

SECURITY THREATS AND TRENDS

AUGUST 2007

SECODE AB

Secode helps companies and organizations gain insight, competence and thereby control over their operations from a complete IT security perspective. We deliver proactive and perpetual vigilance within two areas: 24/7 Managed Security Services and Security Consulting.

The Company was originally founded in 1986 as System Sikkerhet A/S, in Arendal, Norway. In year 2000, Secode AB was founded in Sweden and started its 24/7 Managed Security Services and Security Consulting. The two companies merged in January 2004, thereby forging the leading Digital Security Company in the Nordic region. In March 2006 the Finnish IT-security company Netsol OY (founded in 1996) was merged into Secode. From the first of January 2007 Secode has established sales-offices in both Denmark and The Netherlands and delivers IT-security services to customers in these countries as well. Secode helps many customers in private and public sectors, from seven different locations, using close to 85 security specialists. These specialists have long experience from building large computer networks and/or up-to-date IT security competence. Secode AB today has more than 100 employees.

All this together makes Secode the leading Northern European Digital Security Company within Managed Security Services combined with IT-Security Consultancy Services.

SUMMARY

After the large increase of traffic level last period, the traffic level this period is cut by more than half. VNC is still the most exposed service, and especially around July 7th this service was exposed. The decrease in searches towards VNC and MS SQL from last period is however huge. Among countries of origin it is also registered a large decrease from all sources since last period. The biggest decrease we see from China. Norway is once again among the top 10 countries, even though we see a decrease here too.

In the focus of the month this month we write about identity theft.

TABLE OF CONTENTS

INTRODUCTION	4
THREAT LEVEL	5
RECONNAISSANCE ATTACKS JULY 2007	5
TYPE OF RECONNAISSANCE ATTACKS.....	6
RECONNAISSANCE ATTACKS PR COUNTRY	7
INTERNET WORMS AND SPAM	8
ALERT STATISTIC	9
HANDLED ALERTS.....	9
REPORTED INCIDENTS.....	10
FOCUS OF THE MONTH – IDENTITY THEFT.....	11
WHAT IS IDENTITY THEFT?	11
WHY DOES IDENTITY THEFT HAPPEN?	11
NEW CHALLENGES	11
VALIDATION OF INTERNET SITES	12
HOW TO PROTECT YOURSELF FROM IDENTITY THEFT?	12
SOURCES	14

INTRODUCTION

This report is based on three main parts; Threat level, Alert Statistic and Focus of the Month.

Threat level is a presentation of what threats organizations are exposed to through their Internet connection. In this threat evaluation, reconnaissance attacks from the Internet against customers of Secode are analyzed and presented.

Alert Statistic is based on alerts from Secode's IDS and IPS tools. An alert appear when a sensor recognizes network traffic that fit the implemented signatures/filters, and in these cases alerts will be transferred to Secode SOC (Security Operation Center). All alerts, both false and genuine, are manually handles by analysts at Secode.

