hjälpa till med att rensa bort koden. De handleder användaren hur han tillhandahåller Remote Access (fjärrstyrning) av PC:n och när de väl fått tillgång till PC:n, så övertygas användaren om att skadlig kod installerats. Kostnaden för att rensa den ligger även det på 650-1000 kronor i de fall bankkort inte debiteras flera gånger. Detta har även skett av svenska bedragare i liten omfattning.

Även i dessa fall har raider gjorts mot hela Telemarketingfirmor i Indien som livnärt sig på detta.

16.10 HACKADE KONTON BER VÄNNER OM EKONOMISK HJÄLP

Hackade e-postkonton används för detta och handlar om att bedragare skickar ut likalydande e-postmeddelanden till samtliga e-postkontakter i kontot. Budskapen brukar handla om att man är på en resa och har blivit bestulen och strandsatt och nu vädjar om ekonomisk hjälp för att kunna ta sig hem till Sverige igen. Kontona kapas ofta genom phishing eller pga av innehavarens ”svaga lösenord”.

När det gäller Facebookkonton handlar det om att man ber Facebookvänner om hjälp för att man inte kan logga in på sin Internetbank med sin dosa och ber Facebookvännen pröva och ber om de koder de får fram. Problemet är att koderna är personliga och kopplade till personliga konton, vilket resulterar i att de hjälpsamma får sina egna bankkonton länsade och oönskade transaktioner utförs av den som hackat Facebookkontot och utger sig för att vara innehavaren, tillika vän till de tillfrågade.

16.11 SMS-PHISHING / BETALTJÄNSTABONNEMANG

Detta fenomen har egentligen funnits sedan 2006/2007 men i liten omfattning. Det första kända stora angreppet skickas ut sent på kvällen på nyårsafton 2009/2010 när sk ***SPIM*** (SPAM-SMS) skickas ut till drygt 50 000 svenskar får ett SMS som lyder:

”Hej! Vi onskar er en mycket underbar nytt ar. Vi hoppas att du ar den lyckliga vinnaren av var Karibien semester.Klicka nedan”.

Länken tar den smått överförfriskade mottagaren till en webbsida (yahwin.com) som automatiskt startar en SMS-prenumeration för 8 stycken SMS / vecka (startavgift 80 kronor + 50 kronor per SMS = 480 kronor x 50 000 mottagare = Bedrägeriförsök på 24 miljoner kronor). Genom omfattande kartläggning lyckas anmälan till Etiska Rådet för Betalteletjänster (ERB) leda till att bedrägeriet uppdagas och debiteringarna som satts upp på mobilinnehavarnas telefonräkningar annulleras och Yahwin spärras. Polisen var helt ovetande om att 50 000 smarta mobilinnehavare hade drabbats av detta.

Sedan slutet av 2010/2011 så förekommer denna typ av SMS-bedrägerier av detta slag frekvent, ofta med typiska Nigeriabrevsupplägg som:

”CONGRATULATION!!!YOUR MOBILE NUMBER HAS WON FOR YOU $2,000,000USD IN THE FREELOTTO MOBILE DRAW.TO CLAIM,SEND YOUR NAME & MOBILENUMBER TO: freeukdraw@aol.co.uk”

16.12 SMART-MOBIL-KAPNING / PORRFAKTUROR

Under 2012/2013 har det inkommit flera tusen polisanmälningar till följd av falska fakturakrav/skadeståndskrav som påstår att fakturamottagarens smarta mobil använts för att ladda ner rättighetsskyddat pornografiskt material till mobiltelefonen. Fakturorna har skickats till innehavare av mobiltelefonnummer, vars adress tagits fram från Eniro. Personer från 7 år till 85 år har tagit emot fakturorna/skadeståndskraven.

Användares mobiltelefoners webbläsare har endera klickat på en bannerannons eller besökt en sida, där webbläsaren ”kapats” och en session har tagit webbläsaren till en sida där den initierat nedladdning av material. Skadeståndskrav har sedan sänts på tusentals kronor. Det är såväl samma personer bakom denna kapning av mobiltelefoners webbläsare som fram till 2005 sysslade med modemkapning för flera miljarder kronor. Det är även samma skapare av den skadliga koden.

16.13 FALSKA VÄRDERINGSSIDOR / BLUFFAKTUROR

Runt 2006 dök [fordonsvarderingen.se] (av samma personer som sysslat med modemkapningar tidigare och senare kommer att syssla med kapning av smarta mobiltelefoners webbläsare). Fordonsvarderingen.se erbjöd värdering av din bil. Det enda du behövde ange var bilens registreringsnummer, antal mil, e-postadress och mobiltelefonnummer så skulle värderingen SMS:as till kunden. Såklart var det helt befängda värderingar, men såklart debiterades även 399 kronor, något som inte tydligt framgått av beställningen.

Jämsides med bilvärderingarna (ca 40 kloner i Sverige, Norge och Danmark), så bedrivs flertalet husvärderingstjänster efter samma bedrägliga modell och det bedrevs även kreditupplysningstjänster som Kreditscore och Persondata.nu under liknande modeller, med skillnaden att du även automatiskt initierade en kostsam 24 månaders prenumeration.

Även snabblånsverksamheter, spådomstjänster och ”dödscertifikatstjänster” bedrivs med samma personer bakom verksamheterna.

I Sverige har Konsumentverket löpande varnat för de flesta av dessa skojartjänster, så även norska och danska konsumentinriktade TV-program, som även rest runt till fiktiva adresser i Danmark och Estland för att leta efter ID-kapade estländare som satts som bolagsmålvakter.

16.14 SKRIVARTONER / LYSRÖRSSKOJARE / KONTORSMTRL. / BLUFFAKTUROR

Telefonskojare som säljer skrivartoner och lysrör har förekommit i sedan 80-talet och hade sin storhetstid i slutet av 90-talet fram till början av 00-talet, då samma verksamheter istället börjar med försäljning av andra förbrukningsvaror, som exempelvis rengöringsmedel.

Det vanliga säljupplägget är att ringa för att ”bara kontrollera sitt kundregister” och kontrollera om de fortfarande använder ”4 stycken HP XXX-skrivare” eller ”5 stycken Xerox XXX-skrivare” och som tack för hjälpen för uppdateringen av deras register så vill de skicka över en gratis överaskningsprodukt och önskar verifiera kontaktperson och leveransadress.

Någon present skickades inte, utan istället skickades flera årsförbrukningar av undermåliga toner och färgpatroner till respektive skrivare med kraftigt saltade priser på tillhörande faktura. Returadresser saknades och telefonnumren för support och kontakt som angavs, var felaktiga.

I mitten av 00-talet började denna typ av försäljning bli vanlig rörande bla rengöringsmedel i större enheter om 10-20 litersdunkar. Undermåliga produkter som via telefonskojaremetoder säljs till kraftiga överpriser och i onaturligt stora enheter, omöjliga att returnera.

De senaste åren har denna modell återupptagits igen, men nu handlar det även om andra typer av kontorsmaterial som bland annat försäljning av mycket stora enheter av undermåliga kvittorullar. Kvittorullar som inte är tryckbeständiga och enligt SKL även innehåller förbjudna gifter.

16.15 SEO-SKOJARE / BLUFFAKTUROR

SEO, Search Engine Optimization (Sökmotoroptimering) och sökmotorregistrering är begrepp som handlar om att optimera hemsidor för att hittas och rankas bättre av sökmotorernas indexeringsmjukvara. En bra sökmotoroptimerad webbsida rankas högre vid sökning av aktuella och till webbsidan relaterade sökord och fraser.

Sökoptimering delas vanligtvis upp mellan ***onpage***, optimering av själva sidinnehållet, så att det passar indexeringen på bästa sätt) och ***offpage***, som handlar om ”yttre påverkan” genom att bla andra webbsidor länkar till den aktuella webbsidan som ska optimeras (*så kallade **inlänkar***).

Inom Sökmotoroptimeringen av webbsidor, så delas metoderna upp mellan **White Hat** (tillåten), **Grey Hat** (Osäker, men inte uttalat otillåten) och **Black Hat** (otillåten). Vad som är tillåten/otillåten optimering avgörs av de ledande sökmotorerna och för Svenskt vidkommande så är det uteslutande Google som avgör. Många metoder har genom åren övergetts då användandet riskerar att ”bannas” eller ”nollas” ur Googleresultaten. Istället används i mycket hög grad falska verksamhetssidor och SPAM-bloggar sk *sploggar* som skapas ämnesspecifikt med innehåll som är relaterade till kundernas verksamhet, med avsikt att manipulera sökresultaten och ge betalande kunder till ett sökoptimeringsföretag oförtjänad fördel gentemot sina konkurrenter.

Det är helt fel att säga att denna *manipulering* av sökresultaten är olaglig, för det är den inte – dock oetisk och något som majoriteten av Internetanvändare inte är medvetna om, att resultaten kan ha påverkats av den som köpt sig platsen.

Det är också **helt fel att säga att SEO-bolag är skojare**, för inom denna unga bransch finns extremt duktiga och seriösa *hantverkare* och specialister, till de som är mindre seriösa som riskerar mer med kundens webbsidor (med risken att straffas av Google för otillåten påverkan).

