Summary

Background

To prevent becoming a victim of cybercrime, it is important that people behave safely when performing online activities. Although measures such as firewalls, virus scanners, and two-step verification contribute to mitigate the risks of unsafe password behaviour and unsafe sharing of personal data, a significant part of victimization can be traced back to human behaviour. Previous research by the WODC (Research and Documentation Centre) (Van 't Hoff-de Goede et al., 2019) has focused on the question of how safe Dutch citizens behave online and how this can be explained. One of the main conclusions of this study was that, while both self-reported and observed online behaviour were found to be unsafe, people behaved more unsafe than they reported, especially with regards to password use and the sharing of personal data. The current research focused specifically on the latter two behaviours. The research consisted of a literature review and two empirical studies. It was investigated which psychological factors play a role in 1) whether people generate safe passwords and 2) whether people share their personal data online only when it is safe and/or necessary. In addition, we developed and tested an intervention to increase safe password behaviour and safe online sharing of personal data.

Conclusions of the literature study

In the current study, based on the protection motivation theory (PMT), the following psychological factors have been measured to investigate the extent to which they play a role in safe password behaviour and the safe sharing of personal data online: response cost, perceived vulnerability, perceived severity, perceived self-efficacy, and response efficacy. In addition to the PMT factors, we also investigated the role of responsibility in both target behaviours.

Literature on *response cost* showed a negative relation between response cost (the estimation of the cost incurred to execute the target behaviour) and self-reported safe online behaviour: the higher the response cost, the less people behave safely in terms of password behaviour and the sharing of personal data online. Regarding the perceived *vulnerability* to negative consequences of unsafe online behaviour, the literature showed that people often perceive a low vulnerability, and that vulnerability is positively related to safe password behaviour and the safe sharing of personal data online: the higher the perceived vulnerability, the safer the behaviour. While vulnerability refers to the probability of the negative consequences of unsafe online behaviour occurring, perceived *severity* refers to how serious those negative consequences are perceived to be. Research showed a positive relationship between the perceived severity of consequences of unsafe online behaviour and how safe people behave online: the higher the perceived severity, the safer the behaviour. The literature study also revealed that the extent to which people feel able to counteract risks as a determining factor for displaying safe online behaviour. A distinction is made between *response efficacy* and *self-efficacy*. Self-efficacy is the degree to which a person feels capable of executing the target behaviour and response efficacy is the degree to which a person expects that executing the target behaviour will remove the risks. The literature review by Van 't Hoff-de Goede et al. (2019) showed that both types of efficacy play an important role in safe online

behaviour. Subsequent studies showed similar results: People who feel unable to counteract the risks associated with unsafe online behaviour are also more likely victims of cybercrime. Lastly, the literature showed that *responsibility* also plays a role in safe online behaviour. People who perceive online safety as their own personal responsibility are more likely to take protective measures and display safe behaviour.

In Study 1, we investigated which of these psychological factors promote or hinder safe password behaviour and the safe sharing of personal data online. Next, an intervention was developed and tested in Study 2, that was aimed at important psychological factors as identified in Study 1.

Study 1

Study 1 was a survey study in which we examined which psychological factors promote and hinder safe password behaviour and the safe sharing of personal data online. To examine this, we used a behavioural measure (i.e., strength and uniqueness of a generated password; participation in an online raffle and the amount and type of personal data shared) and a self-report measure of safe online behaviour (i.e., the extent to which participants reported to use strong and unique passwords; the extent to which participants reported to share personal data online in a safe way). The psychological factors were assessed with multiple statements. The study included several open-ended questions and background questions to provide an even more complete picture of the promoting and inhibiting factors of safe online behaviour.

The results of Study 1 showed that unsafe online behaviour occurred to a high extent for both target behaviours. Around 84% of participants displayed unsafe password behaviour by generating weak to very weak passwords. In addition, part of the participants reused passwords. Further, about 81% of the participants participated in the online raffle. With their participation, participants agreed to sharing their personal data online. Over 70% of the participations who chose to participate in the raffle shared all of their personal data, including the last three digits of their bank account (85.2% of participants), while it was not required to share all data. To conclude, there is a lot of room for improvement in both target behaviours.

