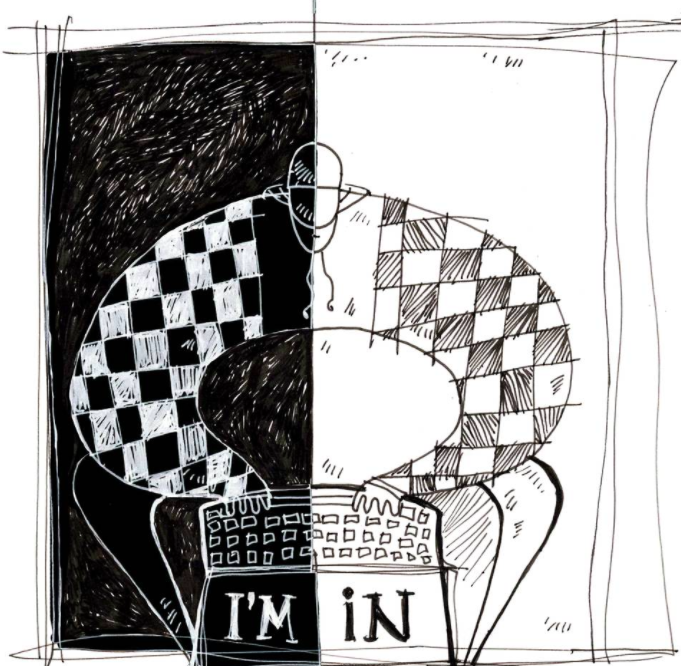
****

**Danish IT Company invents new technology against hacker attacks**

The Danish IT company Linkfactory has invented a new technology which will make it more difficult to be a hacker. According to them, the technology would, for example, have helped the Danish military to defend themselves against attacks from the Russian hacker group Fancy Bear.



**Ole Brockhuus and Annesophia Yttesen have invented the app SpotTheSpy. They run the IT consultancy house Linkfactory, which produces web, app and systems development for public organizations and private companies such as Fitness.dk and Molio. Illustration: Jyllands-Posten**

A few years ago, Annesophia Yttesen experienced that the chairman of the board of a child care centre kept sending her mysterious e-mails.

She wrote that she was in difficulties and asked for economic help from her friends and family. Her e-mail account had been hacked, but she was not aware of it.

This gave Annesophia Yttesen who, together with her husband Ole Brockhuus, runs the IT consultancy house Linkfactory, the idea for SpotTheSpy - a newly launched app which, via new technology, can give ordinary people extra protection against hackers.

The technology functions by crossing the GPS location from the individual user’s smartphone with the location from where the user’s Facebook or G- mail account is logged in from. In the future, it will also be able to connect to Linkedin, Instagram, and Twitter.

*“Studies show that half of the population are either worried or extremely worried about losing data when they are online.” Ole Brockhuus, director of Linkfactory.*

“*When the app has been installed we then always know where the user is located. If their Gmail or Facebook account is then accessed from another location, the app will send them a warning and give them the possibility of throwing the unauthorized user out, changing their access code or upgrading to a two-step verification*,” – says Ole Brockhuus, co-inventor of SpotTheSpy and director of Linkfactory.

The technology has not been seen before, and the company has received confirmation of this by the European Patent Organization. They now expect to secure an international patent in the course of September.

“*We can envisage this technology being used in a multitude of places in the future. We expect to have 100,000 users by the end of 2018. There are two billion Facebook users and more than a billion on Gmail, so there is extreme expansion in the areas we protect. Also, security is on most people’s minds these days - studies show that half of the population are either worried or extremely worried about losing data when they are online*,” says Ole Brockhuus.

More than 100,000 Danes have already experienced hacker attacks, where others have gained access to their e-mails or personal conversations on the Internet. Several companies have also been the target of global ransomware attacks, where hackers force access via phishing mails, encrypt the victims’ files and then demand a ransom for unlocking them.

The latest victim is Mærsk, and analysists estimate that it can come to cost them up to 450 million US Dollars.

The American streaming service HBO is also under attack, and is at present in negotiations with a hacker group who claim to have stolen unreleased episodes of series and scripts.

*“There are no current security methods that cannot be hacked.” Ole Brockhuus, director of Linkfactory.*

Linkfactory believes that its new technology can serve as an extra layer of protection for both companies and private individuals, and in the future they plan to roll out their technology for commercial purposes. They are convinced that their technology could, for example, have helped the Danish military, when in 2015 and 2016 they were attacked by the Russian hacker group Fancy Bear. The hacker group gained access to the Military’s network via the private e-mails of its employees.

“*If they had had access to this technology, which checks if the hacker is in the same location as the legitimate user, then they would have had better protection and would have been less vulnerable,”* says Ole Brockhuus.

The director of Linkfactory, Ole Brockhuus, explains that the technology should be put into play with other security layers, but that it is otherwise “Bulletproof”.

“*The hacker has to guess where the user is located to get around our technology, but one can never know which methods they make use of. We are well aware that when one comes up with a new security method the hacker will find ways to get around it. There are no current security methods that cannot be hacked. But our technology is still a good tool,*” says Ole Brockhuus.