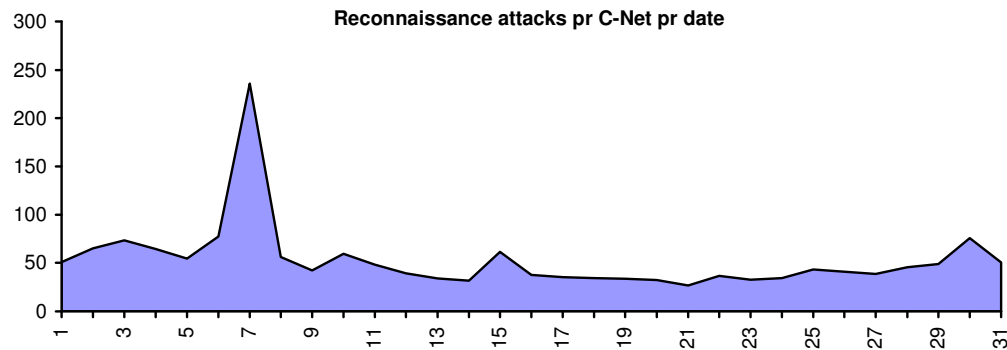
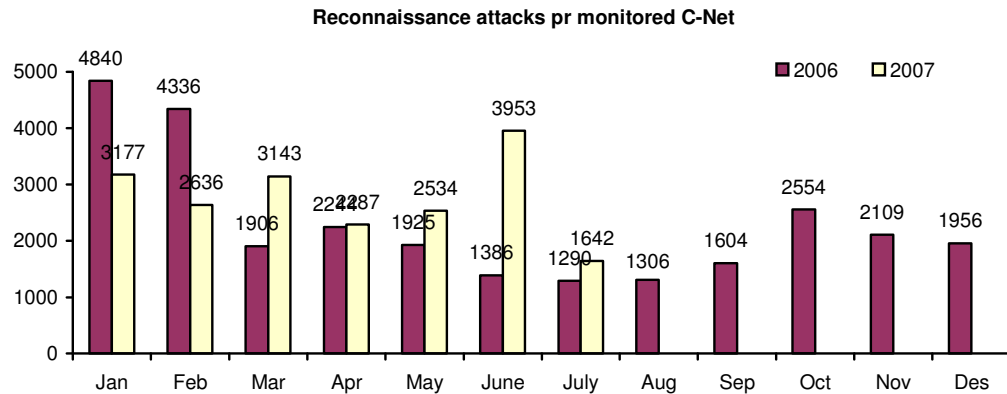
Focus of the Month is an article about relevant topics within IT Security. These might be topics discussed in media, incidents that can influence the threat level, or changes in the attack pattern from the Internet.

THREAT LEVEL

Due to high activity level, Internet worms and spamming are handled in a separate subchapter; "Internet worms and Spam", and are excluded from the other charts in this chapter.

RECONNAISSANCE ATTACKS JULY 2007

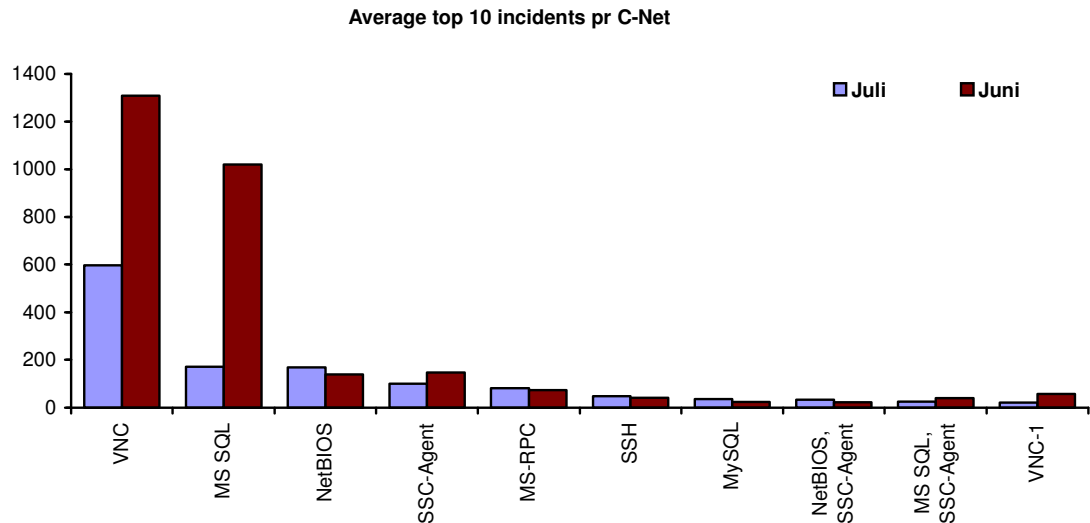
The statistics below gives an overview of the average number of reconnaissance attacks per network under surveillance. However, the activity level may vary from one network area to another. Despite these variations in the total activity level, we (mostly) register the same kind of attacks in different network areas.



