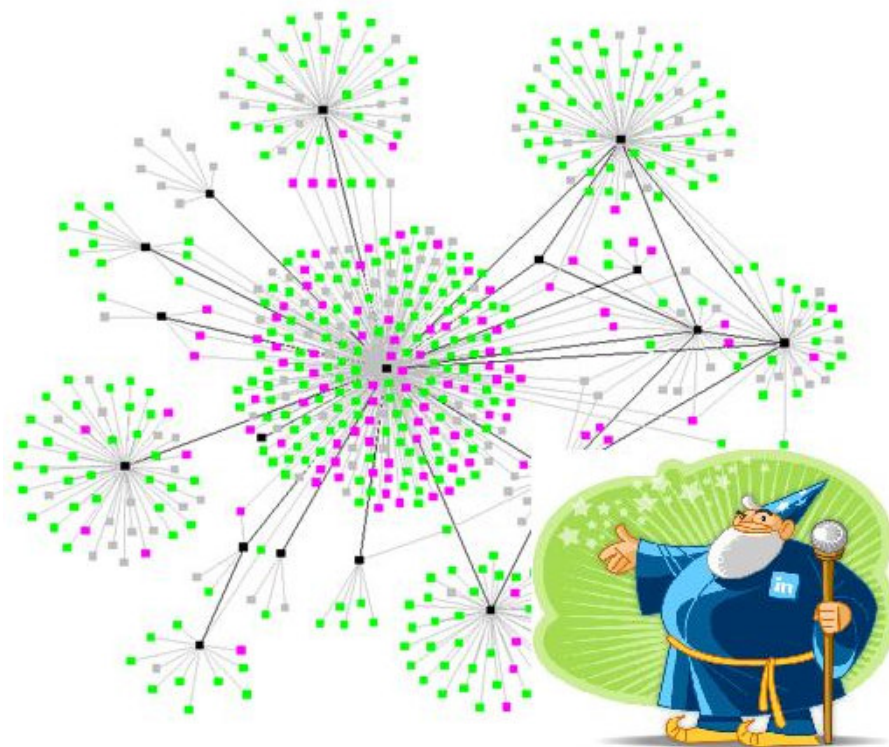




## CSIS Security Research and Intelligence

Research paper: Threats when using Online Social Networks

Date: 16/05-2007



Written by Dennis Rand  
rand@csis.dk  
<http://www.csis.dk>

---

### CSIS Security Group

A. P. Møllers Alle 11 • DK-2791 Dragør • Tlf. +45 8813 6030 • Fax +45 2817 6030  
info@csis.dk • www.csis.dk • CVR 29523355

## Table of contents

|  |    |
|--|----|
| Table of contents .....                                    | 2  |
| Introduction .....   | 3  |
| About CSIS Security Group.....                             | 4  |
| Social Networks - LinkedIn .....                           | 5  |
| Abstract .....   | 5  |
| Employees can bring client information if they leave ..... | 6  |
| Competitors use of your social network .....               | 7  |
| Hackers use of your Online Social Networks.....            | 8  |
| Building up a large network .....                          | 9  |
| Email harvesting.....                                      | 10 |
| Personalized malware and attacks .....                     | 11 |
| Information disclosure of products and vendor usage .....  | 12 |
| Conclusion.....  | 13 |
| Disclaimer .....   | 14 |

## Introduction

---

This research paper is describing some of the threats when companies or a private person uses Online Social Networks. However, in this report I will only look at LinkedIn.

Still, a lot of the problems described within this report are exactly the same in any Social Networking applications available on the internet.

*LinkedIn is an Internet social network service, used mostly for business connections. It has over 10 million registered users (source: LinkedIn)*

The threats when using Social networks are:

It can be used by competitors to gather information about your company's clients and who in the organization that could be interesting to contact.

It can also be used by Hackers to find information about your company.

It can be used by employees to bring client information with them when they leave the company.

It can and possible will be used in the future for more specific attacks, on specific companies or types of business.

## About CSIS Security Group

CSIS Security Group A/S is a privately held Danish IT security company originally founded in 1999. Today we employ more than 20 dedicated and competent people.

### Values

CSIS Security Group operates with a set of values describing our way to act internally, with our customers, as well as generally in the market. It describes our culture and is the very framework for our decisions and strategies and thereby supports us in all we do.

