



Polisen

Bedrägerier och annat otyg

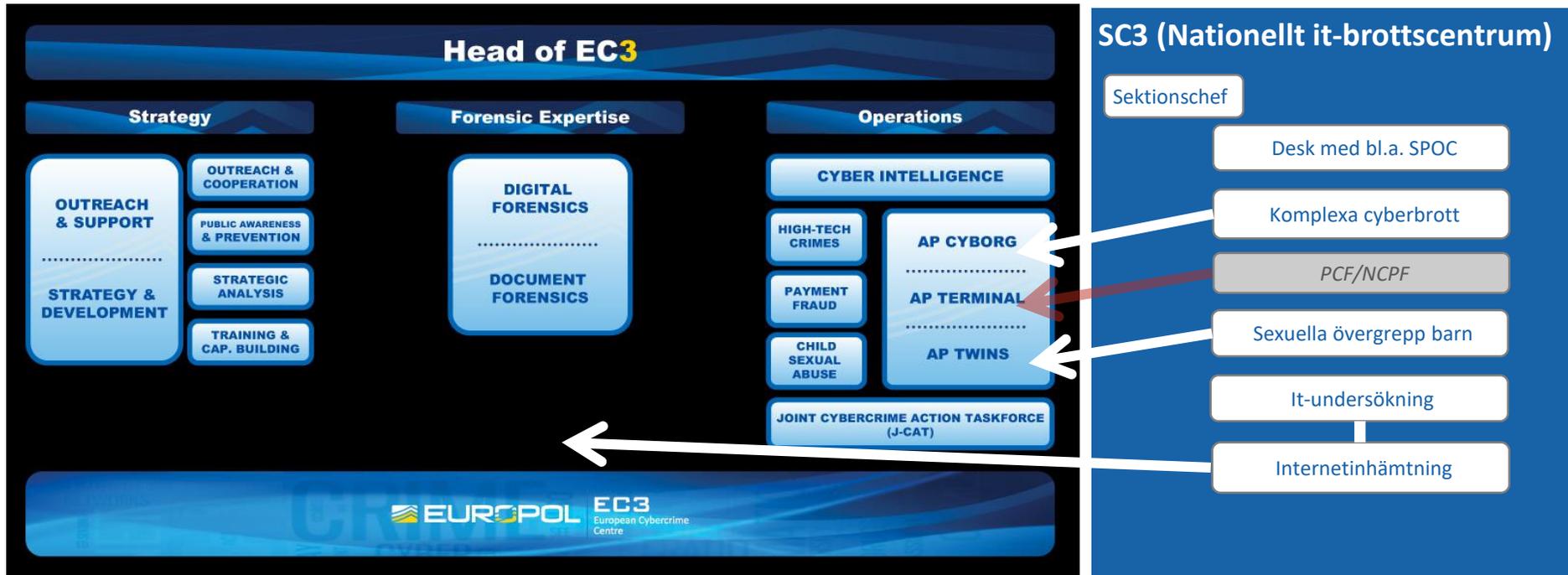
Nationellt IT-Brottscentrum, NOA IT

Swedish Cybercrime Center, SC3

Jan Olsson, KriminalKommissarie



Europols EC3



Sverige speglar EC3 med ett SC3 (Swedish Cybercrime Centre)
RC3 speglar SC3

Bedrägerier – är det ett problem?

Inga svenska beräkningar men:

- Annual Fraud Indicator 2017

The United Kingdom Fraud Costs Measurement Committee
(UKFCMC)

2.069.898.000.000 SEK

(190 miljarder pund 2017)

Motsvarar 31.534 SEK per capita

(65.640.000 invånare)

Går den att översätta?

- En inte alltför vetenskaplig jämförelse, men.....
 - Samma förutsättningar vad gäller datortäthet
 - antal Internetuppkopplingar per capita
 - E-handelsbenägenhet
- Brottbenägenhet/naivitet ?
- Sverige 10 120 242 invånare (december 2017)

319.131.711.228 SEK

(319 miljarder kronor per år)

Vad motsvarar summan ?

- ca 7% av BNP (2017)
- 7 x mer än hela rättsväsendets anslag (2017)
- 10.112 kr/sekund

Ur en samhällsekonomisk synpunkt !!!

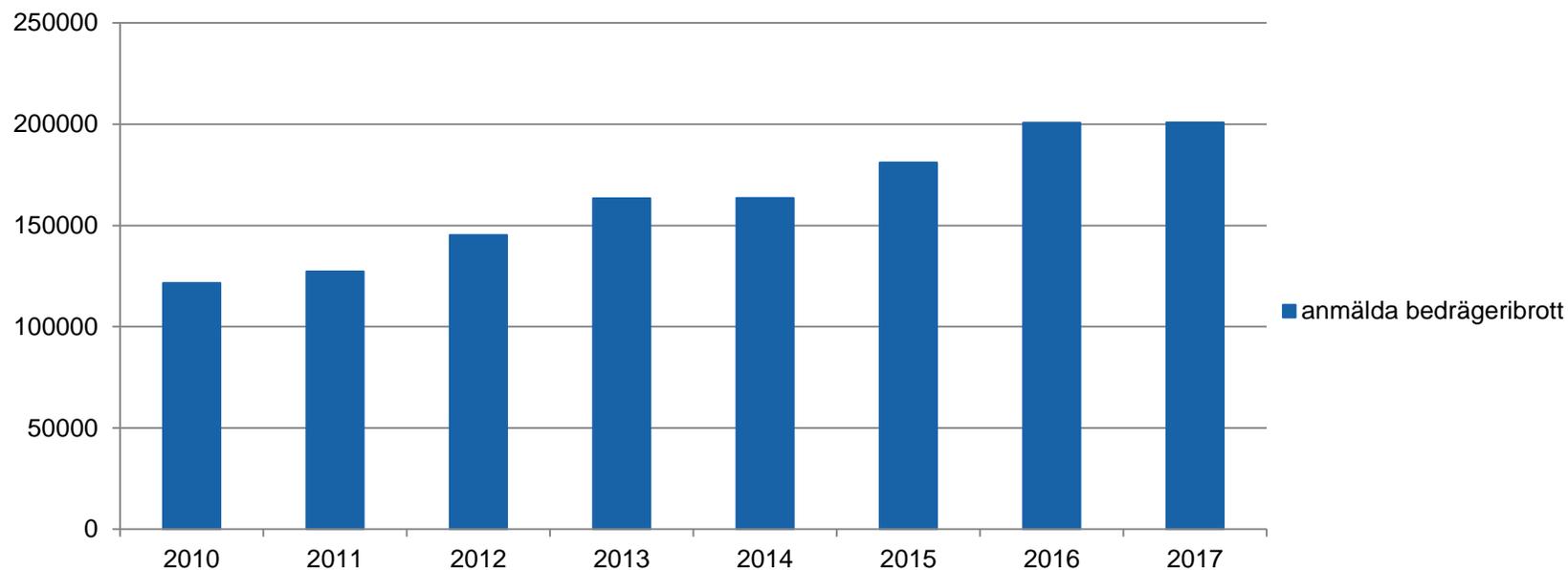
(Google)

Globala kostnader

55.000.000.000.000 Sek = kostnader för dataintrång globalt (Nordea Bank)

38.000.000.000.000 Sek = kostnader för bedrägerier globalt (Infosecurity)

Anmälda bedrägeribrott



2010	2011	2012	2013	2014	2015	2016	2017
121 640	127 244	145 327	163 361	163 550	181 135	200 751	200 913

Card not present, CNP

Stay secure when buying online

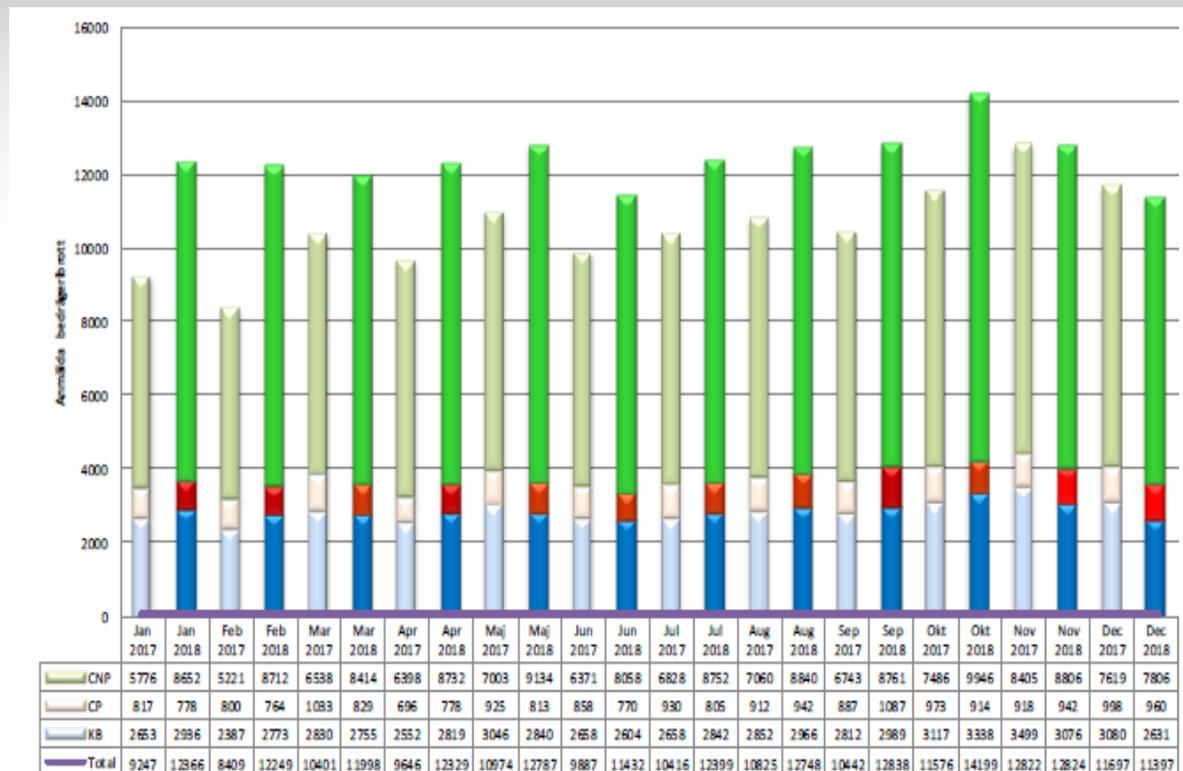


3D Secure

Verified by
VISA

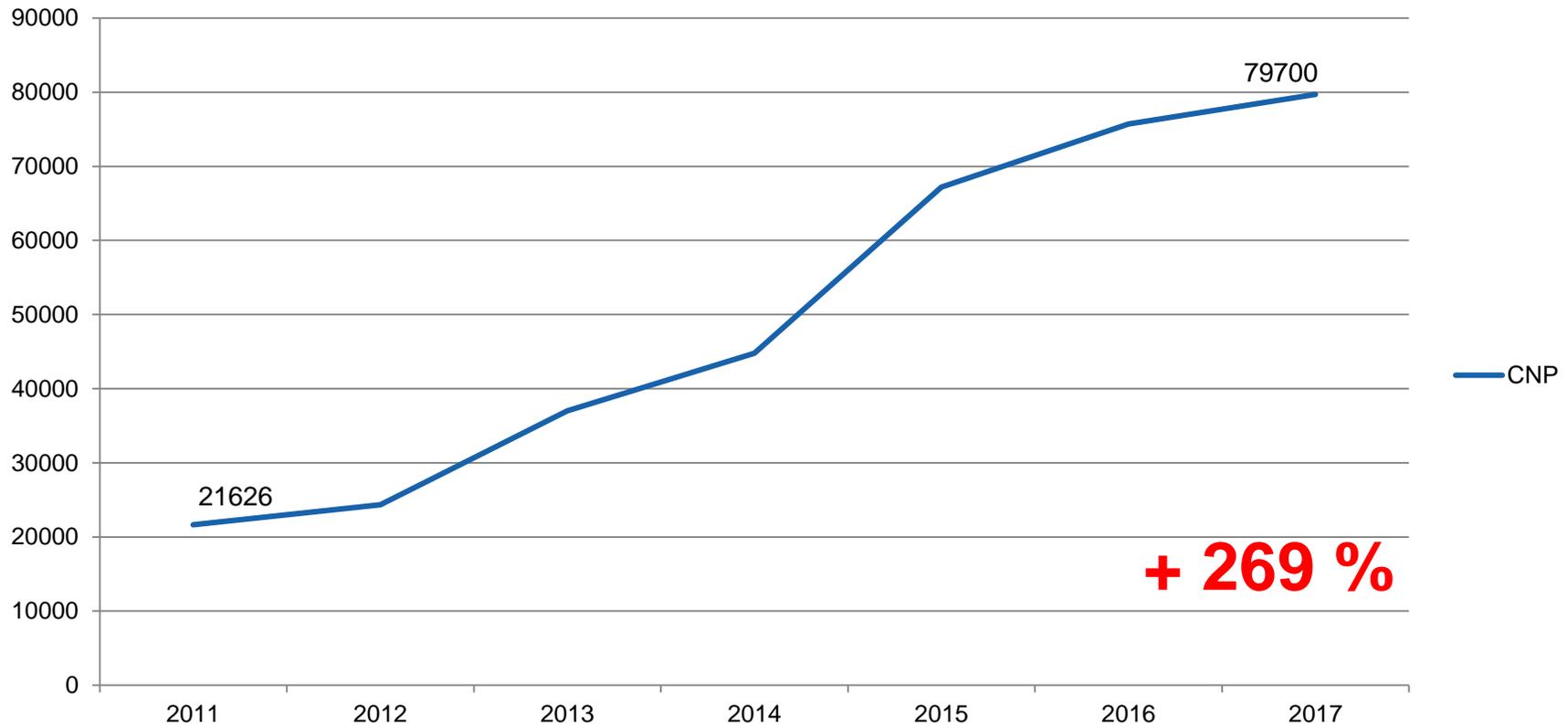
MasterCard.
SecureCode.

105.000 anmälda cnp 2018



28% ökning mot 2017

Anmälda Card not present, CNP

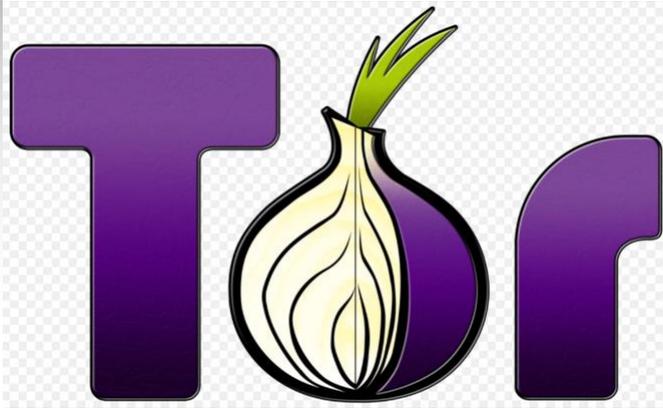


Kortinformationen ?