The traffic level is decreased by half this period in comparison with last period, but is still at a higher level than the same period last year. The peak at July 7th is related to a great deal of searches towards VNC. There are several vulnerabilities that have become known in VNC and RealVNC during June and July, and they are most likely related to this.

TYPE OF RECONNAISSANCE ATTACKS

The diagram below contains a summary of the most common reconnaissance attacks during the last two months. The diagram does not separate scans for one single service from combined scans for several services.

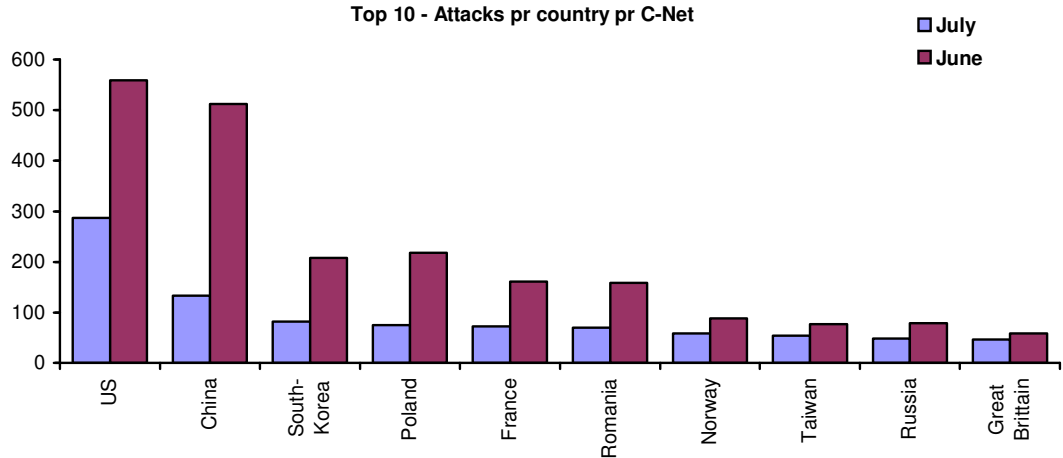


The decreases towards several of the services this period have been severing. The biggest decrease we find towards the services VNC and MS SQL. This can be related to the facts that no sever new vulnerability in VNC have been released this month, and that the new version of MS SQL has been known for a while. Searches towards VNC are still at the top, and the reason is that several critical vulnerabilities are public.

It is registered a small increase in searches towards NetBIOS, MS-RPC, SSH and MySQL. These increases are so small that they can be related to normal variations in the traffic level.

RECONNAISSANCE ATTACKS PR COUNTRY

The malicious activity in the statistic below is mainly automated attacks, which comes from infected computers (e.g. Internet worms or viruses). This means that most of the attacks are not directly aimed.



Among the countries of origin we also see decrease from all sources in comparison with last period.

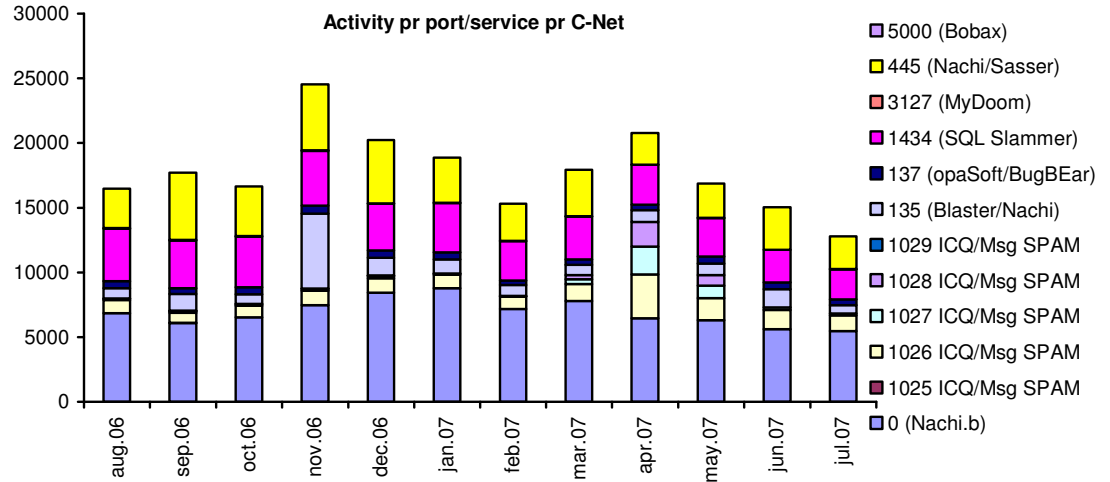
The biggest decreases we see from China, which almost were at US level last period, especially because of searches towards MS SQL.