This set of values makes us capable of attracting and retaining some of the leading competencies within IT security. Our devoted staff and the company value set is the main reason why we keep strengthening our reputation as a trusted, loyal, and competent IT security advisor.

### CSIS Security Group product strategy

- CSIS Security group wants to offer the most extensive and cost effective IT security solutions in the Nordics. To reveal, document, and prevent security breaches for our customers. To support the IT security responsible with gathering and analysis of information to prevent IT related crimes and harmful user behavior.
- CSIS Security Group IT security solutions ensure that management as well as the technical staff has access to an updated overview of the current status, and documents governance and control of security exposures 24x7.
- CSIS Security Groups target is to be among the top 3 suppliers within standardized, stabile, and modular IT security products, while providing economies of scale through a central solution with the possibility for strategic outsourcing

The research paper was written by Dennis Rand at CSIS Security Group  
Questions should be directed to:

Dennis Rand  
rand@csis.dk

<http://www.csis.dk>

## Social Networks - LinkedIn

---

### Abstract

---

This research paper is describing some of the threats when companies or private individuals use Online Social Networks - however, we will only look at LinkedIn in this paper.

*LinkedIn is an Internet social network service, used mostly for business connections. It has over 10 million registered users.*

#### **Through your network you can:**

- *Find potential clients, service providers, subject experts, and partners who come recommended*
- *Be found for business opportunities*
- *Search for great jobs*
- *Discover inside connections that can help you land jobs and close deals*
- *Post and distribute job listings*
- *Find high-quality passive candidates*
- *Get introduced to other professionals through the people you know*

Source: LinkedIn website (<http://www.linkedin.com>)

The above can be abused by competitors to gather information about your company's clients and who in the organization to make contact with.

It can also be abused by Hackers to find information about your company.

The big problem with Online Social networks like LinkedIn is that the people using it are not aware of the threats that lie within. I will try to show some of the issues that you need to be aware of when employees in your organization are using services like LinkedIn.




Also remember that these issues are not only related to LinkedIn, but to most Online Social Networks.

## Employees can bring client information if they leave

Normally there is a policy or personnel contract mentioning that when an employee is leaving the company, it is not allowed to bring along any customer information, but when using LinkedIn or other Online Social Networking services, it can be hard to ensure that this does not happen.

As I see the trend, more and more people add their clients and business partners and friends to these networks allowing them to bring it everywhere, maybe not with that specific purpose when they start, but more because it is being so widely used.

One of the features in LinkedIn is the possibility to integrate it with Outlook; this allows a person to create a network from a list of all contacts that are located in a company's mail system.

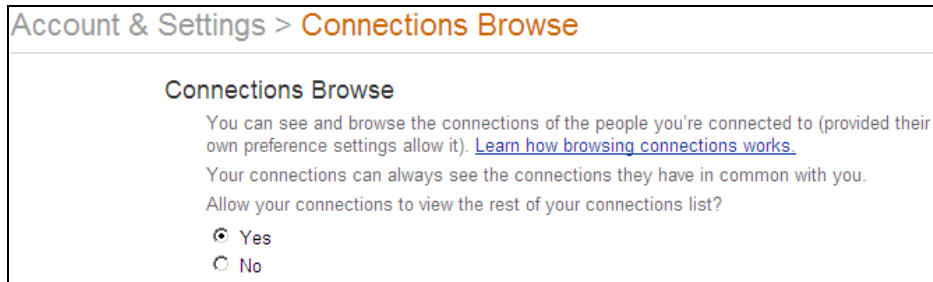
| Build your network from frequent contacts   | Manage your LinkedIn contacts in Outlook   | Stay connected to your network  |
|---|--|---|
|    |   |    |
| <ul style="list-style-type: none"> <li>• Build your network selecting from people you email often</li> <li>• See suggestions of who to invite based on email frequency</li> <li>• Invite with one click to build your network faster</li> </ul> | <ul style="list-style-type: none"> <li>• Update your Outlook contacts with LinkedIn profile information</li> <li>• Receive notifications when your contacts change their LinkedIn profiles</li> <li>• See when people you e-mail frequently are not in your network</li> </ul> | <ul style="list-style-type: none"> <li>• See LinkedIn mini-profiles for everyone that emails you</li> <li>• Use the LinkedIn dashboard to stay up to date with your network</li> <li>• Access LinkedIn with one quick and easy click</li> </ul> |

Because of this, companies need to take action against this and make a description in their contracts and/or security policy on how users are to use Social networks if at all.