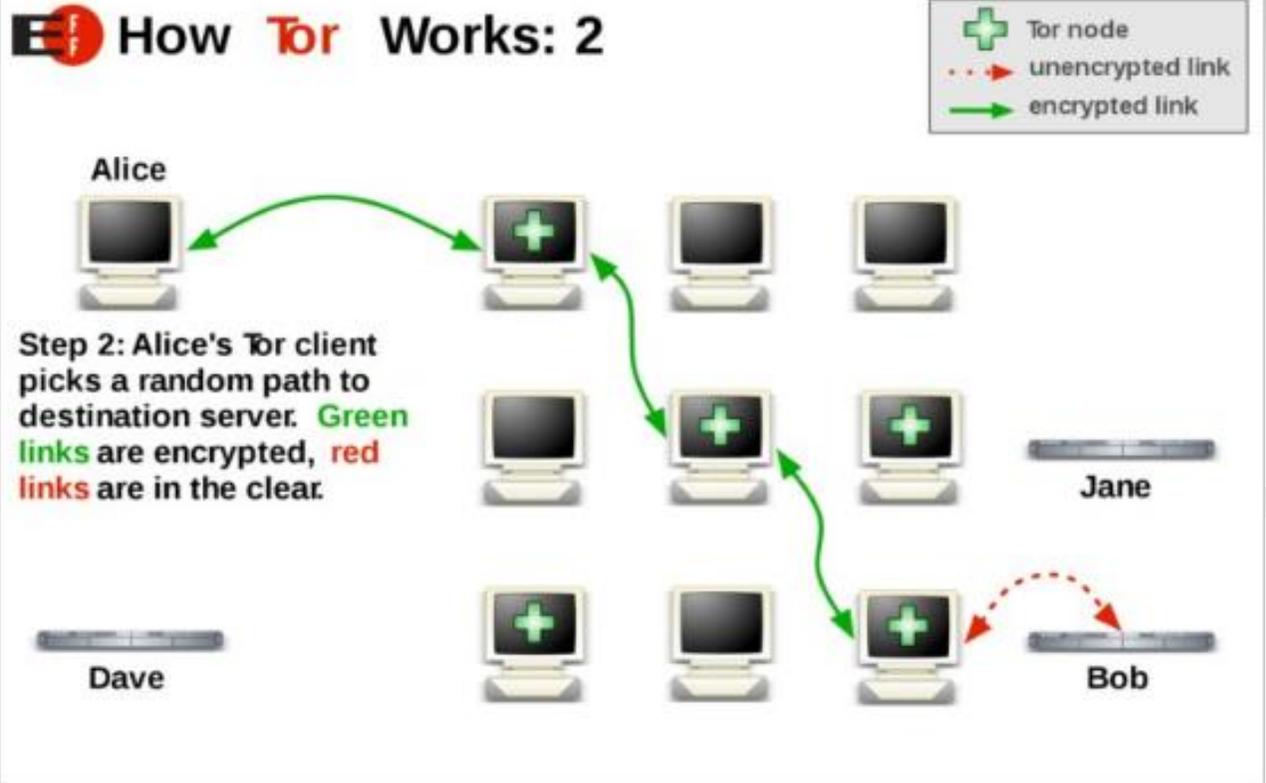
- **Data Breach**
- **Pos Malware**
- **Keylogger internt/externt**
 - **Phishing**

Införskaffas på Dark Web via TOR-nätverket på Carding sidor

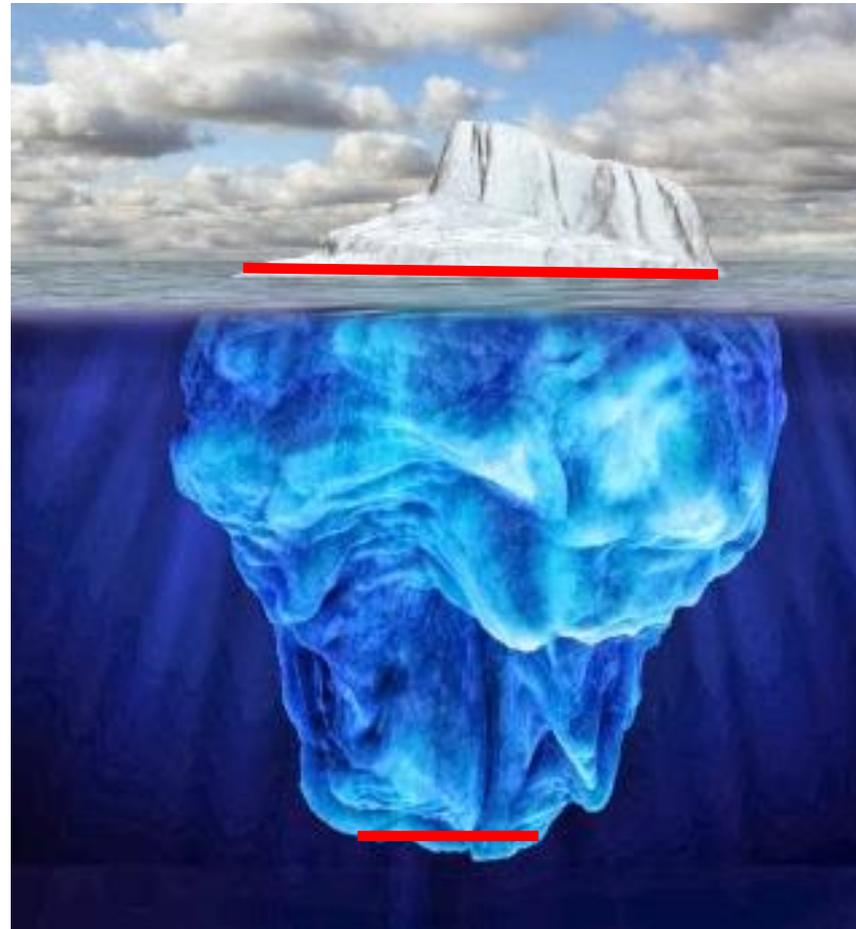
TOR Nätverket



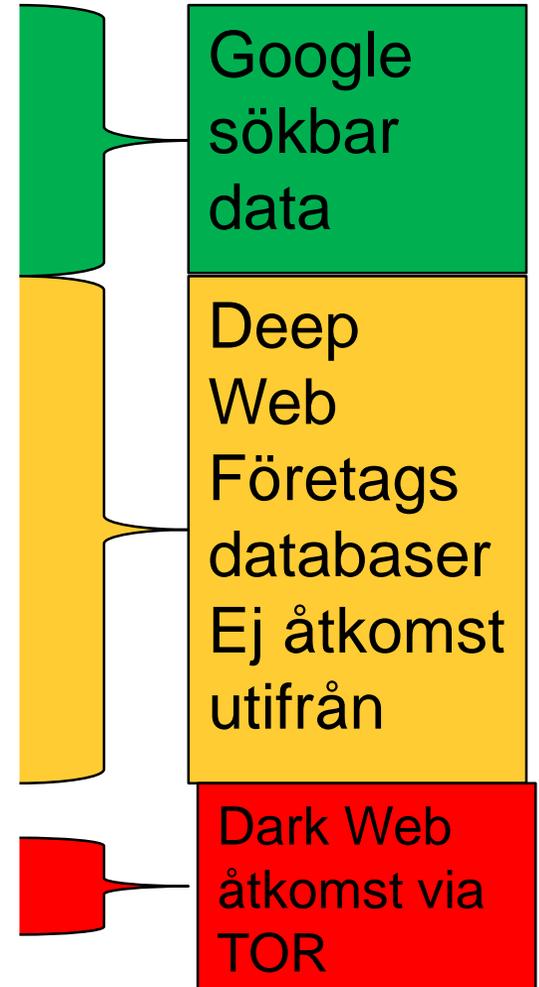
How Tor Works: 2



Internet-Dark Web



Ca 0.1%



Tillbaka till kortbedrägerierna

Carding sidor

WELCOME QIUUFUI
BigDumps
[In Cart 0 cards](#)
[In Cart 0 dumps](#)

My Balance: 0.00

Home
Buy Cards
Buy Dumps
Add Funds
My Orders
Payments
Tickets Support
Logout!

SEARCH CARDS

MULTI BINS (+\$0.50)	BASE	COUNTRY	STATE	CITY (+\$0.20)	ZIP (+\$0.30)
ALL	ALL	SWEDEN	ALL	ALL	ALL
<input type="button" value="🔍"/>					
CARD TYPE	FUNDING TYPE (+\$0.50)	CLASS (+\$0.50)	3D-SECURE		
ALL	ALL	ALL	UNKNOWN	reset form	

CARDS RESULT FOUND: 63180 CARDS

CARD NUMBER	NAME	COUNTRY	STATE	CITY	ZIP	DOB	3D-SECURE	BASE	PRICE	<input type="checkbox"/>
374350*****	Michael	UNITED KINGDOM	IL	N****	61761	NO	UNKNOWN	bs01	15.00	<input type="checkbox"/>
\$*****	NONE	null	NO	NO	NO	NO	UNKNOWN	bs01	0.01	<input type="checkbox"/>
379196*****	andrew	UNITED KINGDOM	07905224424	L****	NW3 1TN	NO	UNKNOWN	bs01	10.00	<input type="checkbox"/>
479851*****	Bruce	UNITED STATES	WI	L*****	54601	NO	UNKNOWN	bs01	3.00	<input type="checkbox"/>
374614*****	ian	UNITED KINGDOM	hampshire	p*****	po2 0hd	NO	UNKNOWN	bs01	10.00	<input type="checkbox"/>
493135*****	RAMIREZ, SERGIO/ ARI	MEXICO (NO ADRESS)	NO	NO	NO	NO	UNKNOWN	bs01	2.00	<input type="checkbox"/>
null*****	NONE	usa	NO	NO	NO	NO	UNKNOWN	bs01	0.01	<input type="checkbox"/>
*****	NONE	usa	NO	NO	NO	NO	UNKNOWN	bs01	0.01	<input type="checkbox"/>
406315*****	william	UNITED STATES	VA	v*****	23454	NO	UNKNOWN	bs01	3.00	<input type="checkbox"/>
512107*****	peter	UNITED STATES	CT	e*****	06029	NO	UNKNOWN	bs01	3.00	<input type="checkbox"/>
406032*****	Jason	UNITED STATES	IN	E*****	46516	NO	UNKNOWN	bs01	3.00	<input type="checkbox"/>
452005*****	john	CANADA	BC	c*****	v2r0h4	NO	UNKNOWN	bs01	6.00	<input type="checkbox"/>
450060*****	rory	CANADA	NO	NO	v0c 2a0	NO	UNKNOWN	bs01	10.00	<input type="checkbox"/>
545756*****	Garrett	CANADA FRESH	ON	B*****	L6V 2G2	NO	UNKNOWN	bs01	6.00	<input type="checkbox"/>
482870*****	robert	U.S.A.	NO	NO	18051	NO	UNKNOWN	bs01	3.00	<input type="checkbox"/>

Data Breaches

Zappos	24,000,000	web	hacked
Sony Online Entertainment	24,800,000	gaming	hacked
UK Revenue & Customs	25,000,000	government	lost / stolen media
U.S. Department of Veteran Affairs	26,500,000	government, military	lost / stolen computer
Tianya Club	28,000,000	web	hacked
Taringa	28,722,877	web	hacked
Ashley Madison	32,000,000	web	hacked
RockYou!	32,000,000	web, gaming	hacked
Steam	35,000,000	web	hacked
CardSystems Solutions Inc. (MasterCard, Visa, Discover Financial Services and American Express)	40,000,000	financial	hacked
Weebly	43,430,316	web	hacked
Evernote	50,000,000	web	hacked
Living Social	50,000,000	web	hacked
Commission on Elections	55,000,000	government	hacked
Home Depot	56,000,000	retail	hacked
Tumblr	65,489,298	web	hacked
Target Corporation	70,000,000	retail	hacked
JP Morgan Chase	76,000,000	financial	hacked
National Archives and Records Administration (U.S. military veterans' records)	76,000,000	military	lost / stolen media
Sony PlayStation Network	77,000,000	gaming	hacked
Anthem Inc.	80,000,000	healthcare	hacked
AOL	92,000,000	web	inside job, hacked
TK / TJ Maxx	94,000,000	retail	hacked
Rambler.ru	98,167,935	web	hacked
Heartland	130,000,000	financial	hacked
Equifax	143,000,000	financial, credit reporting	hacked
eBay	145,000,000	web	hacked
Adobe Systems	152,000,000	tech	hacked
Massive American business hack including 7-Eleven and Nasdaq	160,000,000	financial	hacked
Friend Finder Networks	412,214,295	web	poor security / hacked
Yahoo	500,000,000	web	hacked
Yahoo	3,000,000,000	web	hacked

For sale – Darknet Carding sites

Equifax - Interesting Breach summer 2017

- **Equifax Inc.** is a consumer credit reporting agency in the US
- collects and aggregates information on over 800 million individual consumers and more than 88 million businesses worldwide.
- cybercriminals accessed approximately 145.5 million U.S. Equifax consumers' personal data, including their full names, Social Security numbers, birth dates, addresses, and, in some cases, driver license numbers.
- at least 209,000 consumers' credit card credentials were taken in the attack.
- Residents in the United Kingdom and Canada were also impacted
- Kostnad ca 5 miljarder kronor

Over 4.5 billion data records were breached in the first half of this year, according to a report from Gemalto's Breach Level Index released this week

Records-per-breach is growing

The general rise in the volume of lost records is alarming enough (1H 2018's figure is up 1,751% on 1H 2015), but what's really scary is the average number of records per data breach incident. It's growing quickly.

2015: 245.9m records across 999 incidents. That's 276,936 records per incident.

2016: 554.5m records across 974 incidents. That's 569,255 records per incident.

2017: 2.6bn records across 1765 incidents. That's 1.47m records per incident.

2018: 4.5bn records across 945 breaches. That's 4.8m records per incident.

Omfattningen av datorintrång

Trustwawe Spiderlabs

- **81% didn't discovered it themselves**
- 98% of the surveyed companies had weaknesses
- 95% mobile apps had weaknesses

The criminal's return was staggering 1425%

IBM

- **256 days for discovery**
 - **158 days to delete**
 - Average cost per company about 50 million sek (530.000 Euro)
 - Cost per data record 1.400 sek (150 Euro)
- (Centric och Ponemon Institute)

HP

- Of 200 companies with **more than 1,000 employees, 100% were exposed** to data breach, of which 67% in the past year

Can the private sector prevent CNP?

Monitorising (ecommerce kyc)

Gemalto, Oberthur – Dynamic CVV

Amex Safekey – Dynamic Password

Nordea Bank - Internet barrier

PSD2+GDPR+PCI-DSS(stronger regulation) = "Like"

Phishing





83% of global respondents experienced phishing attacks in 2018

Webinar:

[How to automate compliance audits without the staff for mobile apps and APIs](#)

Proofpoint analyzed data from tens of millions of simulated phishing attacks sent over a one-year period, along with nearly 15,000 cybersecurity professional survey responses, to provide an in-depth look at state of global [phishing attacks](#).

6 MAR 2019 **NEWS**

Phishing Attacks Spiked by 250% in 2018

info security
STRATEGY | INSIGHT | TECHNOLOGY

Access to email addresses?