Men i denna bransch huserar sedan ett antal år tillbaka också rena skojarbolag, som kan lika mycket om SEO som grannens katt.

Men vad gör det när företagare, brottsbekämpning och Internetanvändare i allmänhet inte har den minsta kunskap om vad man köper, ofta under starka påtryckningar.

Med hjälp av säljmanus innehållande floskler, lösryckta påståenden och ”egen Googlesida”, 10 000 unika besökare till hemsidan, val av 10 sökord, synas längst fram i sökresultaten mm. så låter sig 9 av 10 småföretagare luras av totalt lurendrejeri som inte tillför verksamheten någonting mer än ytterligare en eller flera fakturor som brukar ligga i 10 tusen kronors-klassen.

Det finns till och med flera skojarbolag som påstår sig ringa från Google och att det uppringda företaget har legat med på Google under en gratisperiod, men att anledningen till samtalet är att det nu kostar pengar och att de därför kommer att skicka en faktura för de nästkommande 24 månaderna på 20 000 kronor.
När den uppringde vägrar och inte vill ha med det att göra, så erbjuds ofta (efter snabb konsultation med chefen) då ett avslutande avtal på 3 månader för 6 000 kronor som spelas in.

16.16 FALSKA VARNININGS- OCH SPÄRRTÄNSTER

Även om falska telefonspärrtjänster funnits sedan början av 2000-talet, så är det från början av 2007 som de blev en riktig plåga. Med inresta ungdomar som arbetskraft bedrevs falska telefonspärrar från Thailand via IP-telefoni. De drabbade företagarna hittades främst i Norge och Sverige. Då konkurrensen var stor mellan dessa falska spärrtjänster, så startades även falska varningstjänster som bland annat varnade för konkurrerande varningstjänster. Alla influerade av Svensk Handels varningslista. I dagsläget juni 2013 finns det ca 10-15 stycken av dessa falska varningstjänster som alla är aktiva och lurar företagare per telefon, ofta kombineras en massa floskler som PR-rådgivning, hantering av säljsamtal, inventering av marknadsföringsbehov mm – allt paketerat för att låta attraktivt för småföretagaren som inte får något levererat.

16.17 TROJANSPRIDNING VIA SOCIALA MEDIER FÖR BANKINTRÅNG MM.

En *trojan* (från trojansk häst) är en en typ av programvara som utger sig för att vara något annat än det egentligen är. Programvaran kan exempelvis gömma sig i en wordfil, en bild eller ett pdf-dokument. Men innehållet i programvaran (trojanen) är något helt annat än det ser ut att vara och kan bland mycket annat gömma **spionprogram (*spyware*)** som kan skicka din information till utomstående, ***keyloggers*** som spelar in varje tangentnedslag och även ***rootkit*** som kan ta

kommando över PC:n och utföra exempelvis banköverföringar i ditt namn.

Detta har visat sig vara vanligt mot exempelvis olika typer av **Bank-ID** kunder. Flera icke namngivna banker använder sig av en lösning som bygger på att bankkunden autentiserar sig dels genom en personlig PIN-kod och dels genom en på förhand autentiserad dator via https (säker avskärmad uppkoppling mot banken). Detta är en säker lösning som håller utomstående borta, så länge det är rätt person som utför transaktionerna. Men med ett rootkit installerat på datorn så får det precis motsatt effekt. Eftersom inkräktaren endera ”lyssnat av” PIN-koden och andra nödvändiga uppgifter, så kan denne utan problem lpgga in på bankkontot via den smittade datorn och utföra bänkärenden i den kapades namn, dator och PIN-kod.

Spridningen av dessa trojaner är speciellt vanlig i olika Facebookappar och ”falska gilla-knappar” på Facebook. Det är även vanligt med olika typer av priser att vinna, som tekniska prylar, pengar och resor – men som kräver att besökarna tar sig till en webbsida utanför Facebook, där själva trojansmittan sker.

Vid några uppmärksammade tillfällen har sådana härvor nystats upp, då ett 20-tal bankkunder fått påhälsning på ovan vis och till och med fått se sitt aktieinnehav sålt för att fylla på bankkontot med likvida medel som sedan skickats till kontomålvakters konton.

Det anmärkningsvärda med dessa offer är att samtliga drabbade har blivit av med minst 100 000 kronor från sitt bankkonto.
Då den summan sannolikt varit gränsen för när det är *värt att röja sig* och riskera att intrången uppdagas, så får det förmodas att ett mycket stort antal bankkonton innehåller mindre än 100 000 och som fått påhälsning och som kan komma att tömmas närhelst bedragaren så önskar.

16.18 ID-STÖLDER / ID-KAPNINGAR / FALSKA ID-HANDLINGAR

ID-stölder, ID-kapningar och falska ID-handlingar kan ske på väldigt många sätt och jag kommer endast att ta upp några av dessa.

Via Internet går det att enkelt ta reda på **en persons samtliga personnamn och personnummer**, inte minst om personen har eller haft någon typ av styrelseengagemang, då tillhandahålls kompletta uppgifter via statsmaktsregistret Bolagsverket.se för vem som helst att hämta.
Med dessa uppgifter och ett eget foto går det sedan för en knapp tusenlapp att beställa en falsk ID-handling som sedan kan användas för exempelvis att köpa produkter och abonnemang i butik. ID-korten är dessutom numera mycket välgjorda och det krävs misstänksam butikspersonal för att kunna urskilja falsk från äkta ID-handling.

Men det är också väldigt vanligt att exempelvis domännamn under .se, registreras av bedragare, som använder annan persons identitet som innehavaruppgifter. Dessa uppgifter är sedan juni 2013 inte heller sökbara för allmänheten, då Datainspektionen ålagt domänregistret .SE att dölja samtliga personuppgifter vid en kontaktsökning av ett domännamn.

Detta får till följd att en ovetande ID-kapad person först får kännedom om att han/hon står som innehavare för domännamnet när Polisen knackar på dörren eller när nästkommande års förnyelsefaktura skickas ut.

Det är ett mycket stort antal falskt registrerade domännamn som uppdagats de senaste åren. Även registreringar på välkända och folkvalda personer, inte minst under generiska toppdomäner som .com, .net, .info och .org.

Dessa brott sker ofta med hjälp av sk **CARDING** som innebär att bedragaren kommit över kortnummer och cvc-kod för kontokortsinnehavare i Nordamerika.
Då dessa kort inte valideras genom ”secure code-system”, så tar det upp till ett par veckor innan bedrägeriet och det falska kortköpet uppdagas.

En annan ganska vanlig typ av kapning är att med en falsk namnteckning genomföra en förändring av bolagsföreträdare i ett företag. Med lite grundläggande ***social engineering**** så går det även lätt att ta reda på vem som meddelat på exempelvis Facebook att han/hon reser utomlands (och då inte kan opponera sig mot förändringen under flera veckor), ungefär på samma sätt som inbrottstjuvar bevakar och uppdaterar sig om vilka bostäder som dessa semesterresande Facebookanvändare bor i och alltså går att göra inbrott i.

* ***Social engineering***, social ingenjörskonst, handlar om att utan (eller med begränsade) tekniska hjälpmedel försöka komma över information. Tekniken går ut på att vinna människors förtroende, spela på deras känslor och hjälpsamhet och utnyttja brister i säkerhetstänk eller karaktär. På många sätt påminner den sociala ingenjören om en klassisk bedragare, en specialist på att lura, manipulera och övertyga. ”*Genom fragment och mindre pusselbitar kartlägga hela hemligheter*”.

17 NYA TRENDER OCH NYA HOT

Ett domännamn behöver ha en ändelse, som **.se** är ändelsen (landskoden) för Sverige.
domännamn används för bland annat hemsidor och e-mailadresser.
Idag finns ca 240 sk ccTLDer (Landstoppdomäner).