Norway is now back among the top 10 countries of origin, after being out of the list for a while. It is still a decrease registered for Norway since last period. India and Brazil, which were among the top 10 last period, are now out of the list again.

The US is this month followed by China and South-Korea.

INTERNET WORMS AND SPAM

Because of a high level of activity against certain services, such traffic is presented in separate statistics. This applies for services most frequently targeted by Internet worms and spamming attempts.



We see a decrease in the worms and spam activity this period as well. It is mostly traffic towards port 1026 and port 135 that decreases. Towards port 137 however, we see a little increase.

ALERT STATISTIC

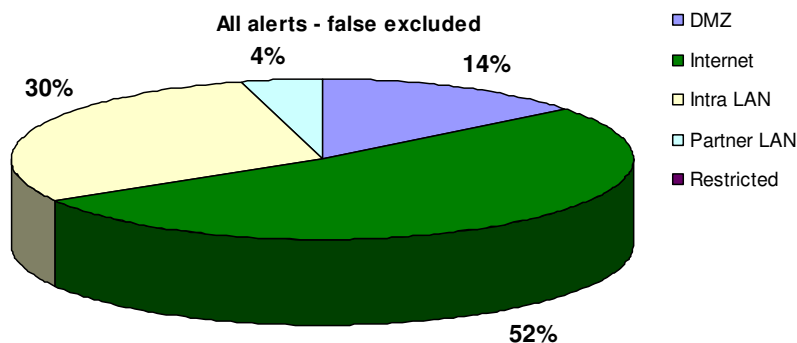
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

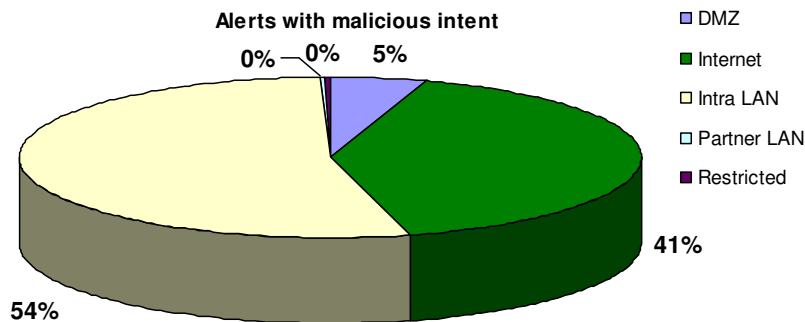
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

