Photo: Nammo

CYBERSECURITY RISK PERCEPTION

NorSIS
Norsk senter for
informasjonssikring

Responsible: Roger Johnsen
Writers: Bjarte Malmedal
and Hanne Eggen Røislien
Layout: Maria Nyheim
Photos: Maria Nyheim

Risk perception

Introduction

Risk perception[21] refers to the judgement that people make about the characteristics and severity of a risk. We are concerned with risk perception in our study, because we are faced with safety or security dilemmas every time we go online. Threats can manifest themselves in many ways, but we fail to comprehend the complex digital chain of events that may cause us to become vulnerable. Should you open the e-mail attachment? Will your posture on digital surveillance by the authorities really make you more secure, or will it cause you to be more exposed to cyber criminals in the long run? Do you accurately assess the risk related to your online activities?

Cyber security professionals often claim[22] [23] that people are lacking knowledge on cyber risks, or that they are naïve[24] [25] and unaware.[26] In the wake of large security breaches, it is not uncommon to see it explained by “the human factor”. People get blamed for making wrong choices, due to misinterpretation of the risk associated with their actions. In the wake of such incidents, we often see that educational programs and awareness campaigns are put in place in order to prevent future incidents.

Risks, especially complex risks which contains a considerable human element, can be based more on our personal judgement rather than scientific calculations. A risk judgement can be influenced by a large number of factors, each of them changing from day to

[21]: http://heatherlench.com/wp-content/uploads/2008/07/slovic.pdf

[22]: http://www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf

[23]: http://blog.trendmicro.com/trend-micro-lack-security-awareness-reason-high-number-cybercrime-victims/

[24]: http://www.welivesecurity.com/2016/01/29/businesses-still-naive-risks-cybercrime/

[25]: http://www.fin24.com/Tech/News/Young-people-more-naive-on-cyber-security-20151006

[26]: http://www.businessinsurance.com/article/99999999/

day, or situation to situation. Facts and knowledge may play a large part in the judgement, but so does experience, how “risky” we feel that day or if you generally are a risk-averse person or not. What are the factors that influence that judgement, and what do we do when we are faced with risk situations? If the goal is to enable people to make better risk judgements, how should we go about that?

In this study, we are interested in different aspects of risk perception, and what factors that correlates with risk perception.

Our findings

72.1% of the participants of this study thinks that they expose themselves to risk when they are online, and most people think that the threat is external, e.g. that someone will do something to them, rather than themselves doing something to compromise their online safety.

Table 2: Perceived largest online threat. N=8166

WHAT DO YOU THINK IS YOUR LARGEST ONLINE THREAT?	%
That you will do something yourself that compromises your online safety.	24.1
That someone else will do something to you (e.g. hack a site where you have some personal information)	67.8
I don't know	8.2

Before looking into how the participants perceive risks associated with online threats, we asked whether or not they feel capable of assessing what is safe to do online. 61.1% of the participants think that they are able to do that assessment, while 23.5% say they don’t think they are able. 15.3% say they don’t know whether they can assess that or not.

We chose a number of online threats that most people are, or can be, exposed to. These are online fraud, identity theft, online bullying or harassment, destruction of information, malicious code and manipulation. We then ask the participants to rate how worried they are that those threats will happen to them on a scale from 1 to 5, where

1 is “Not worried at all” and 5 is “Significantly worried. When presenting the results, we aggregate the responses 4 and 5 into a category we call “Worried” and the responses 1 and 2 into a category we call “Not worried”. The response 3 is called “Neutral” in the following presentation.

HOW WORRIED ARE YOU THAT THE FOLLOWING WILL HAPPEN TO YOU?	Average (1–5)	Not worried %	Worried %	Neutral %	I don't know %
That my bank- or credit cards will be used in online fraud	3.5	20.2	51.3	27.1	1.4
That others will use my identity online	3.6	20.2	53.9	24.4	1.4
That I will be bullied or harassed online	2.3	61.1	17.2	19.6	2.2
That my digital documents or pictures will be destroyed or deleted	3.4	23.9	49.6	24.7	1.8
That a virus will infect my computer	3.6	19.0	56.5	23.2	1.3
That I will be manipulated to send sensitive information to someone	3.0	41.7	36.2	20.7	1.4

Table 3: Risk perception. n=8193

We create a visual representation of the average results, where a larger area means that the participants are more worried.