## Competitors use of your social network

The use of Social Networks are getting more and more common around the world, and are used for keeping a list of clients, friends, co-workers and business partners.

LinkedIn has the option of allowing your current connections to view and browse all your current connections.

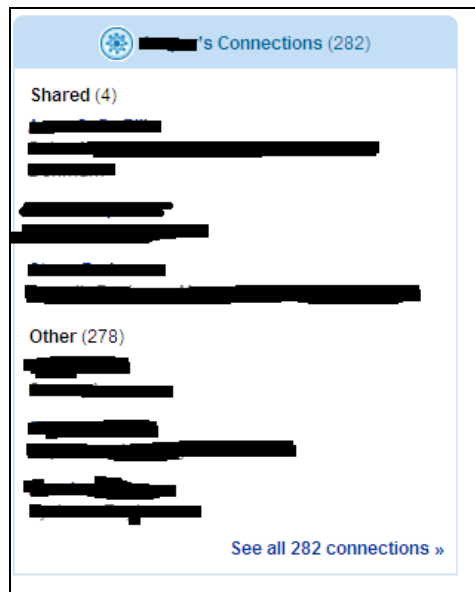


This is a default setting when you start using LinkedIn, so it has to be changed manually.

When looking through the list of connections 90% of people in my list allowed current connections to view all their contacts.

One of the best types of employees to get connected with are the sales people and management, since they are usually the ones who contact companies and not always think about the threats, so these people could pose the "biggest" threat when looking at the competitor "stealing" information through Social Networks.

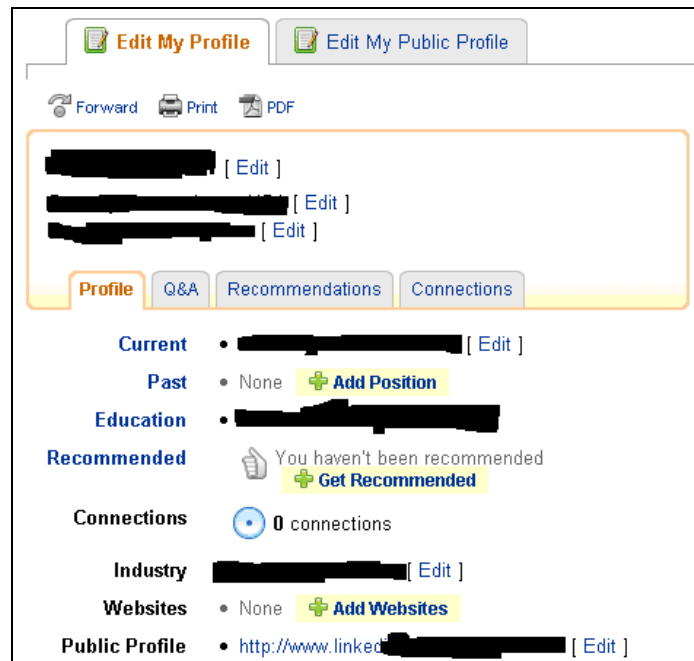
While using LinkedIn it was possible to gather a large list of potential companies and within these companies also contacts that could be used to get your foot in.



## Hackers use of your Online Social Networks

A hackers approach towards abusing LinkedIn would be for the purpose of gathering information, since in LinkedIn and any other Social Networking solution you can be whoever you want to be, or you can take the identity of whoever you want to be.

During this research paper I created a profile with a fake name, and an all in all fake profile, used an anonymous mail address that could not be traced back to me.



Profile has been hidden since I might want to use it in the future as well.

Another reason for not making the profile name public is to protect the people I have connected to.

Now that I had created an anonymous profile, I started building a "reputation", and finding the companies that I wanted to explore deeper.

Since the specific company that I wanted to gather information about does not have their email addresses made public anywhere, I added myself as a previous employee at the company, and used the feature in LinkedIn named "Invite Colleagues". Depending on the size of the company and how I introduced myself a lot of people accepted without any questions asked.

One of the things I experienced was that there were 5 people from that specific company that actually asked to be connected to me, and again I had never worked there.