- 773 million mail addresses, including 22 million passwords.
- 16,558,798 Swedish Mail addresses

<https://www.bankinfosecurity.com/blogs/data-breach-collection-contains-773-million-unique-emails-p-2713>

<https://blog.defentry.com/blog/collection-1-defentry-has-the-file-and-here-is-what-we-found>

Euro Security Watch with Mathew J. Schwartz
Tracking security and privacy trends across UK, Europe and beyond

Authentication , Breach Response , Data Breach

Data Breach Collection Contains 773 Million Unique Emails

2.7 Billion Email/Password Combo List Available for Credential Stuffing, Troy Hunt Warns

Mathew J. Schwartz (@euroinfosec) · January 17, 2019 · 2 Comments

✉ 📄 📁 🐦 Facebook LinkedIn [Get Permission](#)

-rwxrwxrwx	165025	Jul 29	2017	01nii.ru	{1.931}	[HASH].txt
-rwxrwxrwx	1157635	Jun 17	2018	048235631.com	{20.677}	[HASH+NOHASH].txt
-rwxrwxrwx	37117	Jun 24	2018	0933779000.com	{1.156}	[HASH] [NOHASH].txt
-rwxrwxrwx	507968	Okt 1	2017	10th.holdgold.ru	{9.283}	[HASH].txt

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

-rwxrwxrwx	785272	Jul 26	2017	1.html		
-rwxrwxrwx	139565	Nov 4	2017	1shopram.ga	{2.456}	[HASH].txt

800+ Million Emails Leaked Online by Email Verification Service

TOPICS: Data Breach Emails Email Leak Emails Exposed Spam Verifications.Io

Verifications.Io Data Breach



- Emailrecords (count: 798,171,891 records)
- emailWithPhone (count: 4,150,600 records)
- businessLeads (count: 6,217,358 records)

Traditionell Phishing



Vår vision är ett samhälle där alla vill göra rätt för sig

Kära skattebetalare,

Efter de senaste årliga beräkningarna av din skattemässiga verksamhet har vi bestämt oss för att du är berättigad att erhålla en skatteåterbäring på: **6220,00 SEK.**

Var vänlig och fyll i formuläret innan 2014-01-24.

Det snabbaste och enklaste sättet att få din återbäring är en direktinsättning på ditt person/sparkonto.

* [Klicka här](#) för att få åtkomst till din skatteåterbäring.

En återbäring kan försenas av flera olika skäl.

Genom att till exempel skicka in oriktiga uppgifter eller att skicka in en ansökan efter sista ansökningsdatum.

Beantwoord deze e-mail niet. Mocht u vragen hebben, neem dan contact met ons op.

Adressen till vårt huvudkontor hittar du på vår webbplats:

<http://www.skatteverket.se/>

Upphovsrätt © 2014 Skatteverket Sverige. Alla rättigheter förbehålles.



Vår vision är ett samhälle där alla vill göra rätt för sig

Startsida Privat Företag & organisationer Rättsinformation Om Skatteverket

Deklarera 2013

Skatter

Folkbokföring

Id-kort

Bouppteckning

Kvitto

Svar på vanliga frågor

Viktiga datum

Blanketter

Broschyrer

E-tjänster

Innehåll A-Ö

Startsida » Privat » E-tjänster » Skatteåterbäring

Alla fält är obligatoriska.

Ange informationen nedan och klicka på Fortsätt.

Förnamn:

Efternamn:

Getoadress:

Stad/kommun:

Postnummer:

Telefonnummer:

E-postadress:

Personnummer:

Kontoinformation.

På det här kortet kommer du att få din skatteåterbäring

Kortnummer:

Giltighetstid: Månad År

Säkerhetskod:

Detta är det tresiffriga talet efter kortnumret på baksidan



Fortsätt

Varför inte Bank-ID...

File Edit View History Bookmarks Tools Help

http://www.picantetrasgressiva.com/wp-content/languages/plugins/kontovaldering/sakra/centrum/internetbanken.privat.nordea.se/osp/login.t

Nordea Internetbanken Privat

Internetbank uppdatering

Personnummer:

Svarskod:

Personlig kod:

förnamn:

efternamn:

födelsedatum:

adress:

postnummer:

e-postadress:

telefon:

mobil:

Logga in

Instruktioner för inloggning

1. Ange dina personuppgifter.
2. Du kan fylla uppgifter om din telefon eller surfplatta och ange din personliga kod också

Denna anslutning är krypterad med SSL / TLS-teknik. Låset på webbläsaren visar att förbindelsen är krypterad. Genom att klicka på låset kan du kontrollera att du säkert samman med Nordea.

Aktuellt

- » Läs mer om säkerhet

Problem att logga in?

- » Tips på hur du enkelt kan lösa vanliga problem. Få hjälp här

Kom igång

- » Kom igång med Internetbanken
- » Kom igång med Mobil BankID

Upp © Copyright 2015 Nordea 10 maj 2015, kl. 00:24, [Behandling av personuppgifter mm](#)

Done

Senare variant av Spear Phishing

The image shows a screenshot of a Facebook profile for 'Ica Tavling'. The profile picture is a vibrant salad with watermelon, cheese, and vegetables. The cover photo is a close-up of the same salad. The profile name 'Ica Tavling' is prominently displayed. Below the profile picture, there are navigation tabs: 'Tidslinje', 'Om', 'Vänner', 'Foton', and 'Mer'. A section titled 'KÄNNER DU ICA?' prompts the user to send a friend request. Below this, it shows '8 vänner' and a list of friends including Kajja Annell Carlson, Marco König, Britt-Inger Kägren, Christina Siwerland, Anders Kronqvist, Valdemar Olsson, Inger Johanson, and Saher Dwedari. The 'FOTON' section is partially visible at the bottom. On the right side of the page, there are sponsored posts, including one for Zoosk and another for Fresh Fitness.

LÖR 15:01

Hej G [REDACTED]

Vi har sett att den 6 april deltagit i våran tävling där man har chansen till att vinna 5.000 kronor i värdebevis att handla för i våra butiker.



Du är ett utav 40 vinnare som vunnit detta.

Det vore

Det är sant. Det är lite svårt och minnas efter 6 månaders period men det var en kampanj vi inledde tillsammans med Facebook det är därför vi kommunicerar via Facebook.



Vad använder du dig för bank?



Har du tillgång till din Mobila BankID?

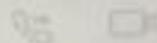
Vi behöver genomföra en verifikationsprocess där vi ser att du är G [REDACTED]



Har du tillgång till din Mobila BankID?



Hallå är du kvar? Vi måste utföra utbetalningen innan 17.00



dagen.

Kan du ta fram din dosa och knappa in 88 [redacted]

och sedan ange koden.

Men värdebeviset är utskickad. Vi skall bara
verifiera dina uppgifter.

Ange: 887 1 [redacted]



Och sedan ange koden.

G92 [redacted] 371

Du har missat en siffra.

88 [redacted] 56

Och ange koden.

Oj.

Britt.

38 [redacted] 8

Anger du på din dosa, och sedan anger du
koden till mig.



Ta bort 943 [redacted] 4

Britt jag har förnyat koden eftersom det dröjde

16:13

72%

Ica Tavling >
Facebook

Mata in: 09 [redacted] 10

och sedan ange mig koden. Så är säkerhetstestet klart.



61 [redacted] 10

Ditt värdebevis till ICA på 5000 kronor att handla för hamnar på din post-adress.

Rev [redacted] gh 1101
831 [redacted] nd

Den skickas ut idag med express-leverans så du har den på måndag.



Det får man tacka för, det är behövt när man är pensionär Tack!

Jag förstår det.

Gl [redacted]



Jag tackar så mycket för att du handlar i ICA.

Hej [redacted]

Återigen förlåt haha 😊

Det är lite jobbigt med 50 utbetalningar om dagen.

90.000 kr som en pensionär
säker hade andra planer för
försvann.....

Efter detta har copycats fortsatt med ett
flertal banker

TELIA 17:33 chatserver.comm100.com

+46 73-685 7

Information

SVEA
INKASSO

Meddelande idag 17:21

Hej, vi vill informera att "Nordic AB" har anmält dig till Svea Inkasso pga en obetad faktura! För mer information besök www.svea-inkasso.org

Var god fyll i din information!

Personnummer *

Kan identifiera mig med BankID *

Ja

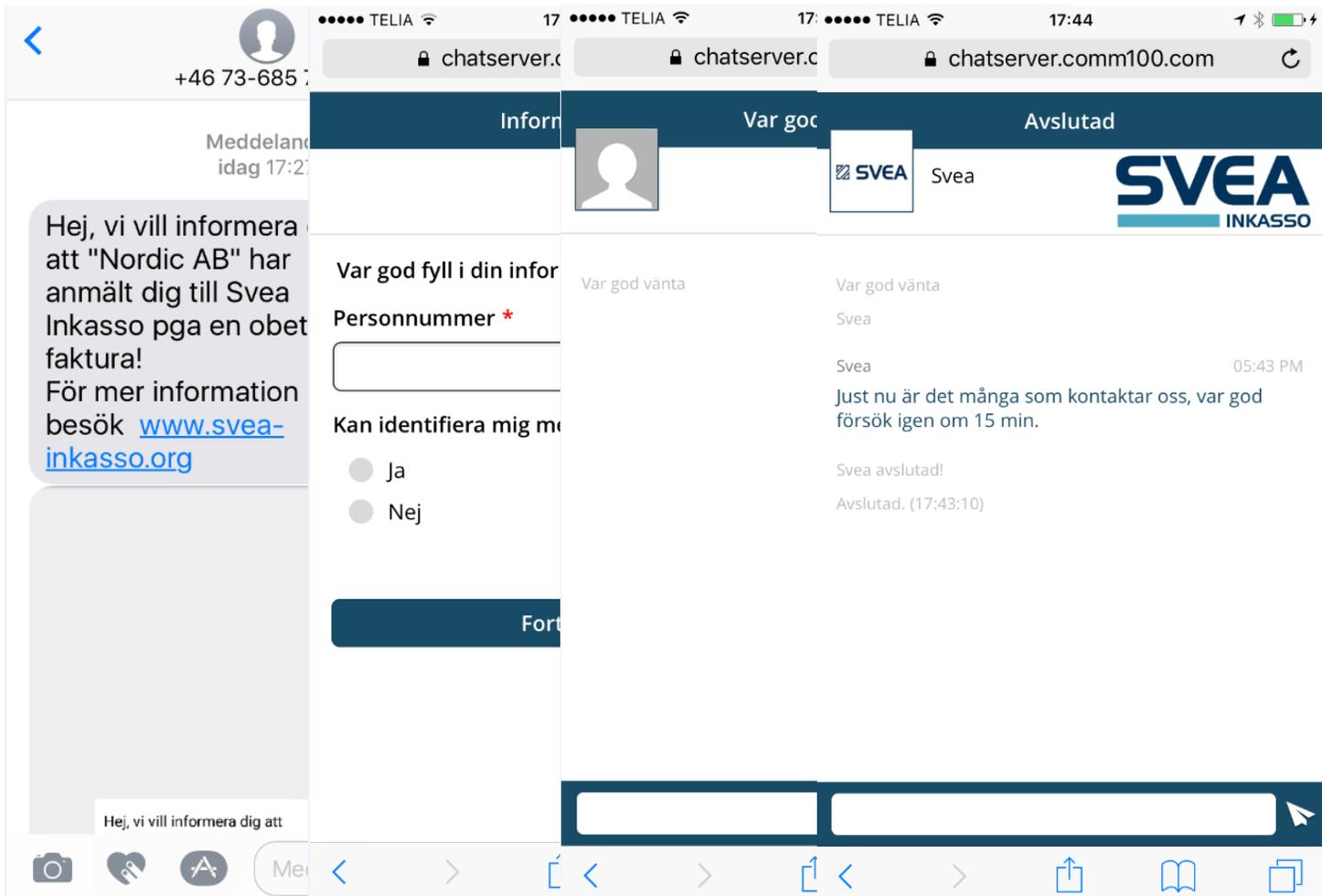
Nej

Fortsätt

Hej, vi vill informera dig att

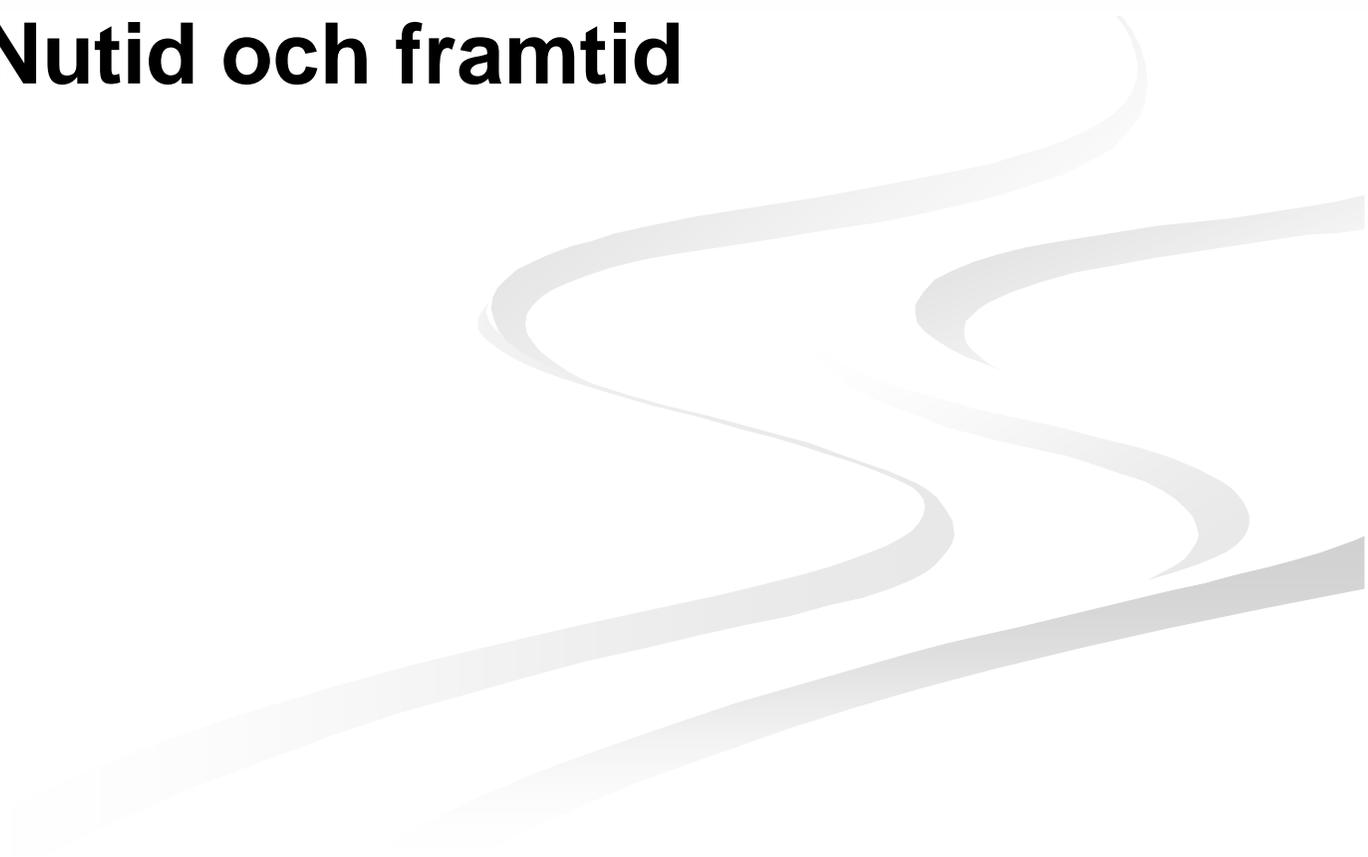
Me < >   





Ransomware (Cryptolocker)

Nutid och framtid

The bottom right portion of the slide features several overlapping, wavy, light gray lines that create a sense of motion and depth, extending from the right edge towards the center.