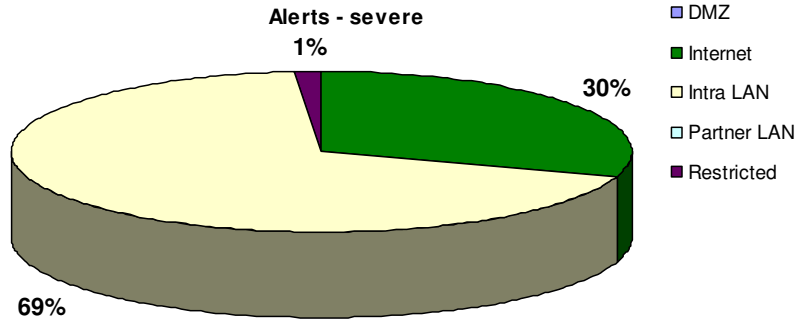
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located inside the network and monitors traffic between clients, servers and other network equipment
- Partner LAN: the measuring point is located in an environment that is used for communication towards external partners. The partner LAN is without Internet access
- Restricted LAN: the measuring point is located in a limited environment with a very well defined traffic pattern and without Internet access



The diagram above shows the distribution for all genuine alerts.



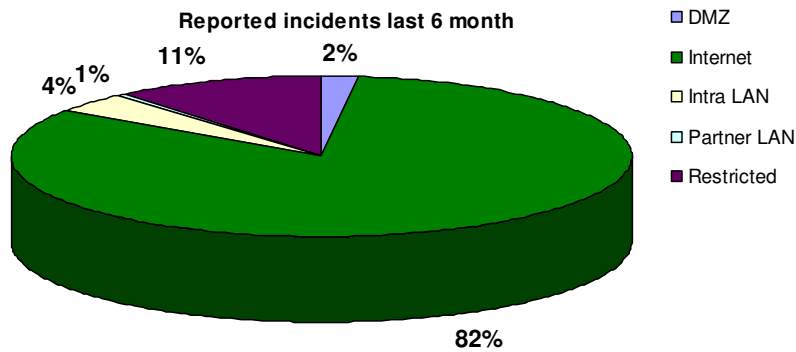
The diagram above shows the distribution for all alerts caused by activity with malicious intent, without the customer necessary being vulnerable.



The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

REPORTED INCIDENTS

The statistic below shows distribution of incidents reported to customers of Secode the last 6 months.



FOCUS OF THE MONTH – IDENTITY THEFT

The last couple of weeks the Norwegian social number system has been in focus. It has been known for a long time that it is relatively easy to find the social number if you know the date of birth and name or sex. Now, however, it has been put in context with the ease of getting more information through the Internet. And Internet also makes it easier to exploit the social number to perform an identity theft.

WHAT IS IDENTITY THEFT?

Some differences in identity theft definitions are available. In Norway the most used and well known is probably the definition of the Norwegian Data Inspectorate.

All situation were a person, without content from the person concerned, either

- Fully or partly is capable to perform some sort of unwanted transaction in another persons name, or
- Obtain access to resources belonging to others, or
- Unlawfully acquires rights belonging to someone else will be seen as identity theft.

The Norwegian Data Inspectorate

WHY DOES IDENTITY THEFT HAPPEN?

It is mostly financial gaining that is the motive behind identity thefts. By stealing a persons identity you can retrieve financial information, order credit card, raise a loan, change address and much more. You can for example get a credit card or raise a small loan in some other person's name, and you will get the money while the other person is run into debt.

Now, as it is possible to do most thing by internet, only by using the name and social number as an indicator, it is much easier for swindlers to exploit your social number to their own interest. In many ways you can say that identity thefts happen because it is easy.

Except for the financial gain it is also some identity thefts happening to bring harm or other unpleasantness to a person. Typical examples of this is the kind of identity thefts you see in American movies, where someone exploit some identity to revenge something, or maybe to protect themselves as they make it difficult for the other person.

NEW CHALLENGES

As previously mentioned it is a bigger chance of someone being exposed to identity theft today than it was some years ago. As more and more services are available through Internet, it becomes easier for a person to exploit other person's identity to their own financial gain. It is also easier to perform actions that make the other person suffer

Examples on services that can be executed on Internet and which can be misused are many. It is actually now possible to raise a loan, order a credit card and perform many banking services on net these days. A credit card company may only be asking for your social number, or your social number and your name. The name belonging to a social number is most likely possible to retrieve from some other Internet site. Some loan companies do not ask for more than social number either. You can also change address or redirect the mail to come to you instead of the real owner. Ordering of telephone services may also be done in others name.