Next, we looked at which psychological factors predicted *safe password behaviour*. The results of Study 1 revealed response cost, self-efficacy, and severity as important predictors of safe password behaviour. The lower the perceived response cost and the higher the perceived self-efficacy and severity of risks, the safer the password behaviour. The results of the open-ended questions about promoting and inhibiting factors underlined the importance of the abovementioned factors. The most frequently mentioned factor was self-efficacy: participants reported difficulty remembering safe passwords. The response cost associated with safe passwords was also mentioned as an inhibiting factor. The open-ended question about promoting factors showed that participants expressed the need for password managers/applications that can help them to display safer password behaviour.

In addition, we examined which psychological factors predicted the *safe sharing of personal data online*. Of the factors studied, self-efficacy and severity were important predictors of the safe sharing of personal data online. The higher the perceived self-efficacy and severity of risks, the safer the behaviour. The results of the open-ended questions about the promoting and inhabiting factors confirmed self-efficacy as an inhibiting factor in the safe sharing of personal data online. In addition, response cost emerged as an inhibiting factor. The open-ended question about promoting factors showed that responsibility was an important factor: participants mentioned that websites/applications should request and collect fewer personal data and indicate more clearly which data are required (i.e., mandatory) and which are not. In addition, technical solutions were mentioned as an important promoting factor: participants indicated than an extra security program or two-step verification would help to display more safe online behaviour.

Study 2

Based on previous research on behavioural change, recent studies in the context of cyber security, and the results of Study 1, in Study 2 we tested by means of an experiment whether increasing the perceived severity of risks of unsafe behaviour and increasing the perceived self-efficacy of execution of safe behaviour results in safer password behaviour and safer sharing of personal data online. Our intervention consisted of the communication of risks of unsafe behaviour (severity), how safe behaviour can be performed (self-efficacy), or a combination of both, with a control group as a reference group.

The results of Study 2 showed that our intervention was effective, as it resulted in safer online behaviour. For *safe password behaviour*, we found that participants who received information about self-efficacy, on its own or combined with severity of risks, generated stronger passwords than participants in the control condition who had not received this information. Passwords had higher entropy scores, more frequently met criteria for strong passwords, and less frequently contained personal information. The passwords of participants who only received information about the severity of risks also in part were safer than the passwords of participants who had not received the information, but the effects overall were weaker.

The results for differences between groups in society showed that the effectiveness of the intervention for password entropy did not depend on participants' gender, age, or education level. Gender did not affect whether the generated password met criteria for strong passwords or whether it contained personal information either. The measure of whether the generated password met criteria for strong passwords did reveal that the effect of the intervention varied as a function of participants' age and education level. While self-efficacy resulted in stronger passwords in all age groups, severity (in particular in combination with self-efficacy) was only effective among middle-aged and older participants. For education level we found that self-efficacy, on its own or combined with severity, resulted in the safest passwords among highly and moderately educated participants. We did not find differences in conditions among low educated participants.

For the *sharing of personal data online*, we found that participants who participated in the online raffle shared a remarkable amount of non-required personal data, both in the control condition and in the intervention conditions. We did find that our intervention was effective here as well, as it resulted in safer online behaviour. Participants that received information about self-efficacy, on its own or in combination with severity of risks, shared less non-required personal data compared to participants in the control condition who had not received this information. The condition in which only information about severity of risks was provided did not differ from the control condition in the amount of non-required personal data shared, but participants in this condition did more frequently decide to not participate in the online raffle compared to participants in the control condition. By not participating in the raffle, they also were not required to share their personal data.

The results for differences between groups in society showed that the effectiveness of the intervention on participation in the online raffle varied as a function of participants' gender (a significant effect for women, not men), but not as a function of participants' age or education level. The results did show main effects of age and education level on the sharing of personal information in the raffle. The older the participants, the more frequently they shared non-required personal data. De results for education level showed that the higher the participants' education level, the more frequently they shared non-required personal data.

Limitations and future research

The current research provides insight in the psychological factors that play a role in safe password behaviour and safe sharing of personal data online. The research further demonstrates that and how an intervention aimed at raising/activating perceived severity of risks and self-efficacy can promote safer online behaviour. Future interventions that based on the current research are developed can potentially make an important contribution to prevent victimization of cybercrime. Nevertheless, there are several aspects of the current research that make it important to interpret the conclusions of the study with care.