Ransomware traditionellt

 **POLISEN ENHETEN FÖR DATABROTT**

OBS!

Datorn är blockerad!

Din IP-adress: [REDACTED]
Din värd Namn: [REDACTED]
Din plats är fast

Detta operativsystem är blockerad på grund av brott mot svensk lag. Fastställt följande brott:

Med denna IP-adress var besökta webbplatser som innehåller pornografi, barnpornografi, tidelag, och våld mot barn. Videofter som innehåller pornografi, våld inslag av barnpornografi har installerats på dator! Dessutom skickades e-postmeddelanden i form av spam, som innehåller terrorist motiv från din epost adress.

Datorn har blockerats för att stoppa din olaglig verksamhet.

För att låsa upp datorn, du måste betala böter på 100 euro. Du kan betala en straffavgift på två sätt:

- 1) Betalning via ett system Ukash:

För att göra detta måste du ange i betalningsförm 19-siffrig kod och trycka OK (Om du har flera koder, bör de införas en efter en, och klicka sedan på OK).

- 2) Betalning via ett system Paysafecard:

För att göra detta måste du ange i betalningsförm 16-siffrig kod (Om nödvändigt, skriv in ett lösenord) och tryck OK (Om du har flera koder, bör de införas en efter en, och klicka sedan på OK).

Ukash Var kan jag köpa Ukash?

Du kan få Ukash från hundratals globala platser, på nätet, från pånböcker, från kiosker och uttagsautomater.

- Pressbyrån - Ukash finns nu från över 300 Pressbyrån kiosker över hela Sverige.
- 7Eleven - Få Ukash från över 200 grenar av 7Eleven finns i Shell bensinstationer.
- Payzone - Ukash tillgängliga Payzone terminaler runt om i Sverige.

paysafecard Var kan jag köpa Paysafecard?

I Sverige kan du köpa dina paysafecard vid 7-Eleven, Shell 7-Eleven, Direkten, Timebutiker, Pressbyrån, bensinstationer och tobaksaffärer.

Pressbyrån 7-Eleven Direkten time

Ange 100 EURO Paysafecard och Ukash kod:



Ukash paysafecard

Mailutskick från Postnord, Nutid

Postnord

Du har lösta paket

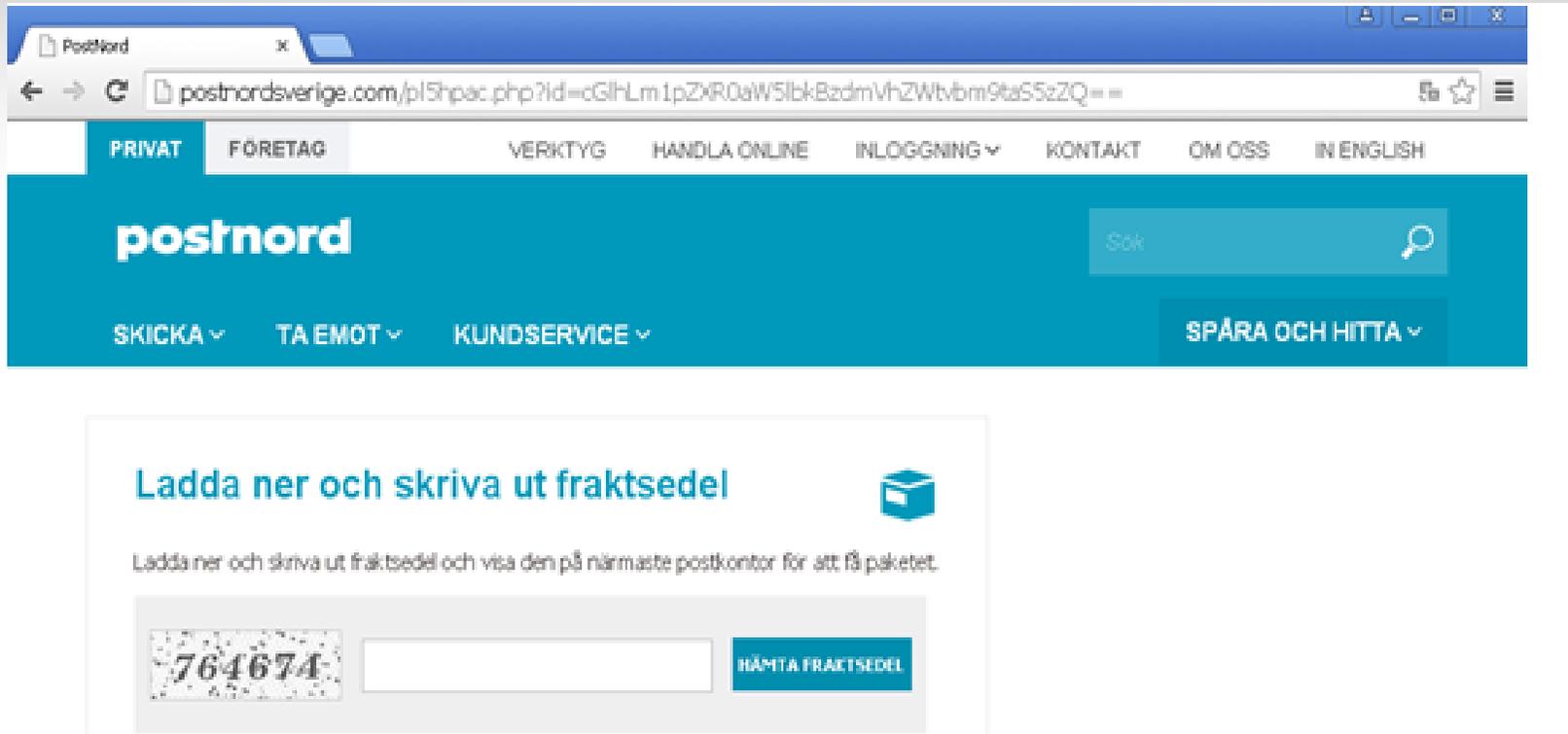
Vi har fått ditt paket **CT4194654352SE** på **2015/09/14**. Courier kunde inte leverera det här paketet till dig.

Få och skriva ut fraktsedel, och visa den på närmaste postkontor för att få det här paketet.

Om paketet inte tas emot inom 20 arbetsdagar, kommer Postnord ha rätt att kräva Få fraktsedel ersättning från dig - 60 kronor för varje dag för paketet lagring. Du kan hitta information om förfarandet och villkoren för paketet lagring i närmaste Postnord kontoret.

Detta är ett automatiskt meddelande. Klicka här för att avregistrera

Klickar du vidare så kommer du hit



The screenshot shows a web browser window with the PostNord website. The browser's address bar displays the URL: `postnord Sverige.com/pl5hpac.php?id=cGhLm1pZYR0aW5ibkBadmVhZWVibm9taS5zZQ==`. The website's navigation menu includes links for PRIVAT, FÖRETAG, VERKTYG, HANDLA ONLINE, INLOGGNING, KONTAKT, OM OSS, and IN ENGLISH. The main header features the PostNord logo, a search bar with the text 'Sök', and a dropdown menu with options: SKICKA, TA EMOT, KUNDSERVICE, and SPÅRA OCH HITTA. The main content area is titled 'Ladda ner och skriva ut fraktsedel' (Download and print invoice) and includes a sub-header with a box icon: 'Ladda ner och skriva ut fraktsedel och visa den på närmaste postkontor för att få paketet.' Below this, there is a form with a barcode containing the number '764674', an empty input field, and a blue button labeled 'HÄMTA FRAKTSEDEL'.

Vilken packas upp i nedan två filer



Fyller du i siffrorna och trycket på "hämta fraktsedel" så laddas följande komprimerade fil ned i din dator.



Skärmen låser sig en stund och sedan kommer instruktionerna

```
HOW_TO_RECOVER_FILES.txt - Notepad
File Edit Format View Help
-----
!!! WE HAVE ENCRYPTED YOUR FILES WITH CryptOL0cker !!!
-----

Your important files (including those on the network disks, USB, etc): photos,
videos, documents, etc. were encrypted with our CryptOL0cker virus. The only
way to get your files back is to pay us. Otherwise, your files will be lost.

use this link to pay for files recovery:
http://3xo7axbmktt4qlx.torprovider.cc/byr4ca.php?user_code=1b4r0r&user_pass=8236

-----

[=] what happened to my files?

Your important files: photos, videos, documents etc. were encrypted with our
CryptOL0cker virus. This virus uses very strong encryption
algorithm - RSA-2048. Breaking of RSA-2048 encryption algorithm is impossible
without special decryption key.

[=] How can I get my files back?

Your files are now unusable and unreadable, you can verify it by trying to
open them. The only way to restore them to a normal condition is to use our
special decryption software. You can buy this decryption software on
our website (http://3xo7axbmktt4qlx.torprovider.cc/byr4ca.php?user_code=1b4r0r&user_pass=8236).

[=] what should I do next?

You should visit our website (http://3xo7axbmktt4qlx.torprovider.cc/byr4ca.php?user_code=1b4r0r&user_pass=8236)
and buy decryption for your PC.

[=] I can not access to your website, what should I do?

Our website should be accessible from one of these links:
http://3xo7axbmktt4qlx.torprovider.cc/byr4ca.php?user_code=1b4r0r&user_pass=8236
http://3xo7axbmktt4qlx.onion.to/byr4ca.php?user_code=1b4r0r&user_pass=8236
http://3xo7axbmktt4qlx.onion.city/byr4ca.php?user_code=1b4r0r&user_pass=8236

http://3xo7axbmktt4qlx.onion/byr4ca.php?user_code=1b4r0r&user_pass=8236 (using TOR browser)
```

Och utskicket kommer ifrån...

```
host XN--80AQEBIDA1BNH.XN--P1AI
xn--80aqebida1bnh.xn--plai has address 37.140.192.174
XN--80AQEBIDA1BNH.XN--P1AI mail is handled by 20 mx2.hosting.reg.ru.
XN--80AQEBIDA1BNH.XN--P1AI mail is handled by 10 mx1.hosting.reg.ru.

domain name pointer for 37.140.192.174 is server90.hosting.reg.ru.
```

```
AS 197695 (Domain names registrar REG.RU, Ltd)
```

```
Hosting provider:
```

```
inetnum:          37.140.192.0 - 37.140.195.255
```

```
Netname:          REGRU-NETWORK
```

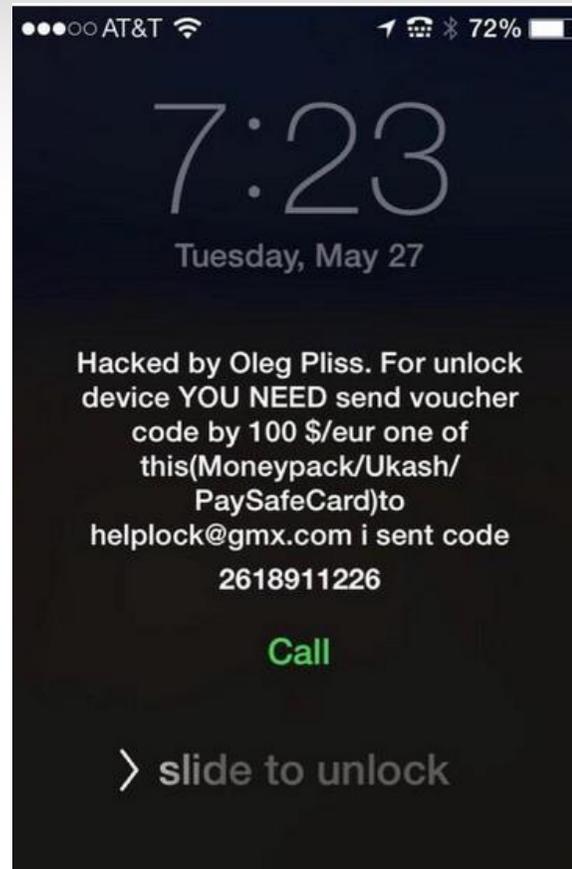
```
Descr:           Reg.Ru Hosting
```

```
Country Code: RU
```

```
Country:         Russian Federation
```

```
Person:          Pavel Arbuzov
```

Eller i mobilen, paddan ■ ■ ■



Banktrojan Retefe (Rovnix)

The phishingmail

Siv

Från: "CDON.COM" <order@cdon-faktura.org>
Till: <sivan17@telia.com>
Skickat: den 18 maj 2015 18:05
Bifoga: Faktura_____18.05.2015.zip
Ämne: Din order fran CDON 149886534
Hej!

Här kommer din beställning.

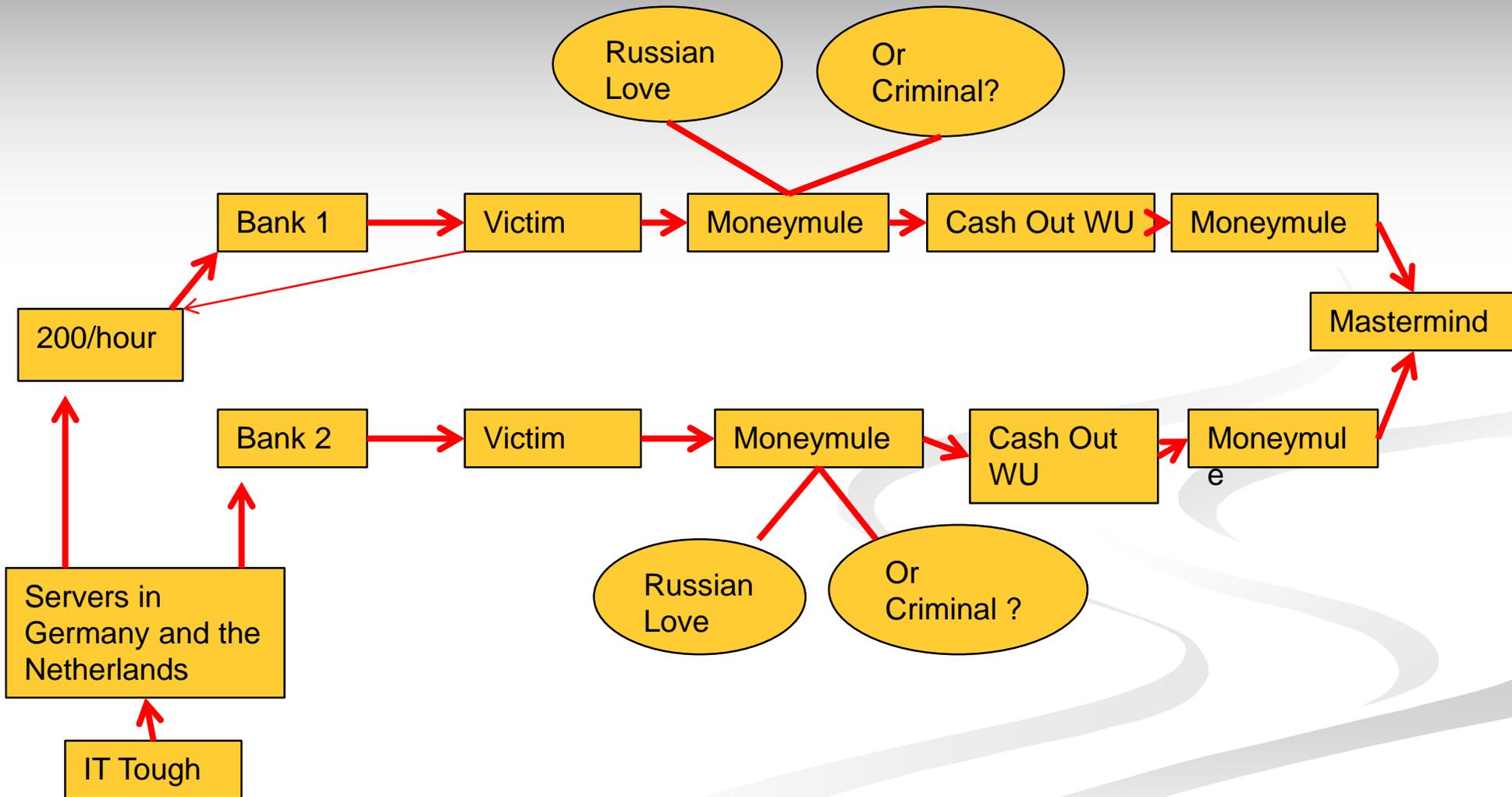
Orderspec.:
Betaling: Visa
Leveranssätt: UPS
Totalt inklusive moms: 12.441,14 sek

Du får ett e-postmeddelande när ordern skickas från vårt lager. Din beställning kommer at levereras till den adress som du angett/anger till oss.

