ABSTRACT

With the advent of the internet, criminals gained new tools to commit crimes. Crimes in which the use of connected information technologies is essential for the realisation of the offence are defined as cybercrimes. The human factor is often identified as the weakest link in the information security chain, and it is often the behaviour of humans that leads to the success of cybercrimes. In this chapter, end-user characteristics are studied that may predict cybercrime victimisation. This is done by means of a review of the literature and by a study on personality traits. More specifically, personality traits from the big five are tested on victims of three different types of online fraud, phishing, Microsoft fraud, and purchasing fraud, and are compared with norm groups of the Dutch population. This chapter ends with implications for online fraud prevention and possibilities to advance the study of cyber victimisation.
INTRODUCTION

Society is digitising, and with it there has been a broadening of the opportunities that people have in many respects, for instance, when it comes to maintaining social contacts and making government services more accessible. The digital revolution, however, is also expanding the range of opportunities that delinquents have for targeting their victims (Bossler & Holt, 2009; Van Wilsem, 2011). The internet is being used to create new kinds of crime, and many traditional crimes can now be carried out in new and simpler ways (Bossler & Holt, 2010; Pyrooz, Dec, & Moule Jr, 2015). Crimes in which the use of connected information technologies is essential for the realisation of the offence are defined here as cybercrimes. A particular kind of cybercrime that is the focus of this chapter is online fraud – deception with the aim of financial gain whereby information technology is essential to its implementation (Stol, Leukfeldt, & Klap, 2012).

Although online fraud always has a digital component, the human aspect of this kind of offence is also crucial (Parrish, Baily, & Courtney, 2009; Wiederhold, 2014). Fraudsters generally target vulnerable, human characteristics as opposed to relying on breaches in technology. They also use deception to get their hands on sensitive information (Parrish et al., 2009) or to persuade people to make fraudulent purchases (Van Wilsem, 2013). Victims participate actively in the offence, as it were, because they themselves give the fraudsters the information they need, for instance, to access their bank accounts (Jansen & Leukfeldt, 2015). This means that people are the ‘weakest link’ in this type of crime. That said, not everyone responds to ‘fake’ e-mails, telephone calls or advertisements. Most people ignore them or delete them immediately (Jones, Towse, & Race, 2015; Parrish et al., 2009). This raises the question of what makes some people respond to the tactics that fraudsters use, and with that fall victim to online fraud, while others do not. In this chapter, an explanation for victimisation is first sought in the routine activity approach (Cohen & Felson, 1979). As will become evident, this approach offers no consensus for what makes a person run an increased risk of falling victim to online fraud. For this reason, the researchers go on to approach the explanation for victimisation from the perspective of personality traits. A better understanding of online fraud victimisation is needed to enhance cyber security.

THE RELEVANCE OF THE HUMAN FACTOR IN EXPLAINING CYBER VICTIMISATION

The rising threat that cybercrime poses has increased the urgency to gain an understanding of online fraud victimisation (NCSC, 2015). The opportunities that the internet offers are multiplying, and society is increasingly adjusting to the idea that these opportunities should be used (Pratt, Holtfreter, & Reisig, 2010). Moreover, the rise in these options is going hand in hand with a decline in the number of analogue alternatives available (NCSC, 2015). As a consequence, people are becoming more dependent on the internet, which in turn is exacerbating their vulnerability (Choi, 2008; Furnell, Bryant, & Phippen, 2007). If we are to steer future developments in the field of information technology in the right direction when it comes to safety and security, then it is essential that we have a good understanding of online fraud and what makes people fall victim to it. The knowledge emanating from this chapter can help various organisations, like the police, banks and commercial companies, both on- and offline, to arrive at more effective, behaviour-oriented preventive measures.