

## Summary

### **Online victimization Prevalence, risk factors and consequences**

Online crime victimization has become one of the major challenges in our digitalized society. Almost everybody is connected to the internet and exposed to potential online offenders. The goal of this study is to gain more insight in the prevalence, risk factors and consequences of online victimization among Dutch people aged 16 years and older. Online crime can be divided into cybercrime and digitalized crime. Cybercrimes can only be committed using information communications technology (ICT), like computer viruses and hacking. Digitalized crimes are traditional offline crimes that are enabled by an ICT-component, such as online fraud and online harassment.

This study includes seven types of online crime: credit card fraud, hacking, online consumer fraud, online harassment, computer viruses, unauthorized bank withdrawal and identity fraud. First, the prevalence of these types of crime is estimated. Second, the question to what extent age, gender, education, internet use, online protection measures and personality traits affect the chance to become victim of online crime is answered. We also investigate to what extent these risk factors for online crime are risk factors for offline crime. Third, we study to what extent online victimization correlates with changes in fear of online crime, internet use, online protection measures and mental health of victims. Fourth, we study to what extent risk factors for a first online victimization are also risk factors for repeated online victimization.

### **Research questions**

The central research question of this study is: what are the trends, risk factors and consequences of (repeated) online victimization?

In order to answer this research question, we answered the following sub-questions:

- 1 To what extent have Dutch citizens become victim of online crime?
- 2 To what extent does online victimization correlate with previous online victimization, internet use, online protection measures, socio-demographic characteristics and personality traits?
- 3 To what extent are fear of online crime, internet use, online protection measures and mental health consequences of online victimization?
- 4 To what extent have Dutch citizens become repeated victims of online crime, and to what extent do potential consequences of previous online victimization affect the chance on repeated online victimization?

### **Methods**

In order to answer the research questions, we use data from the LISS-panel, an online survey among a representative sample of Dutch households. Participants of the LISS-panel have been questioned monthly on various themes, such as their personality, health and leisure activities. Since February 2008, respondents have

participated in a biennial survey on victimization that includes question about victimization of several types of online and offline crimes. We used six waves of this survey with around 5,000 to 6,000 respondents each.

## Results

### *Online victimization decreased between 2010 and 2018*

Results show a significant decrease in the number of victims of the seven types of online crimes combined, from 15.1% in 2010 to 9.5% in 2018. The most prevalent type of online crime has also changed, from computer viruses in 2010 to online consumer fraud in 2018. The number victims of offline crime was slightly higher, but also significantly decreased in the past decade (from 20.5% in 2010 to 12.4% in 2018). The decline in prevalence of online victimization is mainly attributed to the decrease in victims of computer viruses (8.9% in 2010 and 1.7% in 2018). The prevalence of hacking (1.4% in 2010 and 0.9% in 2018) and unauthorized bank withdrawal (3.0% in 2010 and 1.2% in 2018) has also decreased. The prevalence of online consumer fraud and identity fraud has significantly increased. Only a minority of victims have filed a police report: 11.6% of unauthorized bank withdrawal victims, 12.0% of online consumer fraud victims, 20.2% of online harassment victims and 46.0% of identity fraud victims.

### *Higher risks among men, young people and frequent internet users*

Victims of online crime in a previous wave are at higher risk of becoming victim in a subsequent wave. The more hours one spends online, the more likely one is to become victim of online crime. One would expect that using more online protection measures would protect internet users against online victimization, but, surprisingly, having taken more protection measures does not lower the risk of online victimization. Other people who are at higher risk of online victimization are men, young people, impulsive people, emotionally instable and more open people. We also tested whether these risk factors for online victimization are risk factors for offline victimization. Age, emotional instability and openness appeared to be risk factors for both types of crime. Gender is also a risk factor for offline victimization, but in an opposite direction. Men are more likely to become online victim than women, whereas women are more likely to become offline victim than men. Offline victimization is also more prevalent among more altruistic and less conscientiousness people. Impulsivity is correlated with online victimization, but not with offline victimization, and can therefore be regarded as a distinctive risk factor for online victimization.

### *Fear of online crimes increases, but mental well-being does not change after online victimization*

Victims of online crime report an increased fear for online crime. Even though this fear may withhold victims to use the internet, this study does not show a change in internet use among online victims. They do, however, take more protection measures than before, especially those who did not report the crime to the police. A possible explanation is that protection measures are taken by victims of computer viruses, whereas these victims may be less likely to report to the police compared to victims of more serious crimes. The mental well-being of victims does not change among online victims in general, but it decreases among victims of online harass-

ment, possibly because online harassment has a more serious impact on a victim's personal life than other types of online crime.

#### *Repeat victimization correlates with impulsivity, emotional instability and openness*

16.6% of the respondents who participated at least two times reported that they fell victim to online crime just once, whereas 17.5% reported to have fallen victim repeatedly. The more impulsive, emotionally instable or open, the higher the chance to become a repeat victim of online crime. Possible consequences of previous online victimization do not seem to explain why people fall victim again. Internet use and mental well-being do not change after previous online victimization, and can therefore not explain why these people would be more likely to be victimized again. The number of protection measures do increase after online victimization, but do not affect the chance to become victim again.

#### *Strengths and weaknesses*

The main contribution to the existing literature on online victimization is the use of longitudinal panel data, gathered between 2008 and 2018. The temporal order of events and behaviour is clearer using panel data and therewith more suited in estimating risk factors and consequences of online victimization than studies that use cross-sectional data. Another strength of this study is the use of self-reported online victimization. Because not all crimes are reported to the police, these data have a larger scope than police records. The weakness of self-reported online victimization is that it depends on the interpretation and memory of victims themselves who, for instance, may forget when the crime has actually taken place. Besides, not every type of crime was included in the survey. More recent types of online crime, such as malware and ransomware, were therefore not taken into account in estimating the number of online victims.

## **Conclusion**

The number of victims of seven types of online crimes has decreased among a representative sample of Dutch citizens. One of the risk factors is internet use, as people are more likely to be exposed to potential cyber offences when they spend more hours online. People who fell victim to an online crime before, men and young people have a higher risk to become victim. People who are impulsive, emotionally instable or more open are even more likely to be victimized repeatedly than people who are respectively less impulsive, less emotionally instable or less open. These personality traits are possible proxies of online behaviour. Impulsive people may think less about possible consequences of their online behaviour, emotionally instable people may have more difficulties in assessing online risks, and more open people are more likely to share personal information online.

Victims of online crime do not report a change in hours spend online, nor do they report a change in mental well-being. Victims of online harassment, however, report a slight decrease in their mental well-being, possibly because this type of crime has a more serious impact in a victim's personal life. Online crime victims show an increase in fear of online crime and take more protection measures than before. This implies that victims tend to adjust their behaviour after a crime experience, and it is therefore relevant to inform (potential) victims about the actions they can take to prevent (repeat) online victimization.