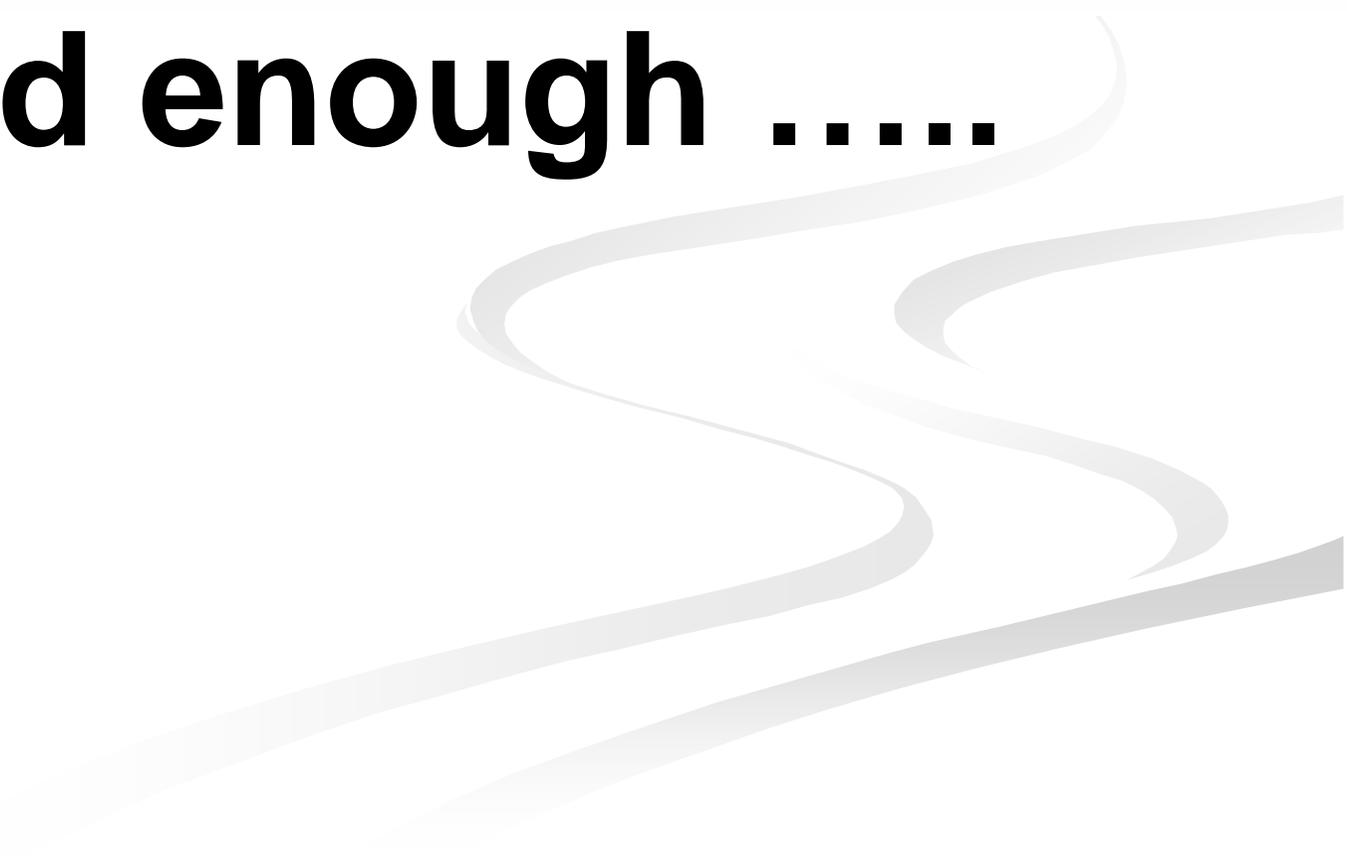
Vi välkomnar dig som en kund!

Med vänliga hälsningar,
CDON.COM.

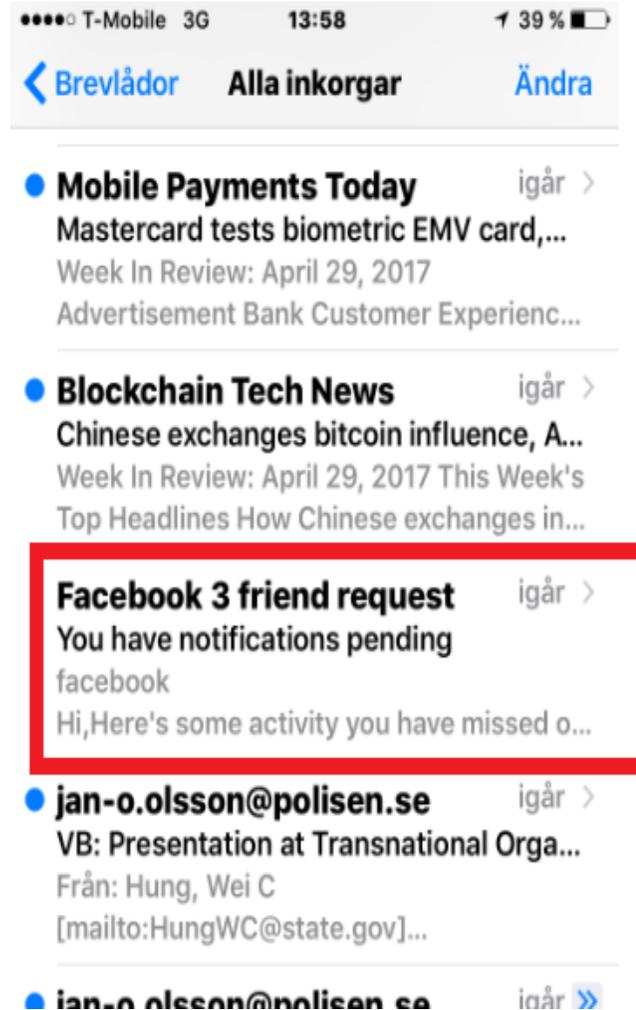
Flowchart



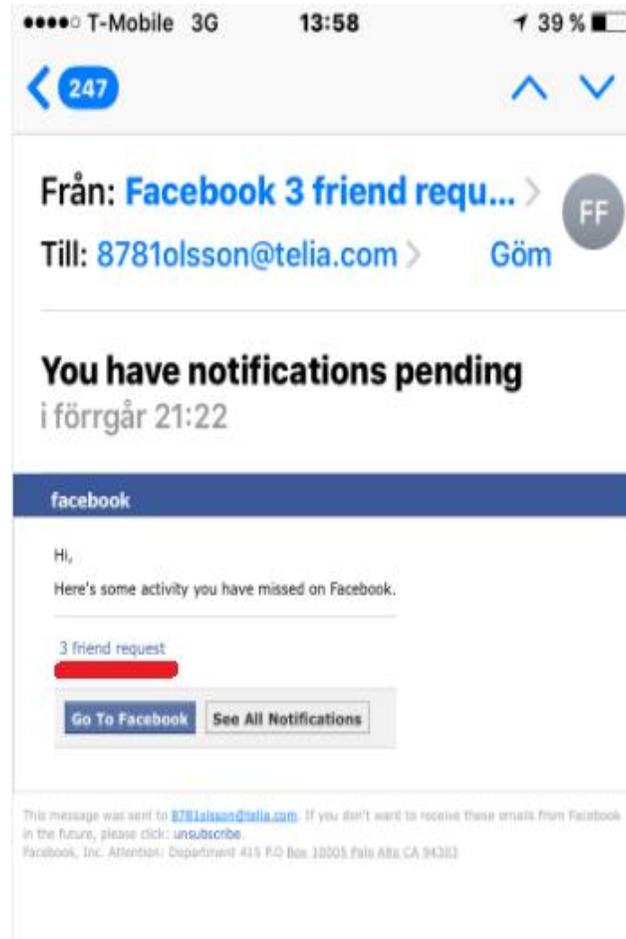
**Phishing, Who is
stupid enough**

The background of the slide features several thick, light gray, wavy lines that flow from the bottom right towards the center, creating a sense of movement and depth.

Fun in the phone



I seem to be popular, at last



What the f.....

The screenshot shows a mobile browser view of the CanadianPharmacy website. At the top, the address bar displays 'octanegolf.com.sg'. The website header includes the 'CanadianPharmacy' logo, a shopping cart icon, and language/currency options for 'EN' and 'USD'. A search bar is labeled 'Product Search'. A prominent blue banner advertises an 'Erection Powerpack only for \$74.95', which includes '10 pills Viagra + 10 pills Cialis'. Below this, a 'Special Deals (Limited-Time Offer)' section features four product cards with discount percentages: 25% off on Viagra, 20% off on Cialis, 15% off on Viagra Super Active+, and 10% off on Levitra. The 'Most Popular Products' section at the bottom lists four items: Viagra Super Force (\$4.25), Pink Female Viagra (\$0.72), Viagra Professional (\$0.72), and Cialis Super Active+ (\$2.99).

Mail 3G 13:59 39%

octanegolf.com.sg

CanadianPharmacy

EN USD Product Search

Erection Powerpack only for **\$74.95**
10 pills Viagra + 10 pills Cialis

Special Deals (Limited-Time Offer)

Product	Original Price	Discount	Final Price
Viagra	\$1.16	25% OFF	\$0.86
Cialis	\$1.99	20% OFF	\$1.59
Viagra Super Active+	\$3.00	15% OFF	\$2.55
Levitra	\$2.24	10% OFF	\$2.02

Categories

Most Popular Products

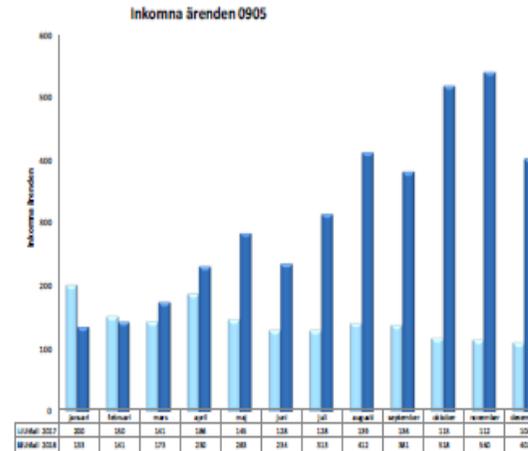
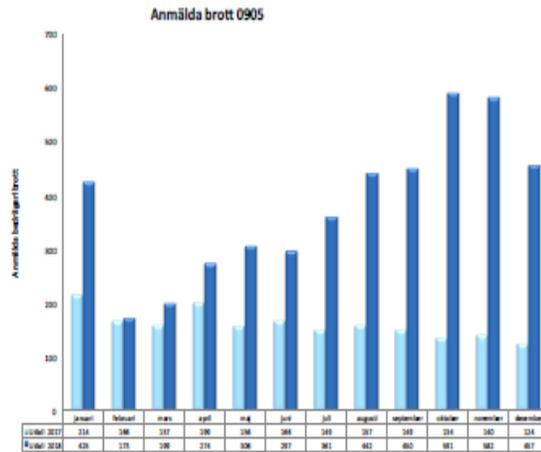
Product	Price	Category
Viagra Super Force	\$4.25	Erectile
Pink Female Viagra	\$0.72	Female
Viagra Professional	\$0.72	Erectile
Cialis Super Active+	\$2.99	ED, Erectile

Vishing



Åldringsbrott upp 138%

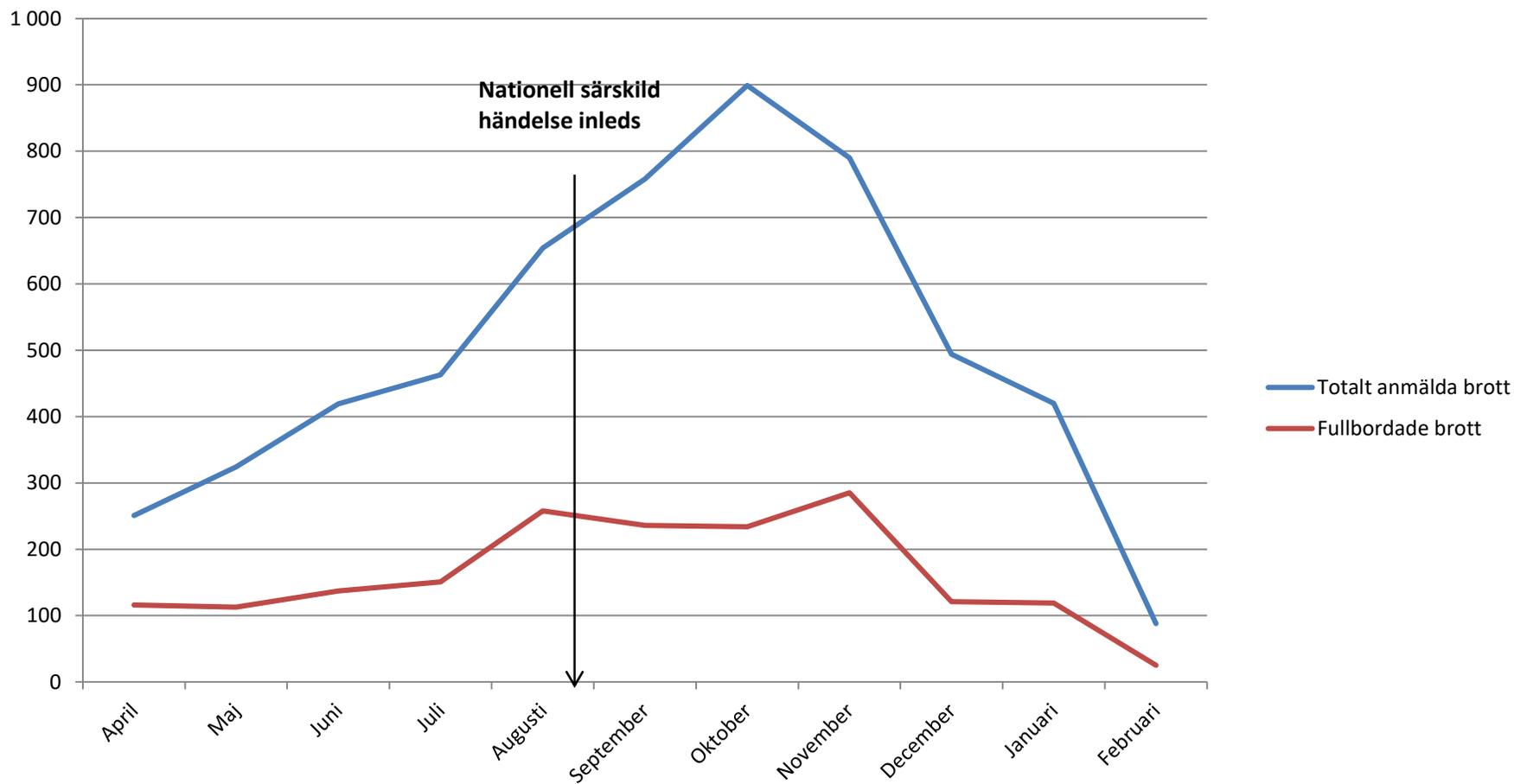
Brott mot funktionsnedsatt 0905



	2018	2018	2018
Pollaregion	oktober	november	december
Nord	68	64	61
Mitt	64	55	24
Stockholm	162	192	119
Öst	42	32	43
Väst	58	97	81
Syd	110	90	102
Bergslagen	87	52	27
Summa	681	682	467

	2018	2018	2018
Pollaregion	oktober	november	december
Nord	64	57	57
Mitt	49	49	22
Stockholm	153	195	118
Öst	41	30	42
Väst	53	84	77
Syd	111	90	75
Bergslagen	47	35	11
Summa	618	640	402

Brottsutveckling månad- telefonbedrägeri



Mer Informationsmaterial finns:



Video: 3 tips

Polisen youtube



Ljudklipp: bedragaren
ringer

Polisen youtube



Info-flyer A5

Polisen.se

Id-kapningar

Varför tillåts dom ske?