.ac .ad .ae .af .ag .ai .al .am .ao .aq .ar .as .at .au .aw .ax .az .ba .bb .bd .be .bf .bg .bh .bi .bj .bm .bn .bo .br .bs .bt .bw .by .bz .ca .cc .cd .cf .cg .ch .ci .ck .cl .cm .cn .co .cr .cu .cv .cx .cy .cz .de .dj .dk .dm .do .dz .ec .ee .eg .er .es .et .eu .fi .fj .fk .fm .fo .fr .ga .gd .ge .gf .gg .gh .gi .gl .gm .gn .gp .gq .gr .gs .gt .gu .gw .gy .hk .hm .hn .hr .ht .hu .id .ie .il .im .in .io .iq .ir .is .it .je .jm .jo .jp .ke .kg .kh .ki .km .kn .kp .kr .kw .ky .kz .la .lb .lc .li .lk .lr .ls .lt .lu .lv .ly .ma .mc .md .me .mg .mh .mk .ml .mm .mn .mo .mp .mq .mr .ms .mt .mu .mv .mw .mx .my .mz .na .nc .ne .nf .ng .ni .nl .no .np .nr .nu .nz .om .pa .pe .pf .pg .ph .pk .pl .pm .pn .pr .ps .pt .pw .py .qa .re .ro .rs .ru .rw .sa .sb .sc .sd **.se** .sg .sh .si .sk .sl .sm .sn .so .sr .ss .st .sv .sy .sz .tc .td .tf .tg .th .tj .tk .tl .tm .tn .to .tr .tt .tv .tw .tz .ua .ug .uk .us .uy .uz .va .vc .ve .vg .vi .vn .vu .wf .ws .ye .za .zm .zw

Till det kommer sedan 21 gTLDer (generiska toppdomäner)
.aero .asia .biz .cat .com .coop .edu .gov .info .int .jobs .mil .mobi .museum .name .net .org .pro .tel .travel .xxx

Men med start hösten 2013 kommer nya generiska toppdomäner att introduceras och det handlar inte om 3, 30 eller 300 nya toppdomäner, utan **1 409** nya toppdomäner. Så det kommer att leda till oöverskådliga konsekvenser vad gäller riskspridning av bedrägliga webbsidor, trojanspridande e-mailadresser och inte minst domännamnsskojare. Det finns även flera ljusskygga aktörer som är applikanter för ett stort antal domäner och riskkapitalbolag som är applikant för flera hundra av toppdomänerna. Ingen kan idag förutse vilka konsekvenser detta kommer att skapa, men om svensk brottsbekämpning idag har svårigheter att söka och säkra bevis på och från Internet, så kommer det snart att bli mångfaldigt mycket svårare inom ett års tid.

Poliser behöver då kunna avgöra äkthet och söka information om e-mailadresser som ser ut så här:
aaa@aaa.aaa, kundservice@nordea.bank info@stadshuset.stockholm

Och webbsideadresser som ser ut så här:
http://laddaner.gratis http://www.facebook.like http://pirate.sale

På nästkommande sida visas samtliga unika toppdomäner som kommer att ligga i rotzonen och de flesta registreringsbara för vem som helst av mestadels kommersiella aktörer, som kommer att göra vad de kan för att på så kort tid som möjligt vinna så många kunder som möjligt.

I skuggan av denna ej tidigare skådad kommers, kommer bedrägerier att frodas och vara mycket svåra att spåra för den som inte besitter nödvändig kunskap.

Många toppdomäner kommer inte heller att lyckas, utan inom 1-2 års tid gå i konkurs eller byta ”ägare” och i det ingemanslandet kommer stora mängder med innehavaruppgifter att spridas till mindre seriösa aktörer.

Kort sagt, **de nya toppdomänerna kommer att förändra det Internet vi känner idag.**

De 1 409 nya generiska toppdomänerna:

.aaa .aarp .abarth .abb .abbott .abbvie .abc .able .abogado .abudhabi .academy .accenture .accountant .accountants .acer .aco .active .actor .adac .ads .adult .aeg .aetna .afamilycompany .afl .africa .africamagic .agakhan .agency .aig .aigo .airbus .airforce .airtel .akdn .alcon .alfaromeo .alibaba .alipay .allfinanz .allfinanzberater .allfinanzberatung .allstate .ally .alsace .alstom .amazon .americanexpress .americanfamily .amex .amfam .amica .amp .amsterdam .analytics .and .android .anquan .ansons .anthem .antivirus .anz .aol .apartments .app .apple .aquarelle .aquitaine .arab .aramco .archi .architect .are .army .art .arte .asda .associates .astrium .athleta .attorney .auction .audi .audible .audio .auspost .author .auto .autoinsurance .autos .avery .avianca .aws .axa .axis .azure .baby .baidu .banamex .bananarepublic .band .bank .banque .bar .barcelona .barclaycard .barclays .barefoot .bargains .baseball .basketball .bauhaus .bayern .bbb .bbc .bbt .bbva .bcg .bcn .beats .beauty .beer .beknown .bentley .berlin .best .bestbuy .bet .bharti .bible .bid .bike .bing .bingo .bio .black .blackfriday .blanco .blockbuster .blog .bloomberg .bloomingdales .blue .bms .bmw .bnl .bnpparibas .boats .boehringer .bofa .bom .bond .boo .book .booking .boots .bosch .bostik .boston .bot .boutique .box .bradesco .bridgestone .broadway .broker .brother .brussels .budapest .bugatti .buick .build .builders .business .buy .buzz .bway .bzh .cab .cadillac .cafe .cal .call .calvinklein .cam .camera .camp .canalplus .cancerresearch .canon .capetown .capital .capitalone .car .caravan .cards .care .career .careers .caremore .carinsurance .cars .cartier .casa .case .caseih .cash .cashbackbonus .casino .catalonia .catering .catholic .cba .cbn .cbre .cbs .ceb .center .ceo .cern .cfa .cfd .chanel .changiairport .channel .charity .chartis .chase .chat .chatr .cheap .chesapeake .chevrolet .chevy .chintai .chk .chloe .christmas .chrome .chrysler .church .cialis .cimb .cipriani .circle .cisco .citadel .citi .citic .city .cityeats .claims .cleaning .click .clinic .clinique .clothing .cloud .club .clubmed .coach .codes .coffee .college .cologne .comcast .commbank .community .company .compare .computer .comsec .condos .connectors .construction .consulting .contact .contractors .cooking .cookingchannel .cool .corp .corsica .country .coupon .coupons .courses .cpa .credit .creditcard .creditunion .cricket .crown .crs .cruise .cruises .csc .cuisinella .cymru .cyou .dabur .dad .dance .data .date .dating .datsun .day .dclk .dds .deal .dealer .deals .degree .delivery .dell .delmonte .deloitte .delta .democrat .dental .dentist .desi .design .deutschepost .dev .dhl .diamonds .diet .digikey .digital .direct .directory .discount .discover .dish .diy .dnb .dnp .docomo .docs .doctor .dodge .dog .doha .domains .doosan .dot .dotafrica .download .drive .dstv .dtv .dubai .duck .dunlop .duns .dupont .durban .dvag .dvr .dwg .earth .eat .eco .ecom .edeka .education .email .emerck .emerson .energy .engineer .engineering .enterprises .epost .epson .equipment .ericsson .erni .esq .est .estate .esurance .etisalat .eurovision .eus .events .everbank .exchange .expert .exposed .express .extraspace .fage .fail .fairwinds .faith .family .fan .fans .farm .farmers .fashion .fast .fedex .feedback .ferrari .ferrero .fiat .fidelity .fido .film .final .finance .financial .financialaid .finish .fire .firestone .firmdale .fish .fishing .fit .fitness .flickr .flights .flir .florist .flowers .fls .flsmidth .fly .foo .food .foodnetwork .football .ford .forex .forsale .forum .foundation .fox .free .fresenius .frl .frogans .frontdoor .frontier .ftr .fujitsu .fujixerox .fun .fund .furniture .futbol .fyi .gal .gallery .gallo .gallup .game .games .gap .garden .garnier .gay .gbiz .gcc .gdn .gea .gecompany .ged .gent .genting .george .ggee .gift .gifts .gives .giving .glade .glass .gle .glean .global .globalx .globo .gmail .gmbh .gmc .gmo .gmx .godaddy .gold .goldpoint .golf .goo .goodhands .goodyear .goog .google .gop .got .gotv .grainger .graphics .gratis .gree .green .gripe .grocery .group .guardian .guardianlife .guardianmedia .gucci .guge .guide .guitars .guru .hair .halal .hamburg .hangout .haus .hbo .hdfc .hdfcbank .health .healthcare .heart .heinz .help .helsinki .here .hermes .hgtv .hilton .hiphop .hisamitsu .hitachi .hiv .hkt .hockey .holdings .holiday .home .homedepot .homegoods .homes .homesense .honda .honeywell .horse .hospital .host .hosting .hot .hoteis .hotel .hoteles .hotels .hotmail .house .how .hsbc .htc .hughes .hyatt .hyundai .ibm .icbc .ice .icu .idn .ieee .ifm .iinet .ikano .imamat .imdb .immo .immobilien .inc .indians .industries .infiniti .infosys .infy .ing .ink .institute .insurance .insure .intel .international .intuit .investments .ipiranga .ira .irish .iselect .islam .ismaili .ist .istanbul .itau .itv .iveco .iwc .jaguar .java .jcb .jcp .jeep .jetzt .jewelry .jio .jlc .jll .jmp .jnj .joburg .jot .joy .jpmorgan .jpmorganchase .jprs .juegos .juniper .justforu .kaufen .kddi .kerastase .kerryhotels .kerrylogisitics .kerryproperties .ketchup .kfh .kia .kid .kids .kiehls .kim .kinder .kindle .kitchen .kiwi .koeln .komatsu .konami .kone .kosher .kpmg .kpn .krd .kred .ksb .kuokgroup .kyknet .kyoto .lacaixa .ladbrokes .lamborghini .lamer .lancaster .lancia .lancome .land .landrover .lanxess .lasalle .lat .latino .latrobe .law .lawyer .lds .lease .leclerc .lefrak .legal .lego .lexus .lgbt .liaison .lidl .life .lifeinsurance .lifestyle .lighting .like .lilly .limited .limo .lincoln .linde .link .lipsy .live .livestrong .living .lixil .llc .llp .loan .loans .locker .locus .loft .lol .london .loreal .lotte .lotto .love .lpl .lplfinancial .ltd .ltda .lundbeck .lupin .luxe .luxury .macys .madrid .maif .mail .maison .makeup .man .management .mango .map .market .marketing .markets .marriott .marshalls .maserati .matrix .mattel .maybelline .mba .mcd .mcdonalds .mckinsey .med .media .medical .meet .melbourne .meme .memorial .men .menu .meo .merck .merckmsd .metlife .miami .microsoft .mih .mii .mini .mint .mit .mitek .mitsubishi .mlb .mls .mma .mnet .mobile .mobily .moda .moe .moi .mom .monash .money .monster .montblanc .mopar .mormon .mortgage .moscow .moto .motorcycles .mov .movie .movistar .mozaic .mrmuscle .mrporter .msd .mtn .mtpc .mtr .multichoice .music .mutual .mutualfunds .mutuelle .mzansimagic .nab .nadex .nagoya .naspers .nationwide .natura .navy .nba .nec .netaporter .netbank .netflix .network .neustar .new .newholland .news .next .nextdirect .nexus .nfl .ngo .nhk .nico .nike .nikon .ninja .nissan .nissay .nokia northlandinsurance .northwesternmutual .norton .now .nowruz .nowtv .nra .nrw .ntt .nyc .obi .observer .off .office .okinawa .olayan .olayangroup .oldnavy .ollo .olympus .omega .one .ong .onl .online .onyourside .ooo .open .oracle .orange .organic .orientexpress .origins .osaka .otsuka .ott .overheidnl .ovh .page .pamperedchef .panasonic .panerai .paris .pars .partners .parts .party .passagens .patagonia .patch .pay .payu .pccw .persiangulf .pet .pets .pfizer .pharmacy .phd .philips .phone .photo .photography .photos .physio .piaget .pics .pictet .pictures .pid .pin .ping .pink .pioneer .piperlime .pitney .pizza .place .play .playstation .plumbing .plus .pnc .pohl .poker .politie .polo .porn .pramerica .praxi .press .prime .prod .productions .prof .progressive .promo .properties .property .protection .pru .prudential .pub .pwc .qpon .qtel .quebec .quest .qvc .racing .radio .raid .ram .read .realestate .realtor .realty .recipes .red .redken .redstone .redumbrella .rehab .reise .reisen .reit .reliance .ren .rent .rentals .repair .report .republican .rest .restaurant .retirement .review .reviews .rexroth .rich .richardli .ricoh .rightathome .ril .rio .rip .rmit .rocher .rocks .rockwool .rodeo .rogers .roma .room .rsvp .rugby .ruhr .run .rwe .ryukyu .saarland .safe .safety .safeway .sakura .sale .salon .samsclub .samsung .sandvik .sandvikcoromant .sanofi .sap .sapo .sapphire .sarl .sas .save .saxo .sbi .sbs .sca .scb .schaeffler .schmidt .scholarships .school .schule .schwarz .schwarzgroup .science .scjohnson .scor .scot .search .seat .secure .security .seek .select .sener .services .ses .seven .sew .sex .sexy .sfr .shangrila .sharp .shaw .shell .shia .shiksha .shoes .shop .shopping .shopyourway .shouji .show .showtime .shriram .silk .sina .singles .site .ski .skin .skolkovo .sky .skydrive .skype .sling .smart .smile .sncf .soccer .social .softbank .software .sohu .solar .solutions .song .sony .soy .spa .space .spiegel .sport .sports .spot .spreadbetting .srl .srt .stada .staples .star .starhub .statebank .statefarm .statoil .stc .stcgroup .stockholm .storage .store .stream .stroke .studio .study .style .sucks .supersport .supplies .supply .support .surf .surgery .suzuki .svr .swatch .swiftcover .swiss .sydney .symantec .systems .tab .taipei .talk .taobao .target .tata .tatamotors .tatar .tattoo .tax .taxi .tci .tdk .team .tech .technology .telecity .telefonica .temasek .tennis .terra .teva .thai .thd .theater .theatre .theguardian .thehartford .tiaa .tickets .tienda .tiffany .tips .tires .tirol .tjmaxx .tjx .tkmaxx .tmall .today .tokyo .tools .top .toray .toshiba .total .tour .tours .town .toyota .toys .trade .tradershotels .trading .training .transformers .translations .transunion .travelchannel .travelers .travelersinsurance .travelguard .trust .trv .tube .tui .tunes .tushu .tvs .ubank .ubs .uconnect .ultrabook .ummah .unicom .unicorn .university .uno .uol .ups .vacations .vana .vanguard .vanish .vegas .ventures .verisign .vermögensberater .vermögensberatung .versicherung .vet .viajes .video .vig .viking .villas .vin .vip .virgin .visa .vision .vista .vistaprint .viva .vivo .vlaanderen .vodka .volkswagen .volvo .vons .vote .voting .voto .voyage .vuelos .wales .walmart .walter .wang .wanggou .warman .watch .watches .weather .weatherchannel .web .webcam .weber .webjet .webs .website .wed .wedding .weibo .weir .whoswho .wien .wiki .williamhill .wilmar .win .windows .wine .winners .wme .wolterskluwer .woodside .work .works .world .wow .wtc .wtf .xbox .xerox .xfinity .xihuan .xin .xperia .xyz .yachts .yahoo .yamaxun .yandex .yellowpages .yodobashi .yoga .yokohama .you .youtube .yun .zappos .zara .zero .zip .zippo .zone .zuerich .zulu .дети .католик .ком .москва .онлайн .opr .рус .сайт .קום .ابوظبي .اتصالات .ارامكو .العليان .بازار .بيتك .شبكة .عرب .كاثوليك .كوم .كيوتل .موبايلي .موزايك .موقع .همراه .कॉम .नेट .संगठन .คอม .みんな .アマゾン .クラウド .グーグル .コム .ストア .セール .ファッション .ポイント .一号店 .世界 .中信 .中文网 .亚马逊 .企业 .佛山 .信息 .健康 .八卦 .公司 .公益 .商城 .商店 .商标 .嘉里 .嘉里大酒店 .在线 .大众汽车 .大拿 .天主教 .娱乐 .家電 .工行 .广东 .广州 .微博 .慈善 .我爱你 .手机 .手表 .招聘 .政务 .政府 .新闻 .时尚 .普利司通 .書籍 .机构 .机构体制 .欧莱雅 .淡马锡 .深圳 .游戏 .点看 .珠宝 .盛貿飯店 .盛贸饭店 .移动 .网址 .网店 .网站 .网络 .联通 .诺基亚 .谷歌 .购物 .通用电气公司 .通販 .集团 .電訊盈科 .飞利浦 .食品 .餐厅 .香格里拉.香港電訊 .點看 .닷넷 .닷컴.삼성

17.1 ID-SKYDD

Alltmedan Polisen meddelar att den snabbast växande brottsypen är ID-kapningar och brott till följd av falska ID-handlingar, så har seriösa verksamheter (exempelvis försäkringsbolag och kreditupplysningsföretag) börjat erbjuda tilläggstjänster till sitt ordinarie tjänsteutbud, som bla kallas just ”**ID-SKYDD”**. Problemet är att det inte är tal om något ID-skydd, utan en meddelandetjänst som via utskick meddelar kunden om att dennes identitet nyttjats på ett otillbörligt sätt.

Det faktum att seriösa verksamheter erbjuder dessa tjänster, gör det svårt för allmänheten att skilja på dessa och de flera oseriösa “ID-skyddstjänster” som sedan ca ½ år börjat etablera sig på Internet och som telefonsäljer sina lufttjänster mot konsumenter och företagare i Sverige. Det är samma personer bakom dessa lufttjänster, som var inblandade i SEO- och Internetkatalogskojeri för 1-3 år sedan.

17.2 STÖLDER AV SMARTA MOBILTELEFONER

En annan påtaglig trend i Sverige är stölder av smarta mobiltelefoner. Det är för tillfället känt att stöldligor från södra delar av Europa genomför stöldräder, där de stjäl smarta mobiltelefoner som sedan fraktas till andra europeiska länder.

Trots att telefonabbonemanget oftast snabbt kan spärras av de drabbade, så kan specialiserade kriminella utan problem ta sig förbi inloggning och tömma telefonen på webbcache, historik och privat information och även få tillgång till inloggning till nedladdade mobilappar, som exempelvis appar (programvaror) för mobil betalning. Därefter kan oönskade transaktioner ske med den stulna telefonens webbläsare/inbyggda dator.

Detta faktum är inte känt hos allmänheten som tror sig vara säker i och med att telefonabbonemenget spärrats. Det är bara en tidsfråga innan svenska bedragare adopterat detta tillvägagångssätt.