HOW WORRIED ARE YOU THAT THE FOLLOWING WILL HAPPEN TO YOU?
(1: NOT WORRIED AT ALL. 5: SIGNIFICANTLY WORRIED)

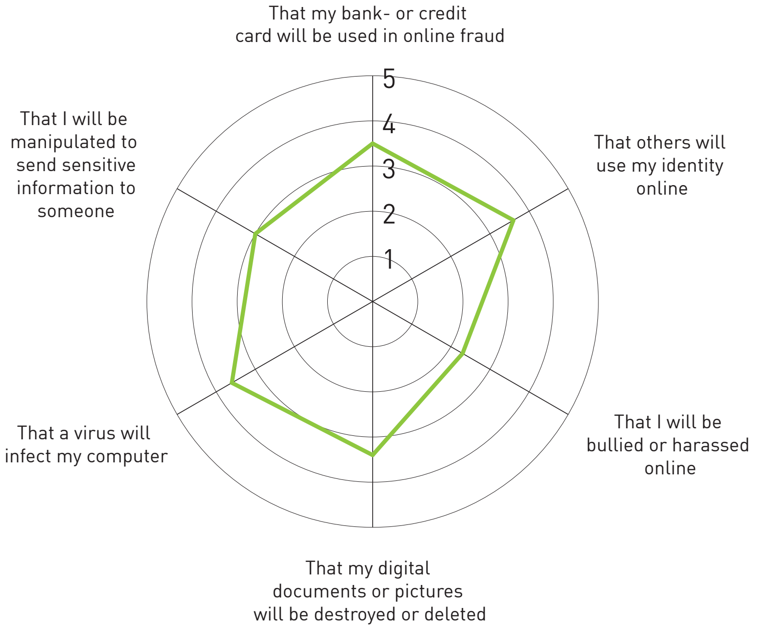

Figure 6: Average risk perception

Many cyber security educational programs aim to raise the awareness on digital threats. In this study, we do not find that those who had cyber security education during the last two years, perceive the threats differently than the group that did not have such education.

HOW WORRIED ARE YOU THAT THE FOLLOWING WILL HAPPEN TO YOU?
(1: NOT WORRIED AT ALL. 5: SIGNIFICANTLY WORRIED)

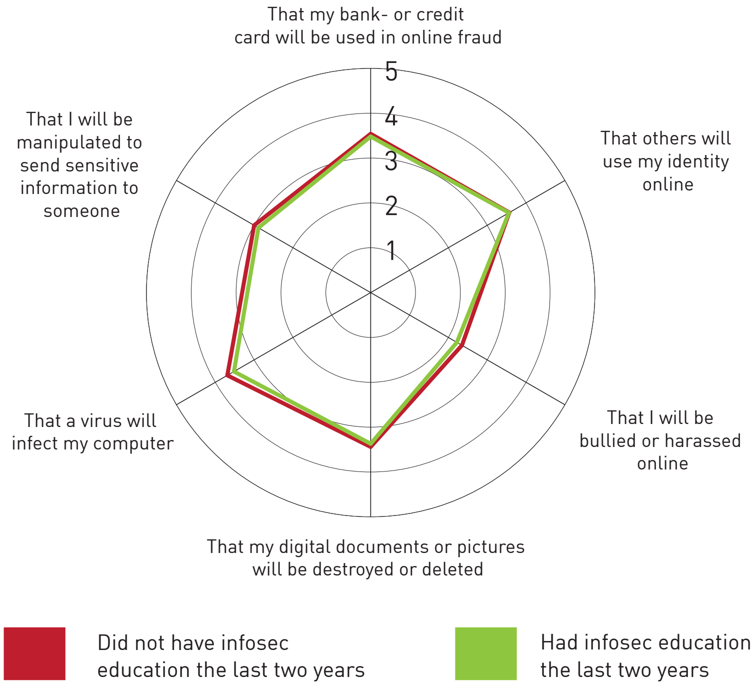

Figure 7: Average risk perception vs. Cyber security education

We do however observe a correlation between risk perception and confidence in the participant's ability to assess risk. In this study, we find that people who do not think that they can assess what is safe to do online are significantly more worried about the online threats.