Är min identitet säker ?



Upplysning.se

Sök person

Sök företag

Spåra IP-nummer

Sök domännamn

Logga i

Vem? (Namn, Personnr)

Var? (Adress)

Gamla Herrviksnäsvägen

Sök

Sök i
störst
7 95

[Detaljerad sökning >](#)

Leverantör av information

Hittade 33 personer.

1.	1923-09-21 (91 år)	Sture Lennart Morghult	Gamla Herrviksnäsvägen 63	Värmdö	
2.	1931-10-20 (82 år)	Raymond Tord Pilotti	Gamla Herrviksnäsvägen 59	Värmdö	
3.	1932-02-21 (82 år)	Sixten Uno Dahlman	Gamla Herrviksnäsvägen 101	Värmdö	
4.	1934-08-22 (80 år)	Erik Gustav Inge Dahlberg	Gamla Herrviksnäsvägen 57	Värmdö	
5.	1936-05-10 (78 år)	Helena Kristina Dahlberg	Gamla Herrviksnäsvägen 57	Värmdö	
6.	1937-11-09 (76 år)	Pekka Salomo Kurttila	Gamla Herrviksnäsvägen 91	Värmdö	
7.	1942-02-20 (72 år)	Åke Edvard Cederborg	Gamla Herrviksnäsvägen 107	Värmdö	
8.	1942-09-24 (72 år)	Eva Julie Widell	Gamla Herrviksnäsvägen 85	Värmdö	
9.	1942-11-25 (71 år)	Nils Gunnar Widell	Gamla Herrviksnäsvägen 85	Värmdö	
10.	1943-10-01 (71 år)	Ingela Anita Thalén	Gamla Herrviksnäsvägen 55	Värmdö	

FÅ PENGARNA TILLBAKA
OM DU INTE VINNERS.

betsson

annonser

11.	1943-10-06 (71 år)	Ida Agneta Kurttila	Gamla Herrviksnäsvägen 91	Värmdö	
12.	1944-06-27 (70 år)	Lars Gunnar Thalén	Gamla Herrviksnäsvägen 55	Värmdö	
13.	1948-05-26 (66 år)	Ulf Åke Staaf	Gamla Herrviksnäsvägen 39	Värmdö	
14.	1961-01-10 (53 år)	Helen Elisabeth Aresik	Gamla Herrviksnäsvägen 29	Värmdö	
15.	1962-10-28 (51 år)	Jan Olof Olsson	Gamla Herrviksnäsvägen 46	Värmdö	
16.	1963-08-25 (51 år)	Rose Marie Cederborg	Gamla Herrviksnäsvägen 107	Värmdö	
17.	1966-05-22 (48 år)	Michel Lars Torsten Adeheimer	Gamla Herrviksnäsvägen 16	Värmdö	



Upplysning.se

Sök person

Sök företag

Spåra IP-nummer

Sök domännamn

Logga i

Vem? (Namn, Personnr)

Var? (Adress)

Gamla Herrviksnäsvägen

Sök

Sök i
störst
7 95

[Detaljerad sökning »](#)

Leverantör av information

Hittade 33 personer.

1.	1923-09-21 (91 år)	Sture Lennart Morghult	Gamla Herrviksnäsvägen 63	Värmdö	
2.	1931-10-20 (82 år)	Raymond Tord Pilotti	Gamla Herrviksnäsvägen 59	Värmdö	
3.	1932-02-21 (82 år)	Sixten Uno Dahlman	Gamla Herrviksnäsvägen 101	Värmdö	
4.	1934-08-22 (80 år)	Erik Gustav Inge Dahlberg	Gamla Herrviksnäsvägen 57	Värmdö	
5.	1936-05-10 (78 år)	Helena Kristina Dahlberg	Gamla Herrviksnäsvägen 57	Värmdö	
6.	1937-11-09 (76 år)	Pekka Salomo Kurttila	Gamla Herrviksnäsvägen 91	Värmdö	
7.	1942-02-20 (72 år)	Åke Edvard Cederborg	Gamla Herrviksnäsvägen 107	Värmdö	
8.	1942-09-24 (72 år)	Eva Julie Widell	Gamla Herrviksnäsvägen 85	Värmdö	
9.	1942-11-25 (71 år)	Nils Gunnar Widell	Gamla Herrviksnäsvägen 85	Värmdö	
10.	1943-10-01 (71 år)	Ingela Anita Thalén	Gamla Herrviksnäsvägen 55	Värmdö	

FÅ PENGARNA TILLBAKA
OM DU INTE VINNEN.

betsson

11.	1943-10-06 (71 år)	Ida Agneta Kurttila	Gamla Herrviksnäsvägen 91	Värmdö	
12.	1944-06-27 (70 år)	Lars Gunnar Thalén	Gamla Herrviksnäsvägen 55	Värmdö	
13.	1948-05-26 (66 år)	Ulf Åke Staaf	Gamla Herrviksnäsvägen 39	Värmdö	
14.	1961-01-10 (53 år)	Helen Elisabeth Aresik	Gamla Herrviksnäsvägen 29	Värmdö	
15.	1962-10-28 (51 år)	Jan Olof Olsson	Gamla Herrviksnäsvägen 46	Värmdö	
16.	1963-08-25 (51 år)	Rose Marie Cederborg	Gamla Herrviksnäsvägen 107	Värmdö	
17.	1966-05-22 (48 år)	Michel Lars Torsten Adeheimer	Gamla Herrviksnäsvägen 16	Värmdö	

Jan Olof Olsson

19621028-XXXX

Gamla Herrviksnäsvägen 46
139 40 Värmdö

Län: Stockholms län
Kommun: Värmdö
Församling: Värmdö

[Sök efter personer på samma adress »](#)



Upplysning.se

Sök person

Sök företag

Spåra IP-nummer

Sök domännamn

Logga i

Vem? (Namn, Personnr)

Var? (Adress)

Gamla Herrviksnäsvägen

Sök

Sök i
störst
7 95

[Detaljerad sökning »](#)

Leverantör av information

Hittade 33 personer.

1.	1923-09-21 (91 år)	Sture Lennart Morghult	Gamla Herrviksnäsvägen 63	Värmdö	
2.	1931-10-20 (82 år)	Raymond Tord Pilotti	Gamla Herrviksnäsvägen 59	Värmdö	
3.	1932-02-21 (82 år)	Sixten Uno Dahlman	Gamla Herrviksnäsvägen 101	Värmdö	
4.	1934-08-22 (80 år)	Erik Gustav Inge Dahlberg	Gamla Herrviksnäsvägen 57	Värmdö	
5.	1936-05-10 (78 år)	Helena Kristina Dahlberg	Gamla Herrviksnäsvägen 57	Värmdö	
6.	1937-11-09 (76 år)	Pekka Salomo Kurttila	Gamla Herrviksnäsvägen 91	Värmdö	
7.	1942-02-20 (72 år)	Åke Edvard Cederborg	Gamla Herrviksnäsvägen 107	Värmdö	
8.	1942-09-24 (72 år)	Eva Julie Widell	Gamla Herrviksnäsvägen 85	Värmdö	
9.	1942-11-25 (71 år)	Nils Gunnar Widell	Gamla Herrviksnäsvägen 85	Värmdö	
10.	1943-10-01 (71 år)	Ingela Anita Thalén	Gamla Herrviksnäsvägen 55	Värmdö	

FÅ PENGARNA TILLBAKA
OM DU INTE VINNEN.

betsson

11.	1943-10-06 (71 år)	Ida Agneta Kurttila	Gamla Herrviksnäsvägen 91	Värmdö	
12.	1944-06-27 (70 år)	Lars Gunnar Thalén	Gamla Herrviksnäsvägen 55	Värmdö	
13.	1948-05-26 (66 år)	Ulf Åke Staaf	Gamla Herrviksnäsvägen 39	Värmdö	
14.	1961-01-10 (53 år)	Helen Elisabeth Aresik	Gamla Herrviksnäsvägen 29	Värmdö	
15.	1962-10-28 (51 år)	Jan Olof Olsson	Gamla Herrviksnäsvägen 46	Värmdö	
16.	1963-08-25 (51 år)	Rose Marie Cederborg	Gamla Herrviksnäsvägen 107	Värmdö	
17.	1966-05-22 (48 år)	Michel Lars Torsten Adeheimer	Gamla Herrviksnäsvägen 16	Värmdö	

Jan Olof Olsson

19621028-XXXX

Gamla Herrviksnäsvägen 46
139 40 Värmdö

Län: Stockholms län
Kommun: Värmdö
Församling: Värmdö

[Sök efter personer på samma adress »](#)

Ann-Marie Elisabet Olsson

19701210-XXXX

Gamla Herrviksnäsvägen 46
139 40 Värmdö

Län: Stockholms län
Kommun: Värmdö
Församling: Värmdö

[Sök efter personer på samma adress »](#)



Villafastighet,
bra

Gamla Herrviksnäsvägen, Stockholms län, Sverige
essen är ungefärlig



Obevakad
brevlåd, check....

Skuldupplysning

Via våra register kan du få veta om någon finns registrerad med en obetald skuld hos oss.

Betalningsanmärkning

Vill du veta om någon har en betalningsanmärkning ska du vända dig till ett kreditupplysningsföretag.

Kontakta vår kundservice

Vår kundservice når du på telefonnummer 0771-73 73 00. Du kan vara anonym och det kostar inget mer än ett telefonsamtal. Du behöver ett person eller organisationsnummer på den du vill fråga om. Har du inte tillgång till personnumret kan du kontakta Skatteverket. Organisationsnumret kan Bolagsverket hjälpa dig med.

Ta del av offentliga uppgifter

Den som vill ta del av offentliga inkomstuppgifter hos Skatteverket gör det lättast genom att kontakta vår skatteupplysning på telefonnummer 0771- 567 567.

Skatteupplysningen kan ge inkomstuppgifter för upp till fem personer. Det går också bra att besöka våra servicekontor för att få ut inkomstuppgifter.

- » [Personuppgifter hos Skatteverket](#)
- » [Servicekontor, besöksadresser](#)

Offentliga uppgifter

 [Lyssna](#)

I stort sett alla uppgifter som skickas in och registreras i Bolagsverkets register är offentliga. Det betyder att vem som helst har rätt att ta del av dem.



Brevia Mail AB

Postboxar sedan 1984

Sekretess

Det finns oändligt många anledningar till att hyra en postbox anonymt. Vi på Brevia tror på en mycket hög grad av personlig integritet. Det är ett av skälen till att du inte behöver legitimera dig vid Brevia. Det finns ej heller och har aldrig funnits några övervakningskameror i vår lokal. Uppgifter om dig som kund lämnas inte ut till någon ej heller några register. Endast person med tillgång till nyckel eller boxnummer och kod (som du själv väljer) har tillgång till din postbox.

För respektive kunds säkerhet lämnas post aldrig ut eller eftersänds utan att kund på detta sätt identifierat sig.

Vid beslut om husrannsakan av åklagare är vi dock skyldiga att lämna ut de uppgifter vi har kring en kund.

Untitled.pdf - Adobe Reader
Arkiv Redigera Visa Dokument Verktyg Fönster Hjälp

1 / 4 133% Sök



NYHET!
Vi kan nu erbjuda fribiljetter till skänetraffiken! De är giltiga för T/R resa inom skåne och till Köpenhamn! Priset är 400kr för 10st! Maila för mer info!

ID och KÖRKORT Säljes! Vi är den enda säljaren som har det fulla UV säkerhetsstrycket på våra SIS Bank ID kort!! Snabb leverans och enkel betalning via UKash!

OBS! OBS!
DET ÄR VÄLDIGT VIKTIGT ATT ÄVEN NI TAR BORT ALL MAILTRAFIK OCH UKASH KODER EFTER NI FÅTT BEKRÄFTELSE PÅ ATT BESTÄLLNINGEN ÄR MOTTAGEN!!!

För mer info kontakta fletch@countermail.com

ID/KÖRKORT

Create your own web pages in minutes...

