# Security Threats

* Phishing

Phishing is a way to get the password out of the user. Typically it’s an email that looks legit or a pop-up window that wants you to put in another password. For example the way to hack Nem-id: have a keylogger on the victims’ computer, and make another pop-up window when the user has put in one of the code from his Nem-id paper. Afterwards the hacker has the username and password from the keylogger, and the victim will type the code from the paper in the new pop-up window the hacker has created.

* Niagara Letters

Niagara letters is the spam mail almost everybody gets. The letters typically says that you have inherited some money and all you need to do is to write your account number. Sometimes the email states that you have won a competition and now they need to send you the money, and again they need you credit card information.

* Fake helpdesk calls to users

This is the old school method. Somebody calls the staff at the company they want to hack.

The hacker then asks them a lot of questions and tries luring the passwords or important information out of the staff.

* Password attacks

Easy password

-When the hacker is trying to hack the computer using the most common passwords.

Typically something like this: 123456, 987654, password, abc123.

(if you are using one of these stop reading and change your password!)

Dictionary

-When the hacker is using a systematic hacking method. Dictionary only means the hacker is trying to hack the password with whole words from the dictionary and doesn’t use combinations or other sequences.

Brute-force

-Brute-force is when you calculate every possible combination.

It might take a very long time to crack the password.

The length of the password increases the time it takes to crack the password.

* Denial of service

DoS

-The main intent in this method is to make the machine or network resource unavailable to the user. This can cause a lot of different symptoms such as slow internet, problems accessing a site and so on. This method only uses one internet connection compared to the Ddos that uses several. Normally the hacker wants to fuck up the users RAM or CPU.

SYN flood

-SYN flood is when the hacker sends a lot of TCP packages to the user, typically with a forged ip address so it is harder to locate the hacker. Since the ip address is forged there will be no answer on the other side. This opens a lot of half-opened connections and every computer/server has a limit. Now the computer/server cant reply to legit request because the SYN flood has taken up all the space.

DDoS

-distributed denial of service is when the hacker creates a flood of unique ip addresses and makes them take up all the bandwidth. This is more effective since more computer can take up more energy. The hacker makes the computers look for a specific internet address, and this goes on and on.

* Worms
* A worm is a kind of virus or a sub-virus. The worm can access your computer and enable other malicious users to take control of your computer. The worm has a way of reproducing which can slow down your computer and force the computer not to respond. The worm can travel through the computer without any kind of help. The best known type will be the one travelling through most people’s emails. The worm will get into the contact list and mail itself or duplicate itself into many worms, which can lead to thousands of worms within hours.
* Virus
* A virus is almost the same as when it comes to humans. The virus attaches itself to the victim, and typically stays hidden in some file. The Virus often can’t spread unless there is human interaction. The virus can potentially destroy your software and hardware or files!

The virus infiltrates the computer and can also go through the email and spam your friends or acquaintances.

* Trojan horses
* Just like the mythical story about the Trojan horse…

The Trojan horse will infiltrate the users system looking like a legit and healthy program. This kind of virus does not replicate itself as the virus and the worm. Often the user will install a program not knowing it’s a Trojan. The worst Trojans will destroy your files although some of the Trojans only fiddle with your desktop adding icons or some other useless thing.