17.3 KUNGÖRELSER AV BOLAGSNAMN

Sedan 2011 har fenomenet ”***frontrunning***” kommit till Sverige för att stanna. Detta tillvägagångssätt är inte olagligt, även om det uppfattas som en utpressningsliknande situation för de drabbade, men trots lagligheten, så är det mycket oetiskt.
Konceptet går ut på att företrädelsevis de omnända bedrägliga grupperingarna, dagligen bevakar firmanamn som bolagsverket kungör och publicerar i olika flöden på Internet. Kort därefter registreras dessa firmanamn som domännamnsadresser av bedragare (för en eller ett par hundralappar), sedan inväntar de att firmainnehavaren kontaktar dem för att köpa domännamnet. Prislappen är då från 5 000 kronor och uppåt.
Detta förfarande sker i stor omfattning och det finns idag flera tusen domäner som registrerats för detta ändamål av 4-5 aktörer som är välkända genom flertal olika bedrägerimodus.

17.4 KLONER AV SERIÖSA WEBBSIDOR

Det blir mer och mer vanligt i så kallade transportbedrägerier att man ”rippar” dvs klonar och kopierar en befintlig verksamhets webbsideinnehåll och registrerar ett domännamn som är mycket likt orginaladressen som exempelvis där [transportbolaget.se] är orginaladressen, så registrera man istället [transport-bolaget.se] (med bindestreck) och laddar upp orginalinnehållet på adressen.

Sedan förändrar man betalnings- och kontaktinformation, men låter i övrigt sidan vara intakt.

Detta används med fördel vid köp&sälj-annonser av fordon, där en köpare ber säljaren anlita och betala till den falska transportfirman, vanligtvis efter att man skickat ett falskt kvitto på en initierad transaktion för slutbetalning av försäljningsobjektet (som även inkluderar en tor summa för transportkostnaden). Den klonade webbsidan används alltså i ett bedrägeriförstärkande syfte.

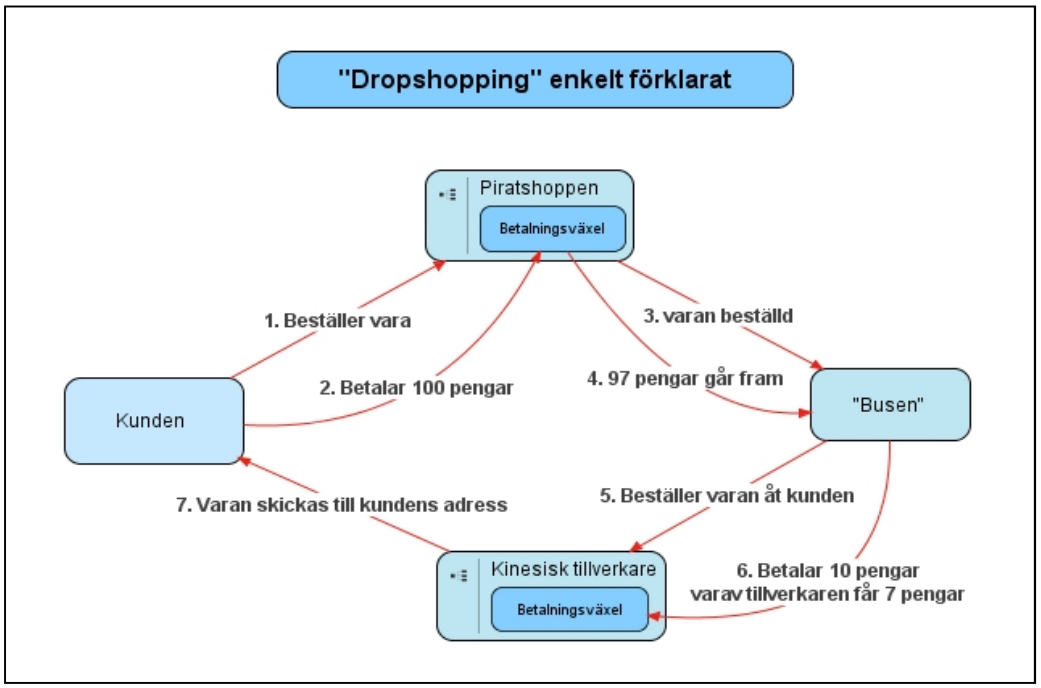
Klonade och väldigt snarlika webbsidor används annars i allehanda bedrägeriupplägg, med alltifrån försäljning av otillåtna läkemedel och doping- och narkotikaklassade substanser till förvillande lika varningssidor som etablerade verksamheters webbsidor, som företagare lätt låter sig luras av.
I exemplet visas Svensk Handels sida (vä) och bedragaren Svensk Varningslista (hö)

Svenska Internetanvändare luras också i stor omfattning av falska märkesklädessidor, där konsumenter luras att betala online för märkesprodukter.
Det är svårt att veta omfattning och ursprung av dessa sidor som är ca 250 stycken som är översatta till svenska och alltså inriktar sig mot svenskar.

I augusti 2012 åtalades 5 svenskar för grova bedrägerier och varumärkesbrott då de sålde piratkopierade märkeskläder över Internet för miljonbelopp, tingsrättsdomen ändrades i december 2012 av hovrätten till 2 års fängelse för huvudmannen i den härvan, som även innefattade cigarettsmuggling till Sverige samt försäljning av piratkopierade apple-produkter (iPad och iPhone).

Och det förekommer även att olika grupperingar fientligt konkurrerar med varandras verksamheter. Något som blir tydligt mellan nedan konkurrenter – observera ”N**UO**VO” och ”N**OU**VO”.

Det händer även att de fientliga kampanjerna leder till våld med dödlig utgång, som mordet på en företrädare i Phuket i augusti 2011, där två personer ur en konkurrerande verksamhet fortfarande sitter häktade för mord i Thailand. Samtliga inblandade har kopplingar till en mängd olika typer av ekonomisk brottslighet, bland annat bluffakturor och *Dropshipping*.*



Eftersom ”vem som helst” kan sätta upp en *piratshop* och utge sig för att vara någon annan, så är det osäkert hur många som har svensk inblandning, dock är det säkerställt med flera stora svenska piratsajter.

Enligt SACG, Swedish Anti-Counterfeiting Group omsätter förfalskningsindustrin årligen 600 miljarder dollar globalt.

18 REVISORER

Ett 10-tal revisorer återkommer ständigt i dessa grupperingar och det finns även enstaka revisorer som haft en osannolik otur i att välja sina klienter, då det visar sig att revisorn ansvarat för bolag ur 7-8 olika brottsliga grupperingar.

Det är även intressant att ett fåtal revisorer satts som revisor i bolaget vid registreringsskedet och trots att styrelsen helt bytts ut i tre omgångar, landsände och verksamhetsinriktning, så sitter revisorn kvar efter 4 års tid.

19 LAGERBOLAG OCH KONKURSHOTADE BOLAG

När ett aktiebolag skall användas för bedrägliga verksamheter, så används ofta så kallade ”lagerbolag”, som är färdigregistrerade och som köps för drygt 5000 kronor. Det som sedan krävs är styrelseledamöter, namn och adressändring på bolaget, för att sedan kunna ansöka om ett bankgiro. Därefter är man startklar för att bedriva verksamhet.

Men minst lika vanligt är att bedragarna annonserar och ”köper” tar över befintliga bolag (ofta med kommande skatteskulder eller där likvidationsplikt föreligger). Dessa bolag är extra intressanta i det fall det finns ett eller flera bankgironummer kopplade till bolaget, som bedragaren kan få omedelbar kontroll över.

Oftast ändras endast en del av uppgifterna som bolagsföreträdare och namn på bolaget, men låter exempelvis telefonnummer och adress vara intakta, varvid den tidigare innehavaren av bolaget blir misstänkliggjord och blir besvärad av klagomål och anmälningar när bedragarna sätter igång med sin verksamhet i bolaget.

20 BARTERAFFÄRER AV INAKTIVA BOLAG

Flertalet (främst) byggbolag i dessa sfärer tillämpar olika typer av barteraffärer där de byter fakturor med varandra (nollsummespel) för att på så sätt få stora transaktionsbelopp in i bokföringen och kunna uppvisa hög omsättning, som i ett senare skede kan lura såväl kreditgivare och investerare.

Även barteraffärer har skett med brittiska 1-pundbolag och 50 dollars *Delaware*-företag som värderats till fantasisummor, för att sedan gå in som delägare i svenska börsnoterade bolag, i utbyte mot de egna aktierna.

På så sätt och tillhörande pressreleaser har bedragarna i flera fall lyckats manipulera och ”haussa” aktiekurser för ett flertal svenska bolag som vid konkurs redovisat flera hundra miljoner till miljardförluster. Detta gäller även där en av de svenska AP-fonderna gått in med poster i 50-miljonersklassen. Det finns flertalet kopplingar mellan dessa bolag och övriga ekonomiska bedrägeriverksamheter.

21 FÖRÄDLING AV PENNINGFLÖDEN TILL FÖLJD AV BEDRÄGERIER

Bland de ”kringbolag” som hittas i de aktuella bolagsgrupperingarna runt de bluffakturerande bolagen hittas i synnerhet byggbolag, finansbolag, leasing- och factoringbolag.

I många fall är det även bygg- och factoringföretag som står som betalningsmottagare för bluffakturorna. Även bolag som handlar med och försäljer utsläppsrätter förekommer i flera grupperingar.