This study has shown that an interest in technology and ICT plays a significant role in how and from whom people learn about cyber security. Interest could very well be a significant factor in how we perceive risk. However, we do not observe any significant differences between the group that is interested in technology and ICT, and the group that is not, with one exception. People who are not interested in technology and ICT are significantly more worried about malicious code (e.g. viruses) on their computer.

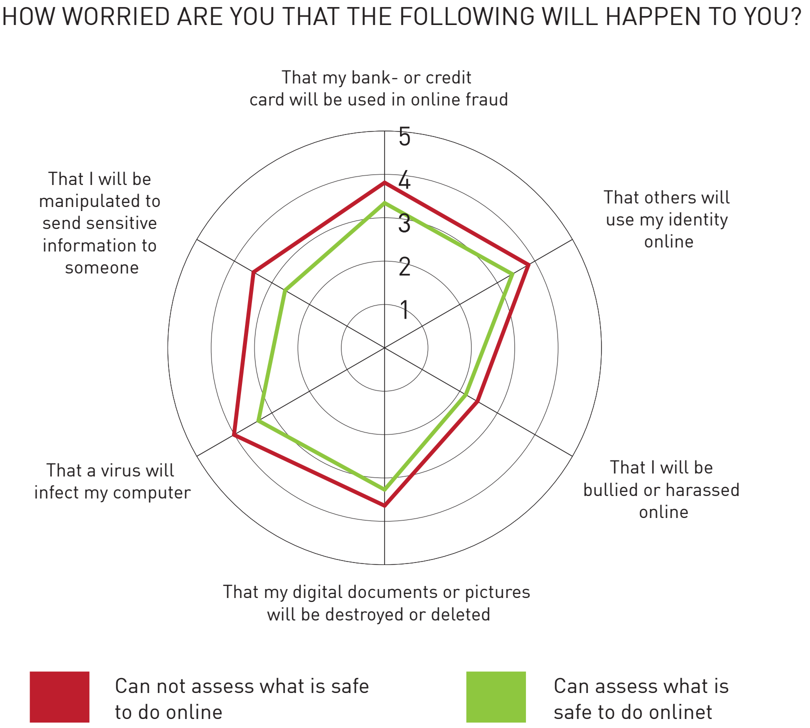

Figure 8: Average risk perception vs. Ability to assess what is safe to do online

Furthermore, we find that age also correlates with risk perception in this study. The older people are, the more they worry about the digital threats.

