THE HAGUE UNIVERSITY OF APPLIED SCIENCES

nscr Netherlands Institute for the Study of Crime and Law Enforcement

How safely do we behave online?

A study of the relationship between knowledge, opportunity, motivation and the online behaviour of Dutch citizens.

SUMMARY

Dr. Susanne van ’t Hoff-de Goede

Dr. Rick van der Kleij

Dr. Steve van de Weijer

Dr. Rutger Leukfeldt

The Hague, 2019

Centre of Expertise Cybersecurity, The Hague University of Applied Sciences

Netherlands Institute for the Study of Ctime and Law Enforcement (NSCR)

SUMMARY

Background

Our offline and online lives are so intertwined that citizens in the Netherlands perform all kinds of online activities throughout the day. However, being online also presents dangers. Online crime is now common and its impact can be severe for victims. Cyber security professionals have tried to reduce online victimisation through technical measures, such as virus scanners and firewalls. These measures often only have a limited effect. To a large extent, victimisation can be traced back to the behaviour of people. After all, internet users click on a hyperlink when they should not, or enter personal data on a phishing[1] website, allowing criminals to misuse that data. In order to reduce victimhood, research into the behaviour of internet users is therefore essential.

Research objective and research questions

Knowledge about how citizens behave online and how they (might) defend themselves against online crime is scarce. To date, it is unknown in which ways Dutch citizens behave online and how they protect themselves against online crime, in part because how people *say* they behave online is not always the same as how people *actually behave* online. However, such knowledge is indispensable as empirical support for interventions aimed at influencing behaviour. It is necessary to gain greater insight into the ways in which Dutch citizens behave online and which factors are related to their behaviour. The aim of this research is therefore to discover how Dutch citizens behave online and to explain their online behaviour based on factors that have emerged from the literature, in order to take an initial step towards developing interventions that make Dutch citizens safer online. The main question of this report is: "How safely do Dutch citizens behave online and how can this be explained?" The following sub-questions will be answered in this report:

1. How safely do Dutch citizens behave online?
2. Is there a relationship between knowledge, opportunity and motivation?
3. Are there similarities between different online behaviours?
4. Can the online behaviour of Dutch citizens be explained by their knowledge of online security?

[1] Phishing is a form of online scam, in which criminals copy the e-mails or websites of legitimate organisations to mislead victims, in order to retrieve login details and gain access to online accounts.

5. Can the online behaviour of Dutch citizens be explained by their opportunity for safe online behaviour?
6. Can the online behaviour of Dutch citizens be explained by their motivation for safe online behaviour?
7. Can the online behaviour of Dutch citizens be explained by other factors?
8. Does the online behaviour of Dutch citizens differ between population groups?
9. Are the ways that knowledge, opportunity and motivation affect online behaviour influenced by other factors?

Research methods

Various methods were used to answer the research questions: a literature study, an experimental survey and an expert meeting. The research started with the literature study. The literature study was conducted to gain insight into existing knowledge about online behaviour, risk factors associated with being a victim of online crime and unsafe online behaviour, persuasion techniques and factors that are important for behavioural change.

Subsequently, a survey was developed based on the literature study and distributed with the help of a research panel agency. The final sample consists of 2,426 persons and is representative of Dutch society with regard to the characteristics gender, if they are employed (yes / no) and the province in which they live, but respondents are more often highly educated and, on average, they are older. We used a so-called "population-based survey experiment" (experimental survey). In the questionnaire, online behaviour was measured in two ways: 1) self-reporting – by presenting respondents with questions and statements, as well as vignettes; and 2) objective measures – while filling out the survey, respondents encountered (fictional) cyber risk situations, allowing the researchers to analyse how respondents dealt with these situations. These formed the objective measurements of online behaviour. The survey therefore provides insight into the extent to which people *think* they are behaving in a safe or unsafe manner and to what extent people *actually* display safe or unsafe online behaviour.