During the last period it has become known that a 16-year old boy have made a program that can generate social numbers from the date of birth [1]. The program retrieves personal information from the Internet site belonging to the telephone-company Tele2. This program is available through Internet, and it makes it even easier to perform identity theft. This program and similar programs may be downloaded by criminals, which either use them for their own gaining or sell the social numbers they get to other criminals [2]. After this became known Tele 2 removed the feature that made it possible to retrieve personal information from their

sites [3]. But this program made it possible to retrieve more or less all information about a person that was born on a given date.

Phishing attempts towards online banking is not an unusual phenomena these days, and if you have access to a persons social number you also have access to a large part of the login information for the online banking service. Use of small programs or Trojans to steal login codes is also available for criminals, since several criminals sell such programs to other. This will then make it possible for someone to log into a given online banking service. All you actually need to know is which bank the owner of the social number actually is using, so that the program for reading login information could be adapted.

In other words, we can say that by retrieving a real social number, which is pretty easy to generate from sex and date of birth, a criminal can do a lot of damage. This creates new demands towards users and the systems of the future.

VALIDATION OF INTERNET SITES

When you retrieve a link on e-mail or you are surfing on the Internet, it may be difficult to know if the sites you are visiting are made be serious firms. In content with the protection of personal information on the Internet, it is desirable to validate that the site is genuine before you leave information there.

There are several methods to validate if the sites you are visiting are made by serious firms, or at least is not malicious. One of the methods available, which is not that popular yet, is the use of Extended Validation (EV) SSL certificates [4]. The idea behind this is more strict control of certificates combined with making it easier for the users to see the validation. If the site is related to an EV SSL certificate the address bar of the web-browser will turn green and the name of the certificate issuer will be available in the bar. The problem is that it is too expensive for small businesses to buy an EV SSL certificate.

Another method for validating Internet sites is to use the service McAfee SiteAdvisor [5]. A McAfee SiteAdvisors validation system is build on tests made by McAfee employees, and then categorizes it by the colours green, yellow and red. Green sites are serious sites, or sites with no malicious content. Yellow sites may contain spyware or similar, or a mail-form that leads to spam. Red sites are "malicious" sites. The categories may be influenced by feedback from other users as well. McAfee SiteAdvisor may either be downloaded as a plug-in to your web-browser (at least for Firefox and IE), or you can visit their site and get the report for other sites there.

HOW TO PROTECT YOURSELF FROM IDENTITY THEFT?

The discussion around the systems of the future is ongoing in Norwegian media nowadays, where many people believe that the Norwegian social number system must be revised. The social number should be more difficult to generate, and it should also be more difficult to relate the social number towards other personal information. New ways for Internet site validation is also under consideration at all times.

On a more personal level you can say that identity theft is a result of poor privacy. It is vital to not give away more information than highly necessary. This is not the first time Secode has written about privacy in some sort, but the media coverage of identity theft proves how important it is. We will here repeat some of our previously given advises, and bring some more general advises to the surface. We will also give some advises around discovery and fighting. All advises is build upon the list of advises at the Norwegian Data Inspectorate site [6].

Privacy advises:

- *Do not give personal information to unknown by telephone or through e-mail.* Remember that many e-mails may pass itself out as being from serious companies, even though it is other persons behind the e-mail. You should therefore never give away personal information through e-mail. This is especially important if the e-mail is retrieved by an online banking service. No Norwegian bank will ask for personal information by e-mail, and if you receive an e-mail from such bank you should delete

it. You may also contact you bank and tell them that you received an e-mail. The bank will then be able to warn their customers as soon as possible.