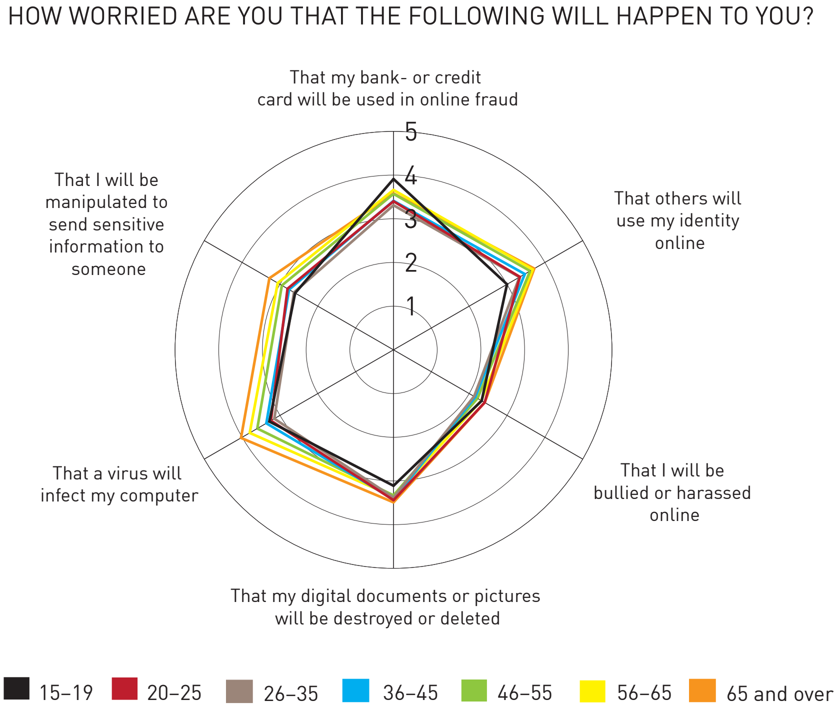

Figure 9: Average risk perception vs. Age

We also study how much risk the participants associate with activities most people engage in online. We ask the participants to rate how they perceive risk associated with the activities on a scale from 1 to 5, where 1 is “Not worried at all” and 5 is “Significantly worried. When presenting the results, we aggregate the responses 4 and 5 into a category we call “Worried” and the responses 1 and 2 into a category we call “Not worried”. 3 is coined “Neutral” in the following presentation.

Table 4: Risk perception in relation to online activities. N=8193

HOW WORRIED ARE YOU THAT THE FOLLOWING WILL HAPPEN TO YOU?	Average (1–5)	Not worried %	Worried %	Neutral %	I don’t know %
Using online banking	2.06	70.8	10.0	10.0	2.1
Using email	2.52	51.2	18.2	18.2	1.2
Sharing passwords with others	4.49	6.2	85.0	85.0	2.5
Using the same password at several online services	3.75	11.6	61.2	61.2	2.0
Using bank or credit cards online	2.83	33.0	36.0	36.0	1.5
Using online gambling	4.13	7.7	45.8	45.8	39.0
Using social media	3.04	27.5	30.4	30.4	6.5
Not back-up your data	3.92	11.5	63.1	63.1	7.1
Using public (government) services online	2.26	61.0	12.6	12.6	4.2

We create a visual representation of the average results, where a larger area means that the participants associate more risk to the activities.

We find that cyber security education does not play a significant role in how people assess the risk associated with the online activities. When it comes to interest in technology and ICT, we find some significant differences. The participants that are interested in technology and ICT, associate more risk to not backing up data and to use the same password at several online services.

We find that the participants who don’t think they can assess what is safe to do online, associate significantly more risk to the online activities. However, when it comes to the more technical activities, which coincidentally also are activities that they control themselves, there are no significant difference between the two groups.

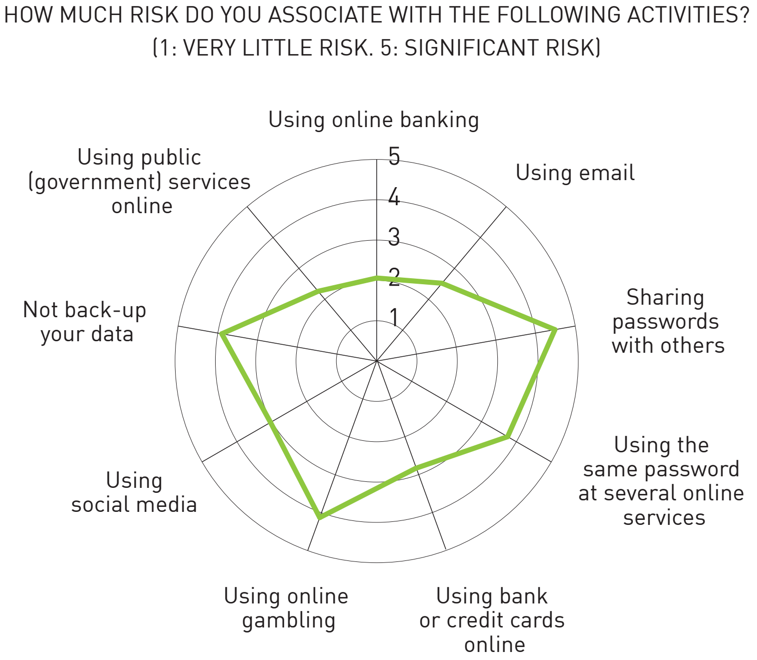

Figure 10: Average risk perception in relation to online activities.