HOME BESTÄLLA KONTAKTA



Lettiskt EU körkort - Detta kort ska du värdå polisen inte kan verifiera i en trafikkl Har ALLA Säkerhetsdetaljer som finns på Pris: 2000kr

Svenskt SIS bank ID (olika banker samt p väldigt länge och som har en bra trovärc använder för att kolla om ett kort är äk Pris: 2000kr

Skatteverkets ID kort med chip! Detta ID Det har UV detaljerna precis som våra SI Pris: 2500kr

Svenskt körkort (modellen som fanns t.o. Har fungerande UV och streckkod. Pris: 2000kr

Slovakiskt ID - Bra att använda för flykti kan kolla i register för att verifiera per lätt för dom att se om det är äkta eller Pris: 2000kr

Oppehållstillstånd ID - Perfekt för pag som ett äkta! Pris: 2000kr

Din våra kort:
ID korten har de säkerhetsdetaljer som syns under UV ljus vilket affärer ofta äkta ID. Körkorten har en fungerande streckkod på baksidan. Leverans sker

Start | Mina Favoritprog... | Falskleg - lars.m... | Dina glömda han... | ID-kapning Lars... | stjäl post - Sök... | Untitled.pdf - Ad... | 09:48

Till vad används mina uppgifter

- Hyra/Leasa/avbetalningsköpa bilar
- Beställer produkter i mitt namn mot faktura
- Tar lån i mitt namn via olika låneinstitut
- Beställer kreditkort i mitt namn
- Öppnar konton i mitt namn
- Hämtar ut förbeställda varor i mitt namn
- Kvitteerar leveranser till angivna adresser i mitt namn
- Adressändrar mig till annan ort, för att där i fred ta emot beställda varor i mitt namn
- CEO Fraud
- Styrelse engagemang

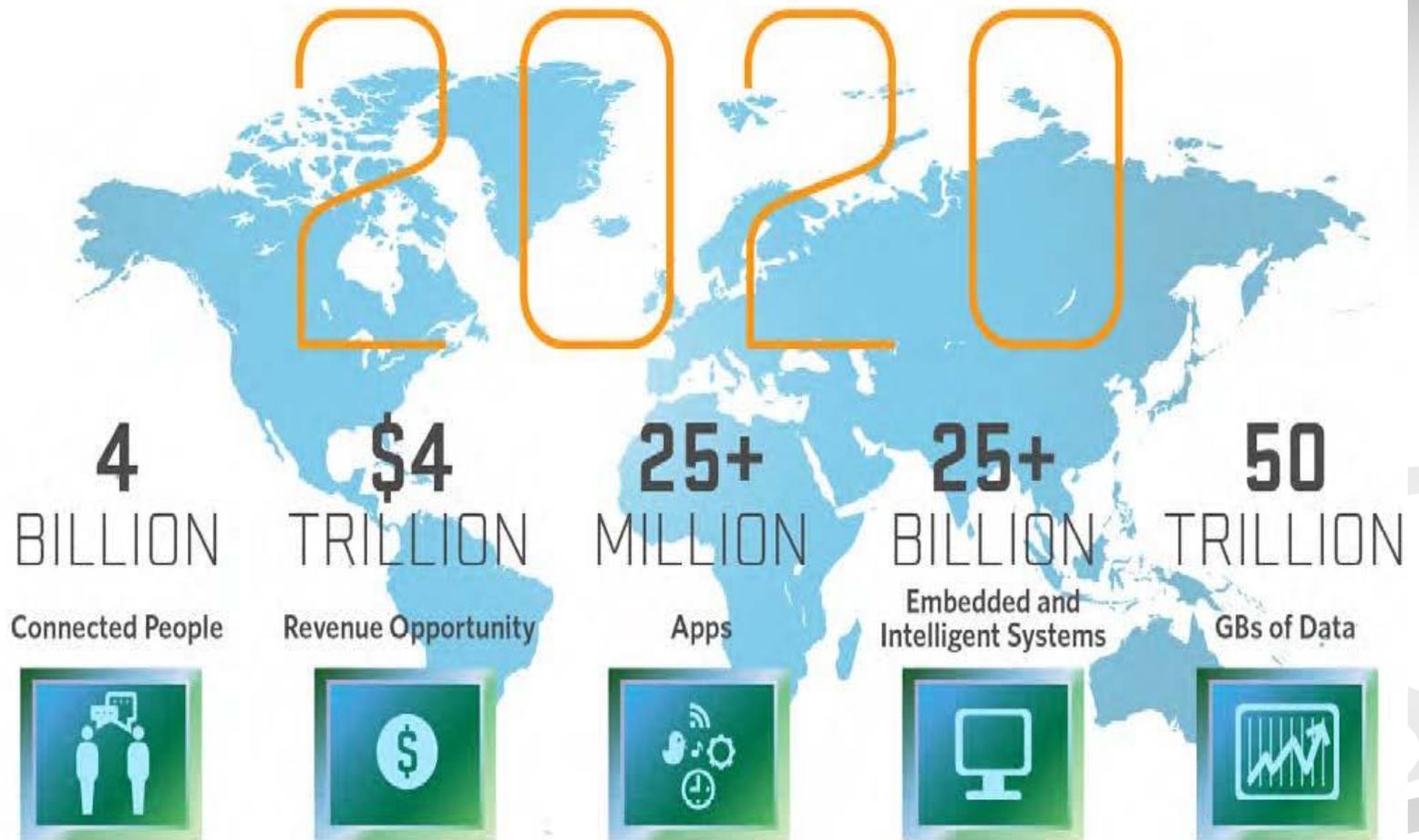
Eller rättare sagt, vad kan de inte göra ??

NFC-Near Field Communication /Tap-and-go



- Teknikval: Induktion eller radio
- Beloppsgränser

IOT



Source: Mario Morales, IDC

IOT

The first digital murder ?

Ok, dags att utreda

**Spear phishing, social engineering, Crime-as-a-service and more...
A case study**





Bad guy

*Hijacking a
facebook account*



mapping "friends"

Lisa

John

Stina

Anna

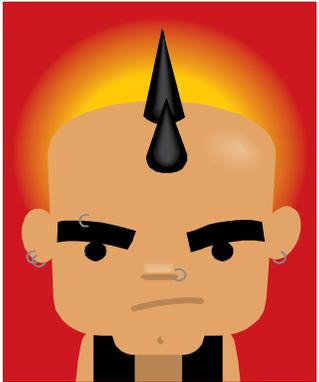
Sven



Everyday communication...



”friend”

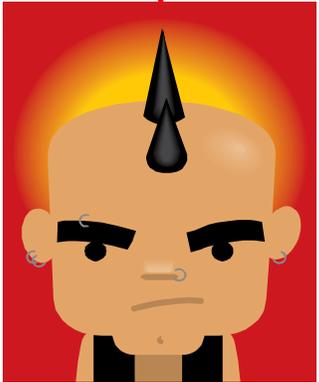


The friend hands over her login (digipass) details to the internet bank...



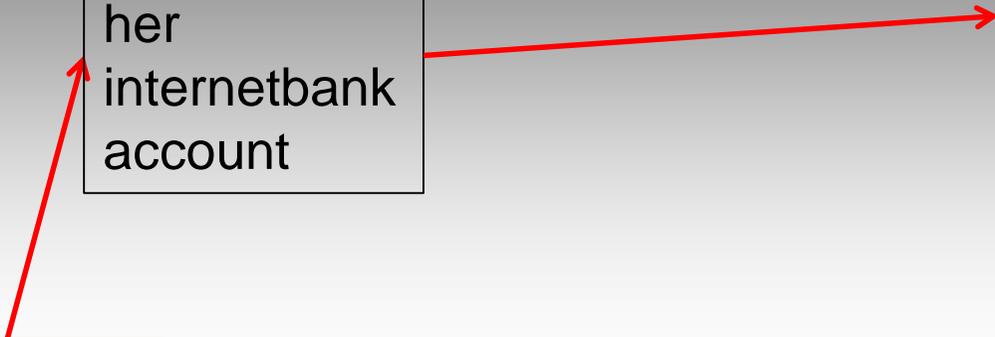
Access to
her
internetbank
account





Access to
her
internetbank
account

Swedbank Account
belonging to Trustly (3:e
party PSP)





Access to
her
internetbank
account

Swedbank Account
belonging to Trustly (3:e
party PSP)

Skrill account (Digital wallet)



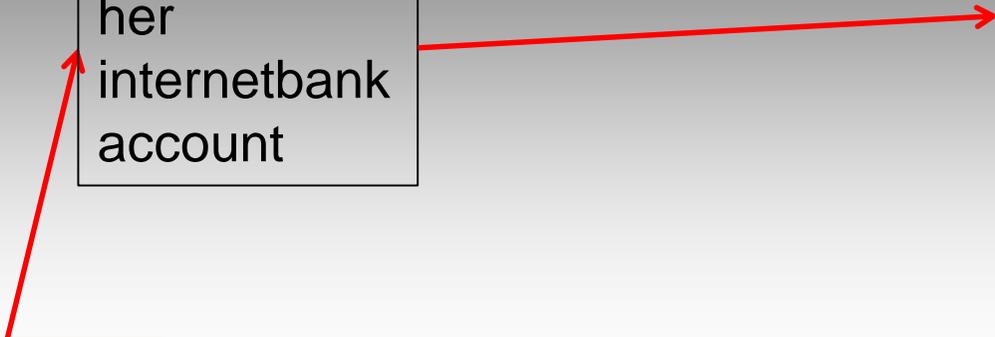


Access to
her
internetbank
account

Swedbank Account
belonging to Trustly (3:e
party PSP)

Skrill account (Digital wallet)

Another skrill account





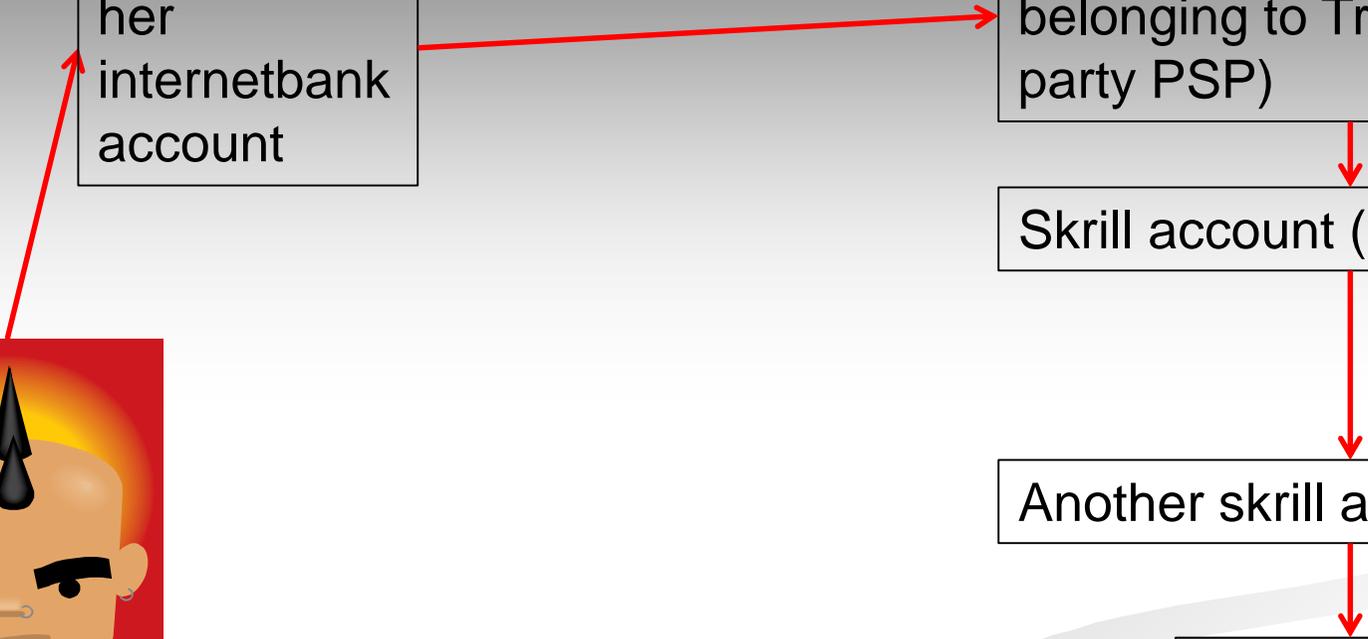
Access to
her
internetbank
account

Swedbank Account
belonging to Trustly (3:e
party PSP)

Skrill account (Digital wallet)

Another skrill account

Skrill prepaid
mastercard





Access to
her
internetbank
account

Swedbank Account
belonging to Trustly (3:e
party PSP)

Skrill account (Digital wallet)

Another skrill account

Skrill prepaid Mastercard

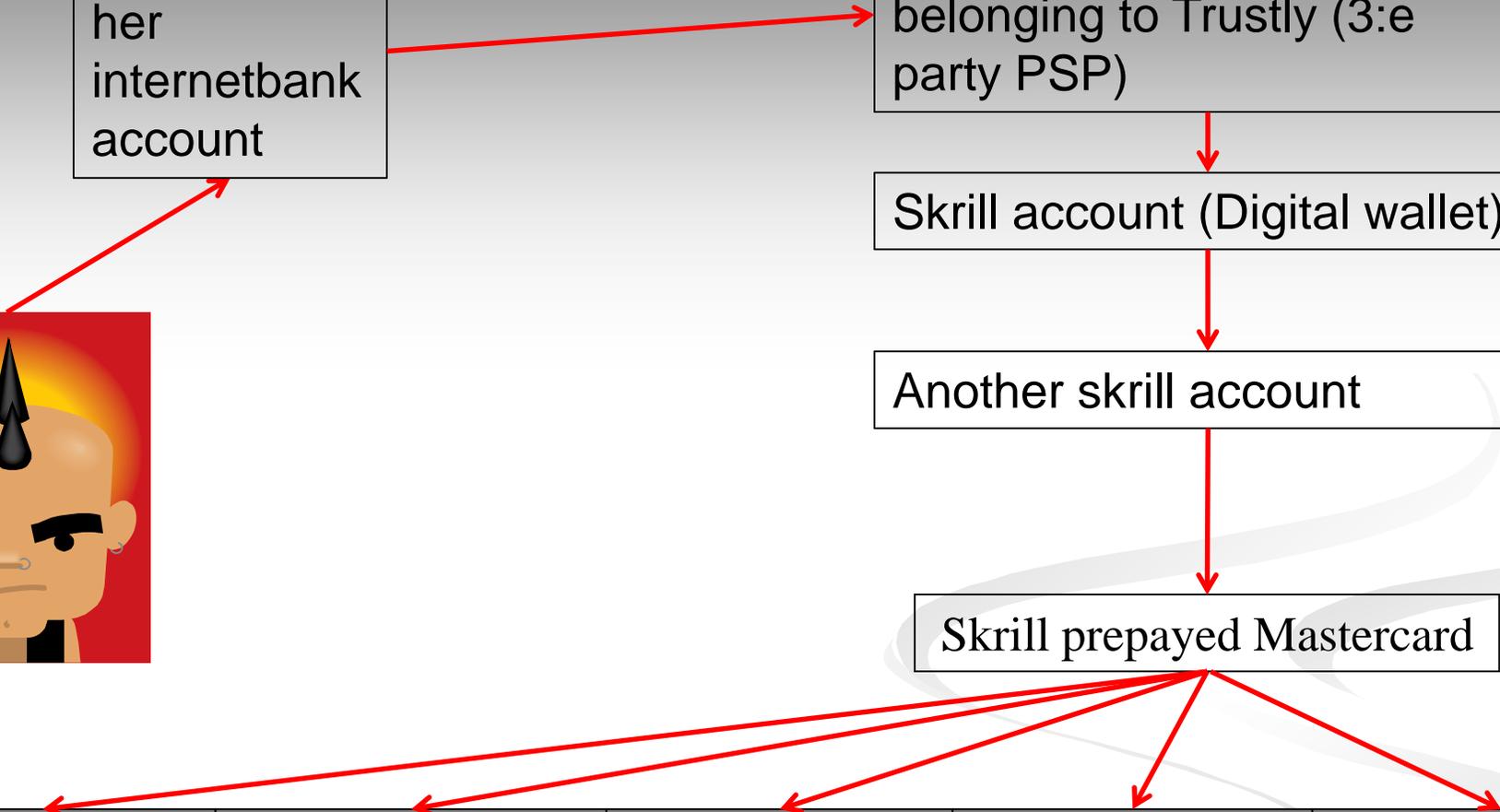
Cash out ATM
Venezuela

Cash out ATM
Frankrike

Cash out ATM
Serbien

Cash out ATM
Letland

Cash out ATM
Slovenien



That is a complicated road to travel...time to change direction. What do we know about the transaction and it's digital footprints?

The background of the slide features several thick, light gray, wavy lines that flow from the bottom left towards the right side, creating a sense of movement and depth.