- *Do not give away personal information on Internet, if this is not a site you have initiated the traffic towards.* Be careful about which information you post, even though you have initiated the traffic. If this is a site asking for your e-mail address, you could use an anonymous or second e-mail address. This to avoid phishing attempts and spam.
- *Do not give away personal information to companies you know little about, or if you are uncertain about what the company will use the information for.*
- *All password and personal identification numbers are personal.* Make sure that you do not keep your passwords or personal identification numbers on places that other can get a hold of them and at least not nearby the system the password is meant for. Do not keep the PIN in your wallet with your credit card. It is best to either learn the passwords and personal identification numbers, or keep them in a password protected area at you PC or at your mobile phone.
- *Lock your mailbox if possible.* Lots of information about you is at all times available at your mailbox.
- *Shred documents which contain personal information before throwing it in the trashcan.* It is best if you can destroy it all together, but most of us do not have machines for destruction available at home. You should however always rip it apart.
- *Protect your PC.* IT security has become more important since more information is exchanged over the Internet or other network. To protect your PC use a firewall, anti-virus software and preferably anti-spy ware software. Many identity thefts are performed by using small programs or Trojans that steal information and report it the criminals behind the program. It is therefore highly important to protect your PC. We recommend that you also install all the patches for the OS and other programs, so that criminals may not use know vulnerabilities to enter the system.
- *Use advanced password.* Wherever you store personal information at the Internet, you should protect it with a password. The passwords should at lest contain letters and numbers, but to make it more difficult to brute force special characters may also be used. Do not use name and date of birth for some family member. It is easy to find how you are related to through Internet.
- *Check that a secure connection is used when transferring personal information.* Secure Internet connections are marked with a padlock either in the status bar or in the address bar of your web browser.
- *Be careful while using credit cards in foreign countries.* For Norwegians this is the most likely place to experience someone stealing your identity, and I guess this is true for several other Europeans as well.

Discovery of Identity Theft

It is many ways to discover an identity theft. The most important thing is to be on the alert and that you give notice whenever you discover something that does not seem right. For example if a transaction is made from your account and you can not remember you having made the transaction, contact your bank and explain the situation. The bank is most likely helpful in figuring out what happened.

Below we have listed some of the signs that could tell you that your identity has been stolen [6]. This list is retrieved from the Norwegian Data Inspectorate. If some of this happens to you, you should take an extra control on what has really happened. This to figure out it this is a real theft.

- You receive bills for products you have not ordered.
- You find unexpected transactions at your credit card bill
- You receive confirmation of credit or credit report without asking for it
- You receive warning about change of address without asking for it
- You receive a phone call or a letter about purchases you have not done
- You receive mail you do not understand the reason for; a bill, some agreement or similar.

- You should keep your receipts or in another way control your transactions from your credit card or other accounts.

If you are exposed to identity theft it is highly important that you contact the right persons as soon as possible. If it is a banking service that has been exposed, check with the bank that nothing more has happened. Be aware of other suspicious activity during the next couple of days. If the problem is with a change of address, contact the postal service and make them change it back. You can also tell them to not allow a change of address through Internet. The most important thing is that you limit the content of the theft, and get it under control as soon as possible. Report the theft to the police.

SOURCES

- [1] Dagbladet –"Lars" (16) kan tømme Folkeregisteret fra gutterommet
<http://www.dagbladet.no/nyheter/2007/07/29/507405.html>
- [2] Dagbladet – Personnummeret ditt videreselges av kriminelle
<http://www.dagbladet.no/nyheter/2007/07/31/507622.html>
- [3] Dagbladet – Systemet åpnet for svindel
<http://www.dagbladet.no/nyheter/2007/07/30/507495.html>
- [4] VeriSign – EV SSL Certificates
<http://www.verisign.com/ssl/ssl-information-center/faq/extended-validation-ssl-certificates.html>
- [5] McAfee – SiteAdvisor
<http://www.siteadvisor.com/>
- [6] Datatilsynet – ID-tyveri
http://www.datatilsynet.no/templates/article_1891.aspx