## Building up a large network

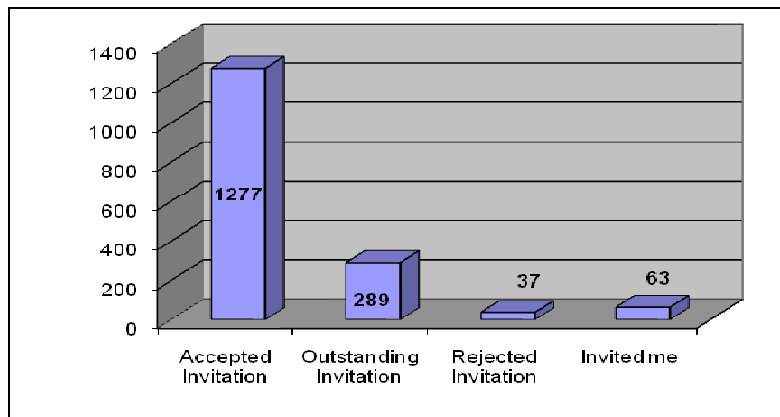
I sent out a base of 10 invites to people I had never heard of with my test person. From there on I used the contacts to get even more contacts through introductions, and also send more invites to people who had published their email addresses so it is shown to everyone.

Due to the fact that a lot of people make their email address public, it was possible to find the first **10 people** with public mail addresses.

Within **3 hours** I received the first acceptances of the invites I had send out to people I had no clue on who was.

After **3 days** I started to get invites from other people just trying to get their network to grow larger, so this also helped me getting an even broader network.

In less than **2 weeks** I had build up a network of **1300+** connections with email addresses, names and a lot of information about the different large companies.



The fact that I was able to build a quite large network of people with such a short timeframe actually surprised me.

Also when looking at some of the large companies that I connected to, and was able to see a lot of information about, people really doesn't think of the possibility that the information they put into their profile can be abused.

I would compare this to Google hacking, but with a new touch that hackers can use to get a lot more information on the internal infrastructure of companies.

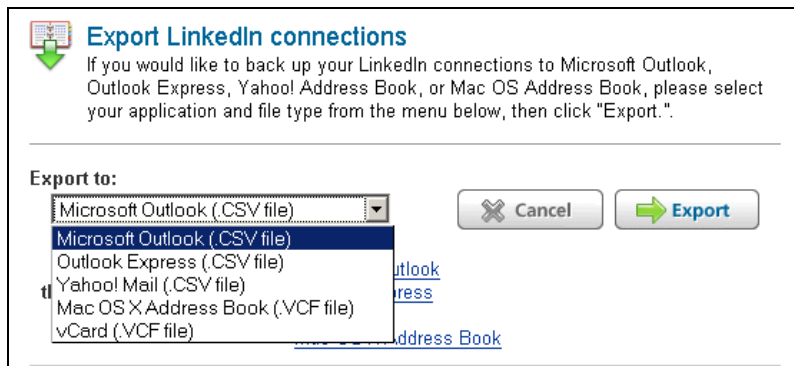
## Email harvesting

If you create an interesting profile, and through your profile appear to be a previous employee, then you can get a list of employees that you can send an invite to without having to know their email address.

The first few contacts are the "hard" ones to get, after that people can see that the identity that I created is already connected to someone within the organization, or some well known people they are more likely to just accept the connection.

During my research project I actually got contacted by 5 current and previous employees that wanted to get back in touch.

Now when you decide you have gathered enough information into your network, you can collect all this information in just one click.



## Personalized malware and attacks

I think that one of the more used ways in the future to distribute malware will be through more personalized or company specific attacks, the reason for this is to ensure a longer undetected life cycle of the specified malware or attack.

This way to attack corporations has already been used with vulnerabilities, and also in some situations malware, but there is no question that this would be a more effective way to attack specific networks.

**Scenario 1:**

A malicious person would use the contacts connected through the network and send mails that includes information available about the people in the network.

E.g.:

Hey Jack, We connect through LinkedIn and I wanted to send you this information.

Please view the attached file or download it from [www.xxxx.dk/myCV](http://www.xxxx.dk/myCV)

Best regards

John Doe

**Scenario 2:**

Publishing a question to specific groups within LinkedIn and add a link to a malicious website that would infect the user when they visit the website.