Vid avstämning av ett större antal relevanta byggbolag med Ekobrottsmyndigheten, så är flertalet av de aktuella byggbolagen föremål för utredningar kring systematiska fusk av sk ROT-avdrag.

Vid kartläggning av bolagsgrupperingar utifrån bla person- och adresskopplingar återkommer mönster som att var 6:e till 8:e bolag är ett bluffakturerande bolag, medan övriga bolag har andra verksamhetsområden, sannolikt avsedda för penningtvätt eller för investering och förädling av penningflöden.

De aktuella finansbolagen tillhandahåller ofta konsumentinriktade verksamheter som sk snabblån, SMS-lån eller handel med ädla metaller (uppköp av guld från allmänheten).
Medan de sk factoringbolagen mot procentuell avgift övertar bluffakturerande bolags fordringar.

22 LEASINGBOLAG

I ett antal fall förekommer utlandsregistrerade bolag som verkar som koncernmoder för ett stort antal svenska aktiebolag, där koncernmoderbolaget påstås ha miljardförluster från flygplans- och fartygsaffärer. Förlustavdragen utnyttjas sedan av de svenska dotterbolagen.

I dessa fall handlar det om att omvandla falska fordringar till annan affärsverksamhet, alltså en typ av penningtvätt.

I andra fall är det välkänt att kända ekonomiska bedragare (”produktspecialister” eller ”1-produktsspecialister”) vid sidan om är verksamma med att tillhandahålla beväpnad eskort för svenska fartyg i utländska vatten (uthyrning av brittiska och ukrainska legosoldater och egna krigsfartyg).

23 ”PUMP N´ DUMP”-VERKSAMHETER

Det finns ett utstuderat sätt för bedragare att lura svenska mediabolag. Sättet går ut på att registrera en verksamhets domännamn/hemsida på en privatperson och sedan beställa annonsering i all tänkbar media på mångmiljonbelopp, som helt kanaliseras till hemsidans bedrägliga produkter. När beställningarna är gjorda och marknadsföringen väl sker, så byter beställarbolaget först namn, för att sedan själv ansöka om konkurs. Kvar är då den privatregistrerade domänen/hemsidan som marknadsförts.
Under tiden så har ett annat företag tagits över och namnbytt för att passa hemsidans verksamhet och tillgodose sig den marknadsföring som det kursade bolaget beställt.

24 SVENSKA BOLAG VERKSAMMA MOT NORGE

Det finns i dagläget ett 30-tal svenska bolag som är verksamma med ett 50-tal verksamheter som är dedikerade mot norska företagare. Det är mycket omfattande och är mestadels 90-talets annonsskojeri, men avser mestadels publicering på Internetkataloger, men även påstådda kataloger. Norsk polis hänvisar till Økokrim, som inte utreder denna typ av bedrägerier. Detsamma gäller för svensk polis, som hänvisar till EBM, som inte utreder denna typ av bedrägerier. En intressant frågeställning är vem som bär ansvaret att utreda?

25 SVENSKA BLUFFVERKSAMHETER I UTLANDET

Det är vanligt att utförare (säljare) i bluffbolagen sitter i Thailand och ringer till svenska företagare via IP-telefoni (med svenska telefonnummer). Det förekommer även att försäljningskontor sätts upp i England, Danmark, Malta, Cypern och i Spanien.

I andra fall sätts juridiska personer upp i utlandet, men verksamheten sker från Sverige, medan betalning går endera via filialverksamheter i Sverige eller via utländska konton.

26 ANONYMA BREVBOXAR

Anonyma brevboxtjänster är ett gissel och något som mycket frekvent används av bedragarna. Det finns flera bolag som erbjuder dessa tjänster och bedragarna använder i synnerhet dessa boxar i Stockholm, Malmö, Helsingborg, Eskilstuna och Kalmar.

Den mest använda postboxtjänsten ligger i Stockholm och heter Brevia.

Brevia bildades på 80-talet av en person (CGT) som inte fälldes för att ha skickat bluffakturor för 40 miljoner kronor, utan för att han inte betalade 20 miljoner av dessa i skatt till svenska staten.

Verksamheten tas sedan över av en annan person (TÖ) som 2004 personligen upptaxeras av SKV med 30 miljoner kronor, och som sedan dess gömt sina verksamheter i kommanditbolagsstrukturer, där de är styrelseledamöter till varandra och (TÖ) endast är extern firmatecknare i brittiska Ltd-bolag.

Brevia-verksamheten flyttar då till (AQ) som driver Brevia idag, med koppling till HAMC och som dömts för grovt bedrägeri och bokföringsbrott och som senare även dömts för förfalskning av 700 000 frimärken (värde 3,1 miljoner) och förfalskade checkar (till ett värde på 12 miljoner kronor).

Totalt finns drygt 1 630 verksamheter registrerade med Brevias anonyma postboxar. Av dessa så bedömer jag att mellan 1200-1300 är förknippade med brottslig verksamhet. Det är mycket vanligt att 3-10 företag använder samma unika boxadress.

27 TELEFONBEDRAGARES LJUDINSPELNINGAR I RÄTTEN

Ett stort problem för drabbade företagare och konsumenter är att en telefonskojare endast behöver spela in själva avtalsbindningen i ett samtal.
Denna avtalsbindning har föregåtts av utpressningsliknande hotbilder och/eller löften om mycket fördelaktiga förhållanden, som aldrig varit avsedda att infrias.
I de fall ljudfilerna spelats upp vid rättsliga tvister, så har rätten i flesta fall godtagit den mycket korta avtalsbindningen och som oftast motsvarar 20 sekunder av ett 5-10 minuters samtal.
Detta faktum spelar bedragarna helt i händerna.

28 SKATTEBROTTSENHETER, SKATTEVERKET

Flera skattebrottsenheter har 2011-2013 meddelat att de endast utreder misstänkta skattebrott som överstiger 500 000 kronor, vilket gör att stort antal bolag avsedda för penningtvätt aldrig kommer upp till ytan, då de ofta systematiskt går i konkurs med skulder i spannet 350 000 – 450 000 kronor. Detta ger helt fel signaler från samhället.

29 DATAINSPEKTIONEN – INKASSOTILLSTÅND / PUL

Datainspektionen är tillstångsgivare och tillsynsmyndighet för inkassoverksamheter i Sverige. Datainspektionen uppvisar allvarliga brister i deras hantering av utgivning och tidigare utgivna inkassotillstånd.

Ett inkassotillstånd ges vanligtvis på 5 års perioder (max 10 år), men under vissa omständigheter, vid osäkerhet från myndigheten ges **prövotillstånd med 1 års giltighet**. Vilket är mer än tillräckligt för bedragares avsikt att nyttja inkassobolagets påtryckning för betalning.

DI:s tillståndshandläggare och jurister har löpande under de senaste åren uppdaterats kring att seriösa inkassobolag driver in avtalslösa fordringar, samt att flertalet inkassobolag med DI:s inkassotillstånd själva är konstaterade bedragare (samma bolagsföreträdare och kontaktuppfifter som bluffakturerandebolagen).

Stora brister i tillsyn och uppföljning av inkassobolag
I skrivande stund redovisar Datainspektionen gällande tillstånd på webbadressen: (http://www.datainspektionen.se/lagar-och-regler/inkassolagen/gallande-inkassotillstand/) där flertalet bolag är försatta i konkurs, likviderade eller har likvidationsbeslut, är avregistrerade, eller saknar styrelse och firmatecknare, eller har allvariga revisorskommentarer som olaga lån, brister i den interna kontrollen, eller har restförda skatter/avgifter.

Dessutom får det anses bekymmersamt att Datainspektionen som tillika är tillsynsmyndighet för PuL, Personuppgiftslagen (1998:204) har ålagt domännamnsregistret .SE att helt anonymisera personnamn för privatpersoner och enskilda firmor som är domännamnsinnehavare under .se, så att dessa innehavare inte längre är synliga som innehavare av en domänadress under .se. Och detta med referens till just Personuppgiftslagen.

Vissa stora, centrala myndighetsregister är beslutade av regering eller riksdag och benämns statsmaktsregister. Många av dessa statsmaktsregister regleras av särskilda registerlagar och/eller författningar som finns publicerade i Svensk Författningssamling (SFS) och undantas Personuppgiftslagen (PuL). Datainspektionens register över inkassotillstånd är inte särskilt upptagen såsom statsmaktsregister, och lyder därmed under Personuppgiftslagen.

I Datainspektionens eget register över aktuella inkassotillstånd på tidigare angiven URL, så listar de själva personnamn och namn på enskilda firmor som innehar tillstånd att bedriva inkassoverksamhet.

30 ARBETSFÖRMEDLINGEN – PLATSBANKEN

Arbetsförmedlingen utför ingen kontroll av vilka företag som annonserar efter personal.
Detta leder till att bedragare vanligen rekryterar ungdomar som telefonsäljare genom Arbetsförmedlingens Internettjänst Platsbanken.

I skrivande stund så hittar jag 4 stycken platsannonser från bluffakturerande bolag på de 2 första sidorna (senast inkomna) när jag söker i kategorierna ”säljare i Malmö”.