Finally, the first results of the analyses were discussed with experts from different fields during an expert discussion meeting. The purpose of this meeting was to start developing recommendations that would be useful in practice for preventing or combating cyber risks. The meeting was therefore preceded by a literature study investigating existing interventions that aim to bring about behavioural change. During the meeting, the results of the experimental survey study and the literature study on interventions

were discussed and the experts were able to critically reflect on the research methods used, the results and promising directions for interventions that ensure safe online behaviour.

Conclusions of the literature study

The purpose of the literature study was to explain how online behaviour has been researched and measured in previous studies. It was also examined which explanations for the display of unsafe or safe online behaviour were found in previous studies. First, the literature study shows that a risk profile for becoming a victim of online crime cannot be outlined based on personal characteristics or routine activities. A number of factors do, however, emerge that may be relevant to online behaviour and they have therefore been included in the current study. These factors are: age, socio-economic status, gender and family composition. In addition, it appears that research should focus on behaviour as a pillar for decreasing the risk of online victimisation, namely safe online behaviour. This is therefore the main subject of the current study. Furthermore, the literature study shows, on the basis of theoretical explanatory models (in particular the Protection Motivation Theory (PMT) and COM-B, in which knowledge, opportunity and motivation are central), that the extent to which people behave safely online depends on the capacities that people have to behave safely, the opportunity they have to do so and the extent to which they are motivated to behave safely. In addition, the theory points to the importance of self-control and earlier victimisation.

Finally, there are factors that were not derived from these theoretical models but that seem relevant to online behaviour: mood, fear of victimisation, type of device, time pressure and persuasion techniques. A person's mood can influence their decision-making and has an effect on the strategies they choose when making decisions. Fear of victimisation can have various consequences for online behaviour, such as avoidance behaviour but also taking fewer risks online. The device used to go online is also important. Devices that people use at home for online activities, such as a smartphone, tablet, laptop or PC, differ in a number of dimensions that influence online behaviour and can influence victimisation. Time pressure could also cause people to ignore signs (cues) that they are at risk, and thus make them take more risks. The persuasion techniques that cyber criminals use in their attacks also seem important. All factors that emerged from the literature study were included in the present study. The current study therefore investigated to what extent online behaviour can be explained by all of the above-mentioned factors.

Results and conclusions of the experimental survey

Research question 1: How safely do Dutch citizens behave online?

It was found that unsafe behaviour is highly prevalent. For example, nearly 90 per cent of respondents use a weak password, 40 per cent download unsafe software and about 30 per cent share personal information, such as their full name, date of birth, and email address. When respondents are presented with phishing emails, more than 20 per cent say they would click on the hyperlink or copy the URL to the web browser, thereby making an unsafe choice.

While the fact that citizens behave unsafely online is partly reflected in the analyses of self-reported behaviour, it becomes especially apparent during the objective measurements of behaviour. However, it appears that there are major differences between self-reported behaviour and objective behaviour. The objective measurements show that people behave even more unsafely than they self-report. Below, we briefly discuss the conclusions for each of the seven online behavioural clusters (use of passwords, saving important files, installing updates, using security software, being alert online, online sharing of personal information, dealing with hyperlinks and attachments in e-mails).

- *Use of passwords.* Respondents self-report that they use safe passwords. They score high on security when it comes to not sharing passwords with others and using difficult passwords. The objective measurements show a different picture: 89 per cent of the respondents used a weak password. Even if we only look at the respondents who indicate, at the end of the questionnaire, that they have chosen a password in the same way as they would normally do, it appears that more than 83 per cent use a weak password. If we look a little more broadly at the password behaviour of the respondents and take as a starting point that only the length of the password matters and we again only look at the group that indicated they had chosen the password in the same way, it appears that 51 per cent choose a password of seven or fewer characters.
- *Saving important files, installing updates and using security software*. Using self-reported data, it was measured how respondents deal with saving files, updating software and using security software. Of all seven behavioural clusters, respondents report, on average, the least secure behaviour in the area of file storage. In the area of updating software, a high (safe) score was reported on all propositions, such as installing updates on operating systems, apps/software and security software as soon as a new update becomes available.