Although the intervention in Study 2 resulted in safer online behaviour, we see that passwords in the intervention conditions were still weak, and participants often still shared their personal data online even when they were not required to do so. The passwords were less weak compared to the control condition, and less non-required personal data were shared, but there is still a lot of room for approvement.

In addition, although we had a large sample for both empirical studies that was largely representative of the Dutch population, we cannot fully conclude that the sample was representative. We had more highly educated participants and fewer lower educated participants and more younger and fewer older participants. In addition, participant dropout levels were higher when they were asked to share their personal data as part of an online raffle compared to when they were asked to generate a password. This shows potential selective dropout of participants, and that a specific group of participants possibly has not completed the studies.

A strength of the current research is the central position of actual behaviour. Participants generated a password and were offered the choice to share or not share specific personal data online. The behavioural measures used do have limitations.

For password behaviour, we used an entropy score to determine the strength of the generated password. However, this does ignore some aspects of password strength. For example, a password may score high in entropy, but still use an existing word, and because of this be relatively unsafe. In Study 2, we have in part addressed this issue by adding a question that assessed whether the generated password contained personal information. Future research could, in addition to the entropy score and questions whether generated passwords are unique and whether they contain personal information, also assess other aspects of safe passwords. This would provide important information about how to promote these specific aspects of safe password behaviour.

The behavioural measure for the safe sharing of personal data online also has limitations. Our participants shared their personal data in the context of participation in an online study. Possibly, participants shared more personal data because they believed they were in a safe environment. In the current research we have not distinguished between websites where it is safe or required to share sensitive personal data vs. websites whether this is not safe or required. Future research could assess the target behaviour in different contexts, to examine whether the same psychological factors play a role, and whether the intervention that was tested in the current research is as effective in different contexts.

Finally, it is worth recognizing that while Study 2 showed that it was a good choice to target our intervention on perceived self-efficacy and severity of risks, we could have chosen to target the intervention on one of the other psychological factors investigated in Study 1. Responsibility, for example, also could be a relevant factor in the safe online sharing of personal data. Future research could focus on increasing people's perceived own responsibility to make them more aware of their own role in safe behaviour, and in this way promote safe online behaviour.

Policy implications and interventions

The aim of the current research was to identify which psychological factors play a role in safe password behaviour and safe sharing of personal data online, and to test whether influencing these factors through an intervention results in safer online behaviour. It was not our goal to develop a ready-to-use intervention that can be implemented by the government, websites, or other institutions to promote safe online behaviour for a wide range of online applications. However, the results can provide a basis for developing interventions.

In addition to showing that interventions aimed at perceived severity in combination with perceived self-efficacy can be effective, Study 1 showed that other interventions may also be effective in promoting safe online behaviour. One concrete advice we would like to give based on Study 1, is that regarding safe password behaviour, interventions aimed at promoting the use of password managers can be effective.

In addition, the tested intervention for safe passwords and safe sharing of personal data online can (in part) be combined with other intervention techniques. For example, a lot can be achieved by the use of technology or adapting the user environment. One could, for instance, make use of two-step verification or biometric data to access accounts or protect personal data from access by cyber criminals (Young et al., 2018). It could also be effective to adjust legislation and force websites to provide information about the perceived severity of the risks or about perceived self-efficacy before users create an account or share personal data. In addition, websites and apps could only be allowed to ask for necessary personal data. In combination with the intervention that was tested in the current research that targeted psychological factors, these technological, environmental, and legislation factors could increase the desired behaviour even more.

Finally, it is important to note that an intervention may not be equally suitable for every subpopulation in society. The analyses in Study 2 clearly showed differences between subgroups in the effectiveness of the intervention on safe online behaviour, and (in both Study 1 and Study 2) on safe online behaviour itself. This means that a careful translation is needed from the current findings into policy, where it must be examined and tested for whom the intervention is most effective and how it can best be used.

To conclude, the current research shows that Dutch citizens display unsafe password behaviour and unsafe sharing of personal data online. Our intervention aimed at increasing perceived self-efficacy and perceived severity of the risks of unsafe behaviour resulted in safer password behaviour and safer sharing of personal data online, but there is still much room for improvement. This may be achieved with technology, adjustments to the user environment, and by changes in legislation.