Dessutom brukar dessa verksamheter söka personal och ibland skenanställa i passiva ”målvaktsbolag”, för att säljare sedan är verksamma i och för de aktuella bluffbolagen.

Det finns flera exempel på där ungdomar blivit ”tvingade” av Arbetsförmedlingens handläggare att söka dessa tjänster, då de annars riskera att förlora sin dagsersättning. Det finns även exempel på att samma dittvingade ungdomar blivit lurade på både lön och intyg.

Detta har påtalats för Arbetsförmedlingen under flertalet år, men representanter för Arbetsförmedlingen uttalar att de uppfyller sitt uppdrag och inte har vilja eller kapacitet att granska annonsörer av lediga jobb.

Det förekommer till och med att bluffbolag i Thailand annonserar efter säljare genom platsbanken och får ungdomar att sätta sig på ett flygplan med löften om bra löner och billigt boende.
Dock har verkligheten visat sig vara en helt annan för dessa ungdomar, som behövt låna pengar av närstående för att kunna ta sig tillbaka till Sverige igen, med arbetslivserfarenheter som de skäms över och helst vill glömma.

31 LOTTERIINSPEKTIONEN

Vid anmälan av Waplotto/Euromillions som i mitten av 2010 skickade ut tiotusentals SMS-krav till privatpersoners mobiltelefoner, med uppmaning att klicka på en länk. De konsumenter som klickar på länken sätter igång en prenumeration för påstådda köp av lotter i Euromillions lottery för 400 kronor i veckan och prenumerationen avser 4 veckor (1600 kronor).
Påstådd avsändare till SMS:en är ett bolag registrerat på brittiska jungfruöarna, men med en postbox i Malmö. Fakturerande bolag var ett svenskt aktiebolag från Malmö.

Det europeiska lotteriet Euromillions Lottery som administreras av belgiska *Nationale Loterij* meddelar att det inte fanns några som helst kopplingar mellan det riktiga lotteriet och Waplotto.

Polisen kunde inte utreda, Konsumentverket varnade ett par tillfällen, men Lotteriinspektionen lät genom sin Pressansvarige meddela att eftersom **Waplotto/EuroMillions inte är baserat här i landet så är det inte så mycket Lotteriinspektionen kan göra**.
- Detta trots att den enda kända adressen för avsändaren är en postbox i Malmö och samtliga inbetalda pengar gått genom ett svenskt aktiebolag i Malmö, som av en händelse har samma koncernmoder (Erika Plus 4 LTD) som Svenska Let To Phone haft, (LTP som var betalningsmottagare för de 1,7 miljarder kronorna som modemkapningen gav under två år).
Källa: http://www.allabolag.se/5565601092/Svenska_Let_To_Phone_AB

Lotteriinspektionens uppdrag är helt verkningslöst pga Internet, då det dagligen sätts upp nya lotterier via Internet inriktade mot svenskar genom bland annat Facebook, men då avsändare påstås vara utlandsregistrerat bolag, så har Lotteriinspektionen inte mandat att ens ha en åsikt. Detta leder självklart till att bedragare som Waplotto växer fram, som bara genom att påstå att bedrägeriet är ett utländskt lotteri går fria från all myndighetsinsyn. En besvärande signal från samhället.

32 BOLAGSVERKET, BRISTANDE KONTROLL

Idag sker ingen kontroll av styrelseföreträdare, något som i synnerhet bolag med brottsliga avsikter systematiskt utnyttjar. Såväl vad gäller ID-kapade personer som hamnar i olika bolagsstyrelser utan sin vetskap, som betalda bolagsmålvakter med exempel på utslagna personer med 40+ konkurser bakom sig, men som aldrig blivit dömda ens till näringsförbud och kan fortsätta att erbjuda sig som slutmålvakt för brottslingars bolag, som oftast har miljontals kronor i skulder.

33 KRONOFOGDEMYNDIGHETEN, BRISTANDE KONTROLL

I februari 2012 så var 1 049 personer belagda med näringsförbud efter grov ekonomisk brottslighet. Men många av dem fortsätter att göra affärer och att begå nya brott.
Vi samma tidpunkt fanns 216 personer med näringsförbud fortfarande med i Bolagsverkets näringslivsregister. Dessa personer har koppling till 279 olika bolag.

Kronofogden är den myndighet som har i uppgift att kontrollera att näringsförbudet följs, men menar att myndigheten varken har tillräckligt med resurser eller verktyg för att sköta kontrollen på ett tillfredsställande sätt, så uppgiften är relativt verkningslöst.

Källor: http://www.mynewsdesk.com/se/view/pressrelease/baettre-skydd-mot-foeretagare-med-naeringsfoerbud-738230
http://www.kronofogden.se/Naringsforbud.html

34 BRANSCHORGANISATIONER OCH PRIVATA INITIATIV

I kampen mot Internetrelaterade bedrägerier, i synnerhet mot bluffakturor finns en rad initiativ utanför svenska myndigheter.

34.1 Svensk Handels varningslista

Sedan många år tillbaka har Svensk Handel tillhandahållit en varningslista över de företag som genererat flest inkomna klagomål och anmälningar till organisationen. Den svenska polisen refererar ofta till Svensk Handels varningslista som det närmast myndighetsliknande vi har i Sverige.

Svensk Handel publicerar varningar som namnger företag, adresser, organisationsnummer och gironummer mm.
Svensk Handels varningslista är referens till de större kreditupplysningsföretagen i Sverige, som ”spärrar” kreditanmärkningar för kunder till dessa bluffakturerande bolag.

Svensk Handel är en medlemsorganisation med ca 12 000 medlemsföretag, varningslistan är publik, men för rättslig hjälp behövs medlemskap för den drabbade näringsidkaren. Ett medlemskap kostar en näringsidkare från 4 100 kronor ex. moms.
Trots att listan är den mest välkända i Sverige och som många refererar till, så framgår endast i undantagsfall skälet till varningen, dvs vad för typ av bedrägeriförsök varningen avser.
Det förekommer även att felaktiga organisationsnummer publiceras, vilket leder till att felaktiga varningar för seriösa verksamheter publiceras, felaktiga bankgironummer som leder till att kreditupplysningsföretagens ”spärrar” inte är är korrekta.

34.2 Företagarorganisationen Företagarna

Företagarna är Sveriges största företagarorganisation med ca 70 000 medlemmar.
Organisationen har tråkigt nog lyst med sin totala frånvaro i arbetet mot bedrägerier och bluffakturor under 10 års tid. Först 2012 träder de in i debatten och hävdar då oförtjänt att de är initiativtagare till samverkansgrupper bla genom TV-reklam och pressreleaser på ett beklagligt sätt.
För att en drabbad företagare ska kunna tillgagna sig juridisk hjälp från Företagarna, så krävs medlemskap. Medlemskapet kostar 1 490 kronor ex moms för nystartat bolag och 3 950 kronor ex. moms efter år 1.

34.3 Varningsinfo i Sverige AB

Varningsinfo Sverige AB är ett privat initiativ och drivs av Svensk Handels tidigare säkerhetschef Dick Malmlund, som tillhandahåller en varningslista, som endast riktar sig till betalande medlemmar.
Dick bloggar även publika varningar med jämna mellanrum. Varningslistan är mer omfattande och mer komplett än den Svensk Handel tillhandahåller. För tillgång till varningslistan och juridisk hjälp krävs medlemskap som kostar 3 950 kronor ex. moms.

34.4 Förenade Bolag AB

Förenade Bolag AB är ett privat initiativ som tillhandahåller en publik mycket omfattande och beskrivande varningslista med automatisk uppdatering av förändringar av bolagen och verksamheterna på varningslistan. Även relationer mellan olika publicerade varningar, som när ett bolag förekommer med flera olika bluffakturautskick. För att få juridisk hjälp krävs medlemskap som kostar från 2028 kronor ex. moms.

34.5 KNYT.SE

Knyt.se drivs av konsumentjournalisten Anders Nyman som löpande postar andras varningar och även publicerar kartläggningar och artiklar själv. Anders bevakar även media, och taggar sina notiser med bla modus, ex "id-stöld". Knyt.se innehåller även en forumdel, där medlemmar kan posta egna varningar och kommentera andras. Anders Nyman är författare till .SE:s Internetguide ”Skydda ditt företag mot bedragare”. Knyt.se är kostnadsfri att ta del av.

34.6 VARNINGSKOLLEN.SE OCH INTERNETSWEDEN.SE

Varningskollen.se är en informationssida avsedd att förstärka bedrägerirelaterade varningar och nyheter. Internetsweden.se är en blogg där mer djupgående kartläggningar och varningar publiceras. Båda dessa webbsidor drivs av författaren till den här rapporten och är kostnadsfria att ta del av.

34.7 10-15 AKTIVA OSERIÖSA VARNINGSTJÄNSTER

Det finns vid sidan av ovan webbsidor även andra lovvärda initiativ som exempelvis tidningen Driva-Eget som skriver om bluffakturor i varje nummer av tidningen. Men det finns mellan 10-15 aktiva varningstjänster, som i flesta har en direkt relation till bedragare. Ofta ger de uttryck för att vara relaterade till någon av ovan sidor som ”i samarbete med Svensk Handel” eller ha en mycket snarlik webbsida, ofta med ”lånade” texter och bilder från andras varningar. Det är många kunder som luras att tro att de ingår avtal med Svensk Handel, när de i själva verket gjort det med Svensk Företagshandel..