- *Being alert online.* When we focus on being alert while being online, the same picture appears: respondents indicate through self-reporting that they behave (very) securely (for example not downloading from illegal sources, not using public Wi-Fi), while the objective measurement shows that 40 per cent of the respondents download unknown software if a pop-up appears while attempting to watch an online video.
- *Online sharing of personal information.* Concerning the online sharing of personal data, respondents indicate that they are aware of the dangers of sharing personal data such as a home address, e-mail address or telephone number and connection requests via social media. During the objective measurement, however, respondents often appear willing to provide (very) personal information. For example, a significant proportion gave their date of birth (37.5%), full name (31%), e-mail address (28.1%) and their postcode (27.0%) and street number (20.4%). A small, but significant, part of the respondents (4.8%) is also willing to enter the last three digits of their bank account number.
- *Dealing with attachments and hyperlinks in e-mails.* Respondents self-report safe behaviour when it comes to dealing with attachments and hyperlinks in emails. For example, respondents indicate that they very often delete emails that they do not trust and they almost never open attachments in emails from unknown senders. However, from the vignettes presented to those respondents – three e-mails, two of which were phishing e-mails and one legitimate e-mail – asking them to indicate how they would deal with the e-mails, it appears that 21 per cent would act unsafely: these respondents indicate that they would click on a hyperlink in a phishing e-mail or type the URL into their web browser.

Research questions 2 and 3: Is there a relationship between knowledge, opportunity and motivation and are there similarities between different online behaviours?

With the ultimate goal being to identify behavioural interventions that increase the safety of online behaviour of Dutch citizens, it was important to examine how traits and behaviours are distributed among the population. For example, do people with extensive knowledge of online security generally also have more social and material opportunity and motivation for safe online behaviour? The results show that the answer to that question is no: hardly any correlations are found between underlying characteristics that could explain safe online behaviour.

Next, it was important to investigate whether the various online behaviours are related. For example, on average, do people who choose a strong password behave more safely in respect of other

online behaviours as well? This question can also be answered negatively. The results of the current study indicate that how safely people behave in one online behaviour cluster is only minimally related to how safely they behave in another online behaviour cluster. For example, when someone shows safe behaviour when dealing with a phishing e-mail, this does not mean that they will, on average, also behave securely in terms of choosing a strong password. There is even a (very small) negative correlation between password strength and the sharing of personal data, which indicates that the stronger the password that respondents choose, the more unsafely they behave in the area of sharing personal data.

Finally, it may be questioned whether a focus on objective behaviour is necessary in follow-up research. Are self-reported and objective behaviours similar enough to base research on (much easier to collect) self-reported data? The results of the current study underline the importance of taking objective measurements of online behaviour. There is a very limited conformity between how people *say* they behave online and how people *actually behave* in the current study. The explanation for this may lie in what is called the cyber security paradox. Although most people indicate that cyber security is important, their self-reported behaviour does not always correspond to their actual behaviour, as underlined by the current study.

Research questions 4-7: Can the online behaviour of Dutch citizens be explained by knowledge, opportunity, motivation and other relevant factors?

Based on the literature, the most important predictive factors included in this study are knowledge, opportunity and motivation. These factors were expected to be associated with online behaviour. The self-reported data confirms this: knowledge, opportunity and motivation are positively related to self-reported safe online behaviour. However, if we look at actual online behaviour, a different picture emerges. Only knowledge appears to be significantly related to two behaviours: password strength and downloading unsafe software. However, the connection is negative: the more knowledge people have, the less strong the password they create. In addition: for every point that respondents score higher on the knowledge test, they become less likely to make a safe choice with the software pop-up. The strength of the chosen password and whether or not they download unsafe software is not significantly related to the (social or material) opportunity or motivation that respondents have for safe online behaviour. Only one connection between knowledge, opportunity, motivation and objective online behaviour corresponds to expectations from theory: when people have more knowledge of online security, they behave more securely when it comes to sharing personal data.