Anonymus cashcard
dongle for Internet access

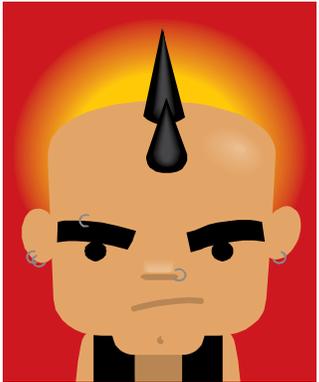




Anonymus cashcard dongle for Internet access



Anonymity service (VPN)

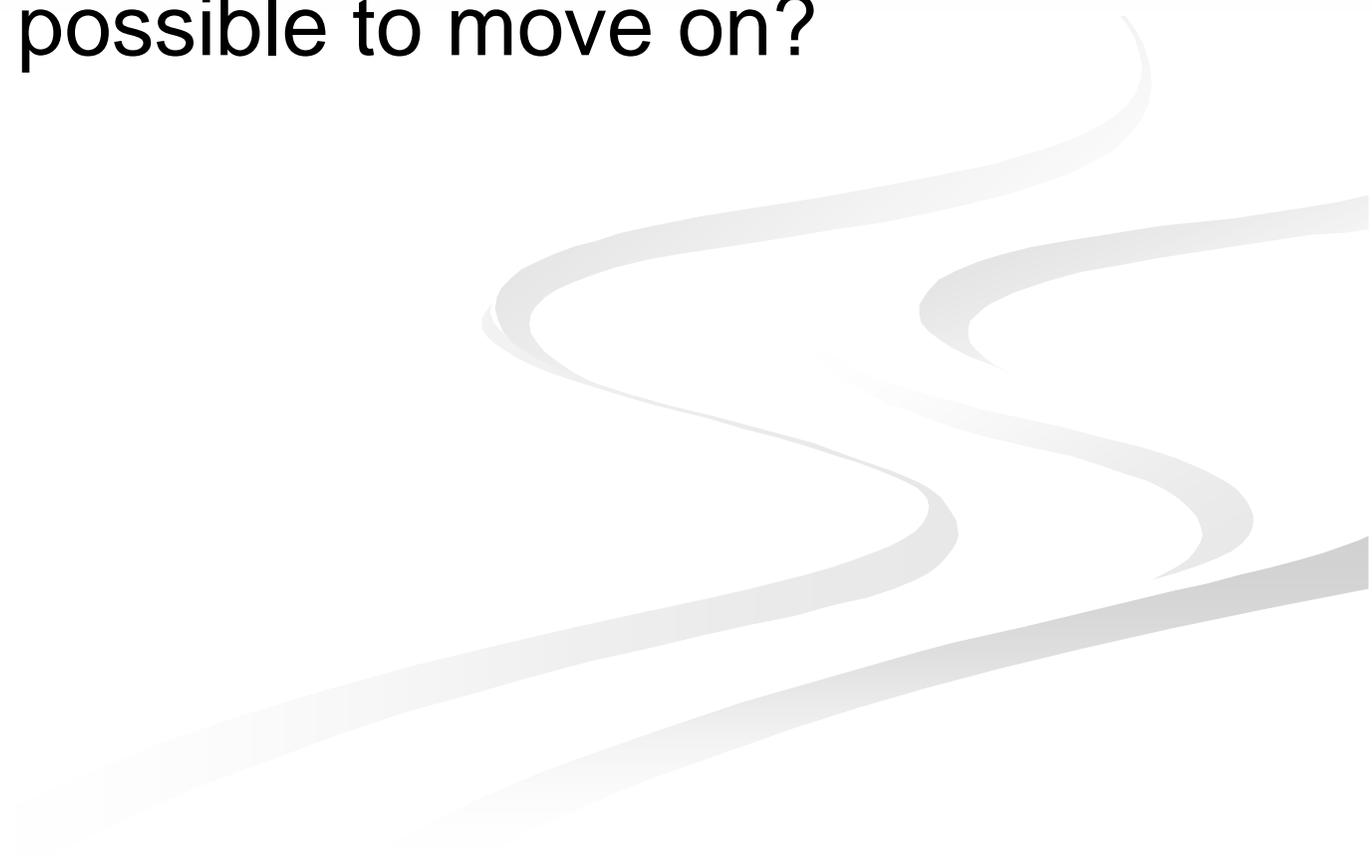


Anonymus cashcard dongle for Internet access

Anonymity service (VPN)

Botnet VIP72 (outside Moscow)

Is it even possible to move on?

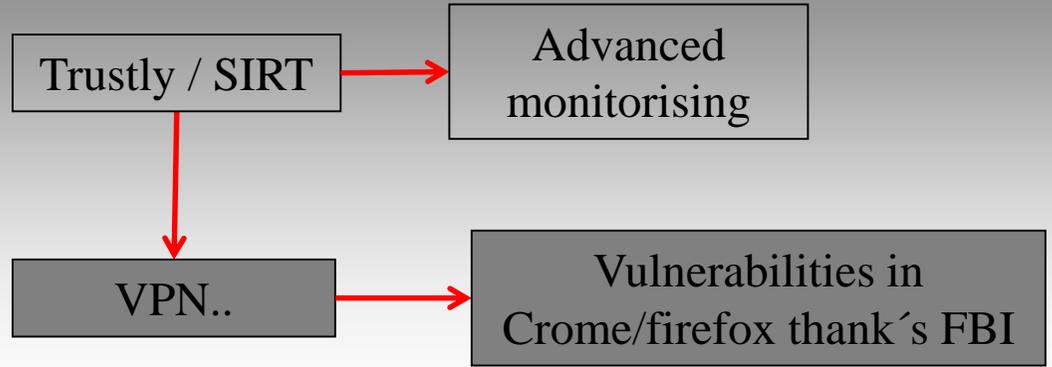


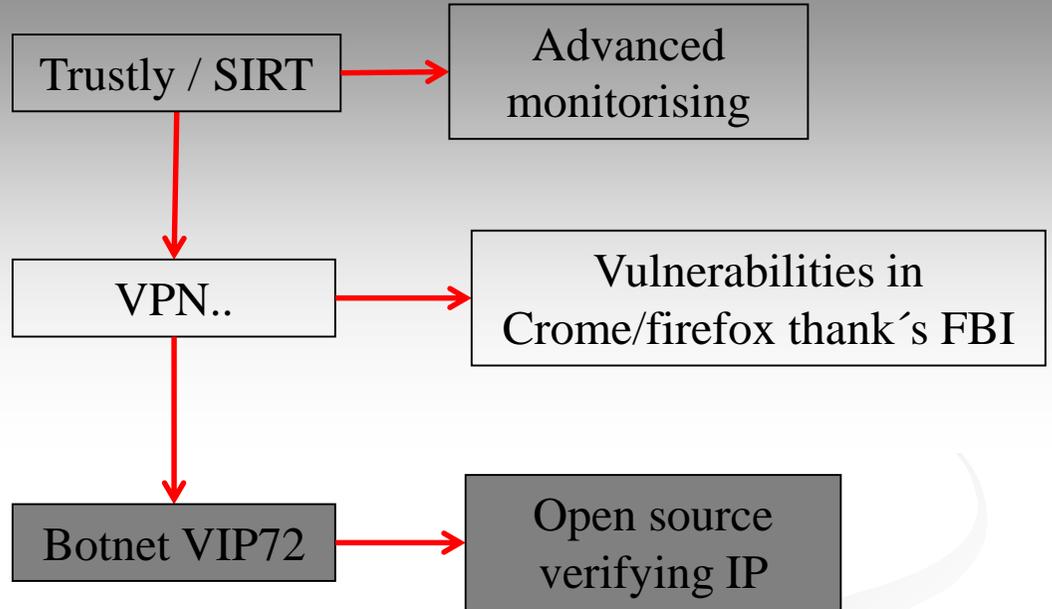
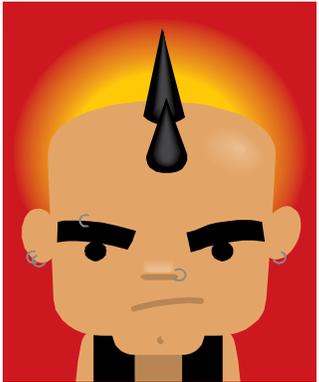
Trustly / SIRT

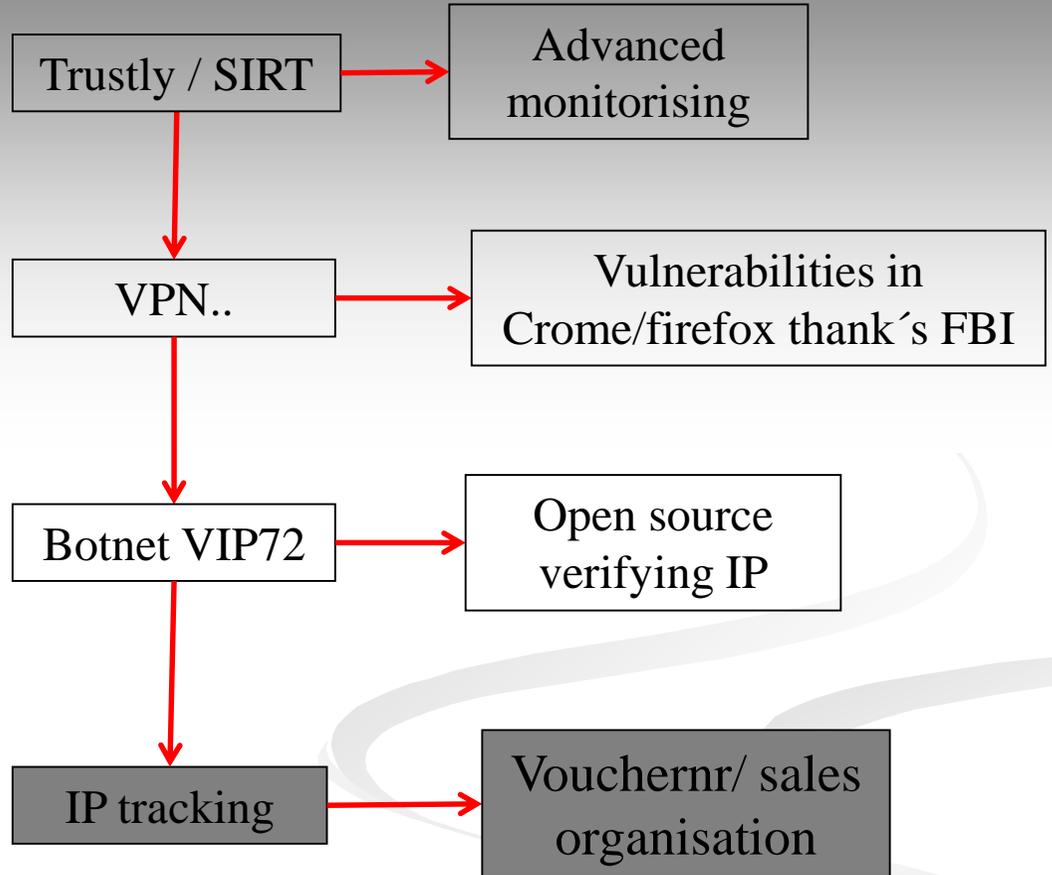


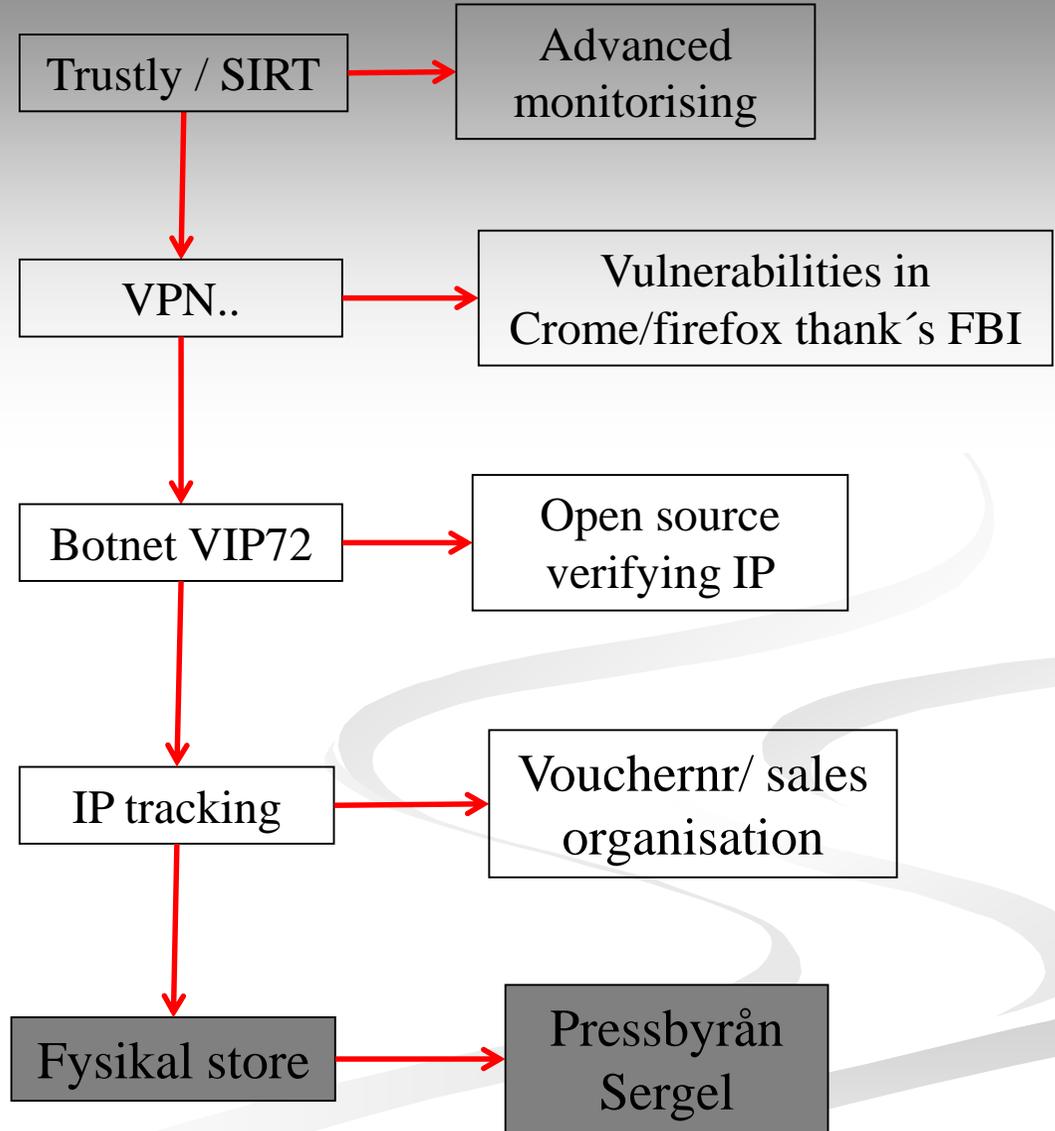
Advanced
monitoring











**Got you !
Nothing is impossible, or is it?**



Konsekvenser av utvecklingen

Hot:

- Hot mot det monetära systemet
- Samhällshot
- Lagstiftningsproblem

Men:

- För stora förluster ökar förändringsbenägenheten
- Politikerna agerar
- PSD2/GDPR

Jan Olsson
070-736 49 32