**Scenario 3:**

Add a link on my public profile to a website that could collect information on all the people visiting the website or add a malicious file for download calling it e.g. CV.exe describing it as a self extracting file containing a PDF with my CV.

## Information disclosure of products and vendor usage

Another security threat concerning Social Networks is that people put in too much information that can be abused by hackers to gain a rather large knowledge about the network and infrastructure.

Look for these types of employees since they are the ones that potentially could be connected with consultants, software and hardware vendors:

- IT-security employees
  - Firewall vendors
  - External consultants
  - Other software / hardware vendors
- Networking people
  - Hardware vendors
  - External consultants
- Infrastructure
- And a lot more

Also people who are working with the above often write what kind of Software and hardware they work with at the current place they are employed.

|   |   |
|---|---|
| <p>Currently working with IT Security:</p> <p>Firewalls<br/>Proxy servers<br/>Mail gateways<br/>AntiVirus<br/>Spam<br/>Encryption<br/>PKI</p> <p>OS:<br/>Windows 2000, Windows 2003<br/>Windows XP.<br/>Linux Red Hat, SUSE SLES</p> <p>Product Experience:<br/>Checkpoint,<br/>Cisco,<br/>BlueCoat,<br/>RSA Security<br/>Symantec,<br/>Trend Micro,<br/>F-Secure<br/>Exim,<br/>Spamassassin</p> <p>Linux Security Baselines<br/>Windows Security Baselines<br/>Disaster recovery guidelines<br/>Service Level Agreements</p> | <p>Management, Office &amp; QA Support Software</p> <p>Microsoft Office (Excel, Word, Access)</p> <p>Operating Systems/System Tools</p> <ul style="list-style-type: none"> <li>* FreeBSD (3 years experience)</li> <li>* Windows 95/98 (8 years experience)</li> <li>* Windows XP (5 years experience)</li> <li>* SMTP(Postfix) (2 years experience)</li> <li>* imap (2 years experience)</li> <li>* pop3 (2 years experience)</li> <li>* <b>spamassassin</b> (1 year experience)</li> <li>* cyrus-sasl2 (1 year experience)</li> <li>* clamav (2 years experience)</li> <li>* apache (2 years experience)</li> <li>* mysql (2 years experience)</li> <li>* postgresql (2 month experience)</li> <li>* rrdtool (1 year experience)</li> <li>* nagios (1 year experience)</li> <li>* snmp (2 years experience)</li> <li>* snort (1 year experience)</li> <li>* nessus (1 year experience)</li> <li>* radius (1 year experience)</li> <li>* squid (2 years experience)</li> <li>* pppd (2 years experience)</li> <li>* bind (2 years experience)</li> <li>* jail (1 year experience)</li> <li>* ftpd (2 year experience)</li> </ul> |
|---|---|

As shown in the above case I would have a really good clue on what these two companies use to protect themselves, and also what OS they have available and how long they have used it, without being connected to the user.

## Conclusion

---

The use of Online networking applications are becoming more and more popular, and should be described in the Companies Security policy, one in which social networks are allowed, and how these are to be used, to protect your company from information disclosure.

There are in short the following issues to be taken into consideration:

- People will write too detailed and possibly confidential information within their profile.
- People will allow everyone to see all connections made, again allowing possible confidential information to leave the company.
- Employees can bring client contacts with them, if they decide to leave the company, "without stealing any information" in the way we usually see; they have just connected to the clients.
- People will trust their connections and click on everything that they receive from these people.

So are Social networks like LinkedIn Good or Bad? Well that again all depend on the usage of it. I find Social networks to be a good thing as long as you remember that your information is to some extent public to the world, so beware of what you write about yourself and your company since this information can and properly will be abused.

Also when you accept connections ensure that people are who they say they are, and whether or not you really want them as a connection.

And last but not least ensure what your company security policy has rules on usage of Social networks for their and your security.

## Disclaimer

---

The information within this document may change without notice.  
Use of this information constitutes acceptance for use in an "AS IS" condition.

There are NO warranties with regard to this information.

In no event shall CSIS Security Group be liable for any consequences or damages, including direct, indirect, incidental, consequential, loss of business profits or special damages, arising out of or in connection with the use or spread of this information.

Any use of this information lies within the user's responsibility. All registered and unregistered trademarks represented in this document is the sole property of their respective owners.

If you use the above information you have to credit CSIS Security Group for the research.