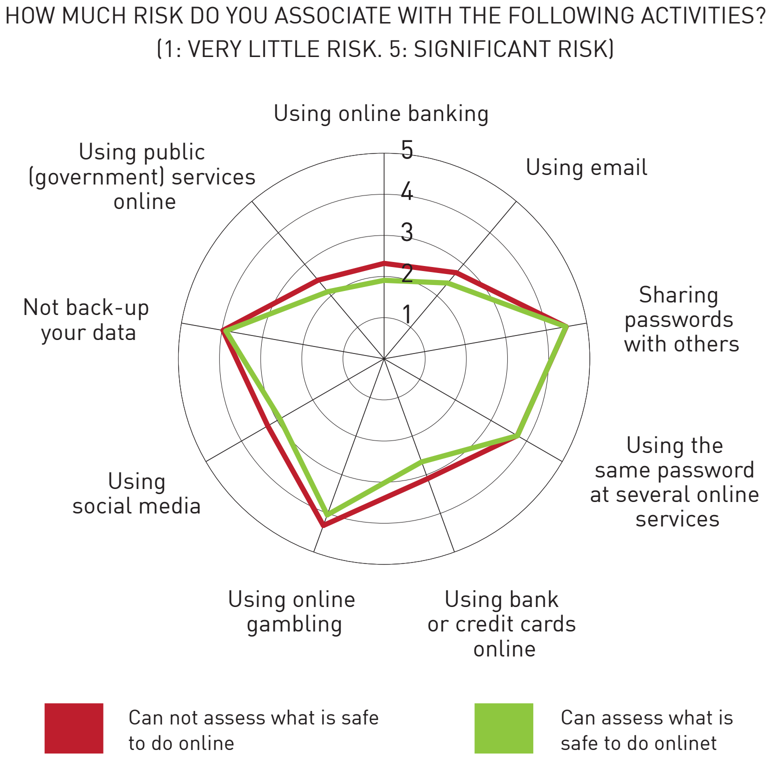

Figure 11: Average risk perception in relation to online activities vs. Ability to assess what is safe to do online

Assessment

The results are not interpreted according to their “correctness”. Risk perception is subjective in its nature, and there are factors that are likely to skew how we perceive the risks we examine in this study. An online bank may appear solid because we “know” they have vaults and other security systems in place. Our feelings about how secure a bank is, may affect how we think about online banking. In the same way, online gambling could be seen as less safe because there is already quite a lot of risk involved with gambling in the first place.

It is still useful to examine risk perception and how it evolves over time, how it changes when security incidents occur and how it relates to other factors. This study, then, can be seen as a baseline study for digital risk perception, and we will be able to discern trends when using the method over time.

We learn that cyber security education does not significantly change how the participants perceive digital risks. These results seem to be in conflict with how many cyber security professionals view the purpose of such education. The general idea is that education, the transfer of facts, about threats and vulnerabilities, will enable the students’ abilities to assess the risks. Subjective risk, however, is not based on careful calculations of facts and factors. Personal experiences, feelings, emotions and events in the recent past plays a much larger role in how we decide what risk we associate with different activities or threats. When cyber security education fails to affect how people perceive digital risks, the issue may very well be that the educational programs are using the wrong kinds of communicational methods or that the syllabus is inadequate.

We find that age correlates with risk perception, and that people worry more about digital risk as they get older. This may prove to be a troubling factor in the digitalization processes that are happening in both the private and public sector. The society expect the individual to be a part of the digital transformation, and how we perceive the risks associated with this transformation can affect the effectiveness of the transformation itself, or how we cope with it as individuals. If people think that some digital services are unsafe, they may very well refrain from using them. 44% of the participants in this study say that they have refrained from using an online service after they have learned about threats or security incidents. A recent study[27] by the US Department of Commerce National Telecommunications & In-

[27] https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

formation Administration corroborate these findings, and show that many Americans are deterred from engaging in important economic and civic online activities due to privacy and security concerns.

Risk perception also seem to be linked with how the participants think they can assess what is safe to do online. The people who think they can assess what is safe, tend to see online activities as riskier, though there are some exceptions. We find no differences when it comes to technical matters, such as not backing up their data, sharing passwords with others or using the same password on several online sites.