34.8 NATIONELL VARNINGSLISTA

Med lite olika brister hos befintliga listor blandat med den förvirring och okunskap som råder inom denna avgränsade verksamhet, gör det närmast omöjligt för företagare att känna våga lita på varningar och många låter sig luras att betala för blufftjänster.

Från myndighetshåll har det aldrig tillhandahållits en varningslista av detta slag, trots att en myndighetsövergripande nationell varningslista är ett självklart samhällsansvar, som staten inte bör förvisa till kommersiella aktörer eller branschorganisationer som får ta oproportionerligt stort samhällsansvar, alltmedan myndigheter duckar för utmaningen.

35 POLISENS PROAKTIVA OCH BROTTSFÖREBYGGANDE VERKSAMHET

Sedan ett flertal år, så bedriver flera polismyndigheter brottsförebyggande verksamhet, varav Stockholmspolisens insatser varit mest synlig, inte minst genom deras medverkan till varningar och artiklar i massmedia, men även via exempelvis Facebookgruppen Polisen Bedrägeri
https://www.facebook.com/pages/Polisen-Bedrägeri/546406245370971
Arbetet som utförs är viktigt och föredömligt, då det ofta ges exempel på bedragares tillvägagångssätt. Men problemet är att Facebookgruppen får alldeles för liten spridning och de som verkligen befinner sig i riskgruppen för olika bedrägerityper, nås sällan av polisens varningar genom denna kanal. Ett annat gott initiativ från Stockholmspolisen är ett 5-sidors .pdf-dokument som kan läsas eller laddas ner från [bestrid.nu], och som utformats i samverkan med andra aktörer, bland annat Företagarna, Svensk Handel och Kronofogdemyndigheten. Dokumentet innehåller alla de olika steg som behövs för att bestrida och anmäla en bluffaktura.

35.1 NBC, NATIONELLT BEDRÄGERICENTER

Som en lösning på den rusande mängden bedrägerianmälningar, så går Rikspolischefen i januari 2013 ut i media och lovar rekrytering av 5-6 stycken civila bedrägeriexperter till en ny planerad satsning ***NBC, Nationellt Bedrägericenter***, med start hösten 2013 i Stockholm.
När dimman lättat är 3-4 analytiker anställda med lönenivå motsvarande 2/3 av medellönen för en analytikertjänst i Stockholm. En signal av **total oförståelse** från polisledningens håll, för den mest ökande brottsligheten i Sverige, när 3 miljoner allokeras denna verksamhet av polisens totala anslag på **20, 536 miljarder för 2013**. NBC ska verka som nationell uppsamlande enhet för bedrägerianmälningar med tre fokus: ***Brottsförebyggande insatser, Metodutveckling*** och ***Polisoperativt arbete***. Efter uppsamlandet ska anmälningarna ”skyfflas” ut för brottsutredning, sk brottsforum, lokalt ute i landet.

NBC:s 3 fokusområden leder **inte** till att bromsa antalet bedrägerianmälningar, som ökat med 28% under första kvartalet 2013. De leder **inte** heller till en högre uppklaringsgrad.

Poliskåren saknar, mer än i undantagsfall, den förståelse, kompetens och de resurser som krävs för att bekämpa den Internetrelaterade organiserade ekobrottsligheten. **Personuppklaringsgraden för bluffakturaanmälningar ligger de senaste åren på 1-2%**

Det krävs ett nytt sätt att arbeta för att kartlägga och utreda vilka personer som döljer sig **bakom** fasaden av brott, organiserar och tillägnar sig alla "brottspengar". ***Denna typ av brottslighet anmäls inte utan måste spanas fram och kartläggas.***

Det fjärde fokusområdet som NBC, eller annan myndighetsinstans behöver inrätta, är nödvändig och helt avgörande för att lyckas bromsa och vända trenden för den eskalerande ekonomiska seriebrottsligheten. Och det är ”**Spaning och kartläggning**”.

Det är helt avgörande att kompetens för denna resurs sker genom rekrytering av erfarna och målinriktade bedrägeriexperter, från privat sektor och från andra myndigheter.

36 FÖRSLAG TILL ÅTGÄRDER

36.1 GENERELLT UTBILDNING

- Det bör ligga högt på agendan att snarast tillgodose att samtliga bedrägeriutredande poliser får tillgodose sig en grundläggande utbildning kring hur Internet fungerar och hur det går att söka och säkra information på Internet. Därtill även utbildning kring hur bedragarnas nätverk ser ut, hur bolagsstukturer och målvaktsgenerationer för större förståelse och identifiering av desamma.
- Lika viktigt är att åklagare och domarkåren får ta del av ovan utbildning, för att få förståelse för bedrägerier över Internet.

36.2 GENERELLT INFORMATION

- Svenska myndigheter bör å det snaraste skapa en myndighetsövergripande varningstjänst för såväl konsumenter som näringsidkare. Dessutom innehållande FI:s befintliga varningar över investeringsbedrägerier.

- Svenska myndigheter bör via Public Service Televisionen varna för tillvägagångssätt i exempelvis ”*Anslagstavlan*”, för att nå ut till den målgrupp som är i mest behov av varningarna och inte letar efter dem själva, utan riskerar att låta sig luras. Även bulletiner om samhällsfarliga hot bör kunna användas på detta sätt, såsom ”*stora DDOS-attacker mot banker*” eller ”*stora phishingattacker i Telias namn*”.

36.3 GENERELL SAMVERKAN

- Brottsbekämpande myndigheter måste långsiktigt, och inte endast i projektform, samverka kring länsöverskridande brottslighet. Det måste skapas samsyn om vad som är seriell brottslighet och vem som skall bära ansvar för utredning. Det får inte finnas tillvägagångssätt som faller mellan myndigheter.

36.4 OPERATIVA FÖRSLAG

- Det absolut viktigaste NBC, Nationellt Bedrägericenter eller annan myndighet har framför sig är att skapa en spanings- och kartläggningsgrupp för den Internetrelaterade organiserade ekobrottsligheten i Sverige. Denna satsning måste vara **permanent** och tillåtas vara kostsam, då civila experter och kostsamma rekryteringar från andra myndigheter kommer att krävas. Att rekrytera och behålla hög kompetens kostar pengar men ger resultat. Att rekrytera juniora analytiker är varken lösning på problem och identifierat behov, utan leder endast till en fortsatt eskalering av ett redan enormt problem.

- Spanings- och kartläggningsgruppen behöver ha löpande avstämning med SKV, EBM, berörda polismyndigheter och inte minst åklagarmyndigheten.

37 AVSLUTNING

Jag har sedan 2002 bevakat och sedan 2004 varnat för bedragare och oseriösa aktörer. Sedan 2007 har jag haft ständig kontakt med brottsbekämpningen och bidragit till utredningar och kartläggningar av verksamheter och grupperingar. Under åren har jag haft kontakt med utredare från de flesta delar av Sverige och gemensamt är att de känner uppgivenhet över när de ”slår ner” på en bluffverksamhet idag, så dyker den bara upp på annan ort och under snarlikt domännamn imorgon.

Men jag ska ärligt säga att min bild av polisens generella IT- och Internetkunskap är att den är mycket dålig.

Inte sämre än allmänhetens Internetkunskap i stort. Men av den enkla anledningen att poliser precis som de allra flesta användare av Internettjänster **konsumerar** Internet och inte förstår vad som sker ”under huven”. En ”vanlig” Internetanvändare kommer vanligtvis ihåg och återkommer till ett 20-tal webbsideadresser – fler är det inte, utom i undantagsfall.

Därför låter sig allmänheten luras av de enklaste bluffar och därför kommer inte polisen på egen hand kunna lösa den Internetrelaterade mängdbrottsligheten, för de ser inte ens ”stenarna” som går att lyfta på.

Internet är det största som hänt vår generation och är en fantastisk tillgång på många sätt, men det är också en spegelbild av vårt samhälle i övrigt på gott och ont. Samhällets integrering med Internets olika tjänster innebär då också att brottsbekämpningen måste finnas och verka förtroendeingivande där medborgarna finns och utsätts för brott, såväl genom en (1) myndighetsövergripande webbadress för varningar, men även för att beivra begångna brott.

Men den svenska brottsbekämpningen är sedan länge *omsprungen* och *varvad* av de kriminella som haft Internet som lekstuga under 10-15 års tid.

Det är inte ens en obalans som går att utbilda bort längre, då polisen är hjälplöst efter. Polisen **måste** ta hjälp genom rekrytering av *civilister* med motsvarande eller mer kunskap och erfarenhet än den de kriminella besitter. Först då kommer brottsbekämpningen lyckas bromsa trenderna och få den brottsbekämpning som svenska medborgare ska kunna förvänta sig.

Svensk brottsbekämpning måste anpassas för dagens och morgondagens brottslighet.

Peter Forsman i Stockholm juni 2013