Based on the literature study, in addition to knowledge, opportunity and motivation, various other factors that may be related to online behaviour were included in the analyses. We examined whether online behaviour is associated with a negative or positive mood, fear of victimisation, earlier victimisation, self-control, device type, time pressure, persuasion techniques used by criminals, threat appraisal, coping appraisal and locus of control.

Self-reported online behaviour is related to a number of these factors. A negative mood is negatively related to self-reported safe online behaviour. In other words, the greater respondents' negative mood, the less safe their (self-reported) online behaviour is. A positive mood, on the other hand, is positively related to the safety of self-reported online behaviour. Based on earlier research, we had expected that a positive mood would be negatively related to safe behaviour. It was expected that citizens would see the outcomes of risky situations as more positive and be more willing to take risks. However, the results show a different picture. An explanation cannot be given based on the current study. Self-control is also significantly associated with self-reported online behaviour. In line with expectations, it was found that the more self-control respondents have, the safer their (self-reported) online behaviour is. The type of device used to fill in the questionnaire is also related to self-reported behaviour: respondents who used a PC or laptop indicate that they behave more safely online than those who used a tablet.

However, if we look at actual behaviour, only a positive mood, fear of victimisation, earlier victimisation, type of device and persuasion techniques remain. A positive mood is related to both password strength and downloading software from an unreliable source, but in opposing directions. The greater respondents' positive mood, the stronger the password they choose. On the other hand, it has been found, in line with the literature, that the greater respondents' positive mood, the greater the likelihood of them making an unsafe choice with the software pop-up ("clicking behaviour"). A positive mood, overall, is therefore related to both safe and unsafe online behaviour; this relationship depends on the type of online behaviour. Fear of victimhood is also significantly related to password strength; the more afraid respondents are of becoming a victim of online crime, the stronger their chosen password. In addition, victimisation is negatively related to actual clicking behaviour; respondents who have previously fallen victim to online crime more often make a safe choice by not downloading software from an unreliable source. The type of device used by respondents has a significant relationship with all objectively measured behaviours. Respondents who use a PC or laptop choose a less strong password than respondents who use a tablet. They also behave less safely in the areas of downloading software from an unreliable source and sharing personal data. Respondents who used a smartphone make a safe choice more often than respondents using a tablet with respect to downloading software from an unreliable

source. Finally, one of the persuasion techniques that cyber criminals use appears to be related to unsafe online behaviour. Respondents to whom the "reciprocity" persuasion technique has been applied share significantly more personal data.

Finally, it was investigated whether the way in which people evaluate the online threat and safety measures influences the extent to which they are motivated to protect themselves. Threat appraisal, coping appraisal and locus of control have a positive connection with the motivation for online self-protection. Based on the Protection Motivation Theory (PMT), this motivation can be expected to influence the safety of online behaviour. However, we cannot draw that conclusion. In fact, if we look at the relationship between threat appraisal, coping appraisal and locus of control and online behaviour, we see only one significant relationship: that between coping appraisal and self-reported online behaviour. Coping appraisal – the extent to which respondents believe that online security measures are effective, the extent to which they are able to take those measures themselves and whether they think the costs of these measures are not too high – is positively related to self-reported online behaviour. The higher the coping appraisal, the more safe online behaviour is reported. However, in respect of all objectively measured online behaviours (password strength, click behaviour and sharing of personal data) and in respect of the "e-mail choice" vignette measurement, no significant relationships with the PMT elements are evident.

Research question 8: Does the online behaviour of Dutch citizens differ between population groups?

Several of the background characteristics of respondents are related to self-reported online behaviour. The higher the age, the safer the self-reported online behaviour and the safer the self-reported handling of hyperlinks in phishing emails. For education, the relationship is negative: the higher the education, the less safe the self-reported online behaviour is. Having live-in children under the age of 16 is also related to handling hyperlinks in phishing emails more unsafely.

In terms of actual online behaviour, we also find a number of relationships with respondent characteristics. For example, being employed has a significant relationship with both password strength and whether or not respondents download software from an unreliable source. Employed respondents choose a less strong password and more often download software from an unreliable source. In addition, respondents with higher education choose a less strong password, but they do behave more securely when it comes to sharing personal data. The clicking behaviour of men is, on average, less safe than that

of women and they also share more personal information. Cohabitants, on the other hand, display safer clicking behaviour. Finally, it seems that the older citizens are, the more personal information they share.

Research question 9: Are the effects of knowledge, opportunity and motivation on online behaviour influenced by other factors?

It was investigated whether the relationships between knowledge, opportunity and motivation and online behaviour can be explained by interactions between these variables and the following (moderator) variables: negative mood, positive mood, fear of victimisation, previous victimisation (ever) and self-control. Taken together, the results indicate that most interactions are not significant but, in some cases, the relationships between knowledge, opportunity, and motivation and online behaviour are influenced by self-control, mood, fear of victimisation and, in one case, previous victimisation.

Most of the significant interactions were found in the analyses in which self-reported online behaviour and password strength are predicted. A few interactions show that the direction of the relationships found depends on the level of one's scores on the moderator variables. For example, among respondents with very little fear of becoming a victim of online crime, there appears to be a positive link between social opportunity and the safety of self-reported online behaviour. However, as fear of victimisation increases, this connection weakens. For respondents who are (very) fearful of victimisation, the relationship even becomes negative: they report less safe behaviour when social opportunity increases.

In addition, there are a number of interactions in which the relationships found do not change direction but become stronger, as one scores higher or lower on the moderator variables. For example, the positive relationship between motivation and self-reported online behaviour becomes less strong as respondents have a more positive mood and as respondents have a greater fear of victimisation.

Limitations

Like all research, this study also has its limitations. Firstly, we do have a relatively large number of respondents who are representative of Dutch society by gender, employment (yes / no) and the province in which they live, but the data are not entirely representative. For example, on average, respondents are more often highly educated and less often younger than 39 years old.

The significant added value of this study is that not only has self-reported behaviour been measured, but actual behaviour has been measured objectively too. This was moreover done in a large

sample, with respondents who answered a variety of questions about their online behaviour on their own device in their own home. However, the objective measures each have their own limitations. Firstly, due to the length of the questionnaire, it was not possible to include objective measures for all seven behavioural clusters. Concerning the data on sharing personal data, we do not know which data was entered and whether this was actual/correct data. Other factors may have influenced the results on downloading unsafe software (clicking behaviour). For example, we used a pop-up that was designed in the style of the Windows operating system. Therefore, non-Windows users would be less familiar with the pop-up. This may make them more suspicious or more likely to say yes. Further research is needed, with a range of pop-ups that are technically realistic and adapted to the device and operating system. Finally, although the method - a survey with experiments - is very appropriate for conducting this type of research, we are of course dealing with respondents who may feel safe in the research panel agency's online environment. As a result, they may have made unsafe choices more quickly than usual.

Looking to the future: interventions

The aim of this study was to discover how safely Dutch citizens behave online and to explain this based on factors that have emerged from the literature, in order to take an initial step towards developing interventions to make Dutch citizens safer online. The results of this research were therefore discussed with experts to identify promising directions for interventions.

In summary, it appears that there is no silver bullet for promoting safe online behaviour. Different online behaviours seem to stem from different sources. There is also a perception among experts that people differ in their sensitivity to interventions and that the timing of interventions is crucial to their success. Experts do see a lot of value in interventions that focus on adaptations to the technology that people use for online activities, such that the possibility of unsafe behaviour is reduced and the possibility of safe behaviour is increased – also known as security by design. There is a role here for policy measures encouraging technology manufacturers to make adjustments that make it easier for people to adopt safe behaviours. However, designing specific interventions aimed at manufacturers or citizens themselves is no easy task. Future research could focus on developing and evaluating a specific set of interventions aimed at influencing the unsafe behaviours found in this study.