

Criminal offences committed by means of computers

In this chapter computer-related frauds (§ 213), the so-called usual frauds committed by means of computers (§ 209), sexual offences against minors (§§ 175–179), some offences against intellectual property (§§ 222–225, exc. 222¹) and money laundering (§ 394) are considered as criminal offences committed by means of computers.

1260 criminal offences committed by means of computers were registered: 470 computer-related frauds, 677 usual frauds committed by means of computers, 83 money laundering offences, 18 sexual offences against minors and 12 offences against intellectual property. As money laundering offences and sexual offences against minors are dealt with in other chapters of the compilation, these are not dwelled upon here.

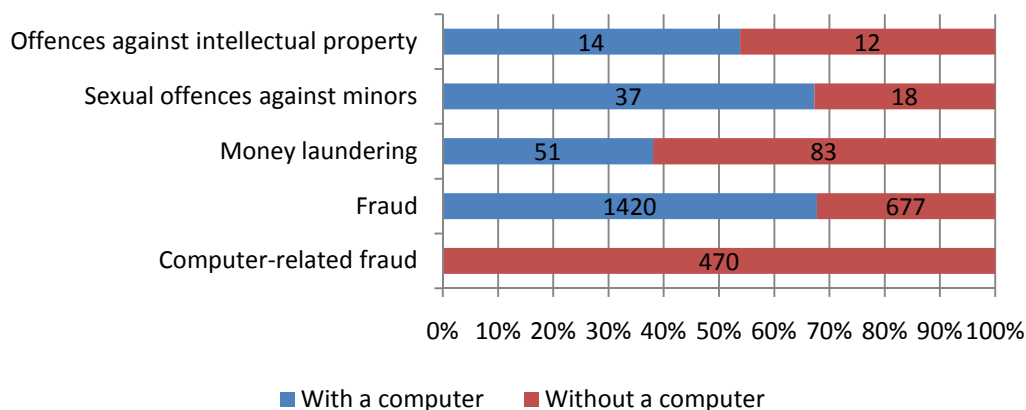


Figure 35. Criminal offences committed by means of computers in 2009

Cyber frauds

A very large proportion of criminal offences committed by means of computer are formed by frauds (91%), and also vice versa, many frauds are committed by means of computer (43%). These indicators include the criminal offences registered both as computer-related frauds (§ 213) and as ordinary frauds (§ 209) which were committed by means of computer (§ 209), otherwise it has been specified in the text differently. Computer-related frauds are divided into five big groups: fast loan frauds, frauds with the use of stolen credit or debit cards, mobile phone frauds and Internet auction frauds.

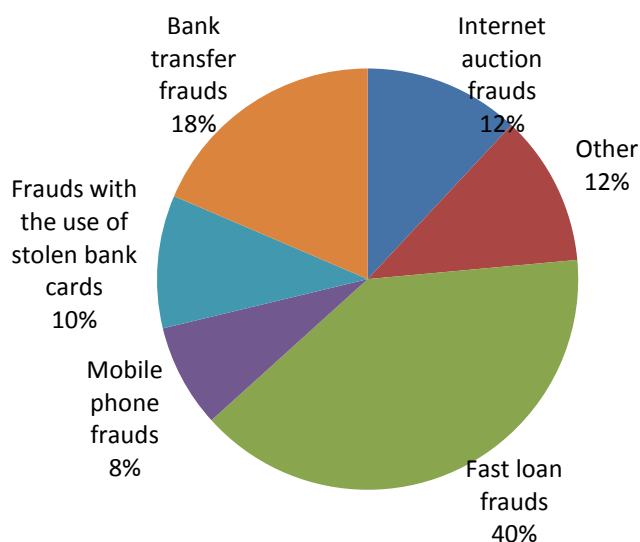


Figure 36. Types of computer frauds in 2009

456 cases of fast loan frauds were registered (124 pursuant to § 213 and 332 pursuant to § 209). In case of these criminal offences, the criminal offenders requested money in the name of somebody else to the person's account using for that purpose the User ID of Internet bank, passwords or password card which were stolen, swindled or obtained in some other manner. After a loan was received, the money was forwarded to offenders' bank account.

213 bank transfer frauds were registered (125 in Estonia pursuant to § 213 and 12 in foreign countries pursuant to § 209). Criminal offenders obtained victims' Internet bank passwords, entered the Internet bank and forwarded money with bank transfers to their own bank accounts. On another occasion a victim had to perform a bank transfer to the criminal offender's account for some service, after which the criminal offender asked for the Internet bank ID codes in order to "check" the transfer and executed bank transfers to his bank account.

Paid striptease in MSN Messenger

A man who pretended to be a girl in the Internet offered a paid striptease service for the users of MSN Messenger. The users of MSN Messenger forwarded to "the girl's" bank account depending on the user up to 400 kroons, however, the promised show did not follow. After that, the "the girl" lied that the money had not been forwarded and asked the users to forward their Internet passwords for checking, which the latter also did. After that, the cheater forwarded the victims' money to his bank account.

Compared to 2008, the number of national bank transfer frauds increased considerably, while the number of international banks transfer frauds has decreased – when in 2008, 44 frauds inside Estonia were registered pursuant to § 213, then 125 were registered in 2009; during the same period, the number of international frauds decreased from 116 down to 13. In case of international frauds, software was used in order to obtain the victims' data which forwarded the data entered by victims to criminal offenders (phishing): the user was asked, for example, to enter on a fake homepage his/her user ID and passwords.

117 frauds with the use of stolen credit or debit cards were registered (only on the basis of § 213). Frauds committed with stolen bank cards differ from bank transfer frauds by this that in case of the latter someone else's bank passwords have been obtained; however, in case of stolen bank cards a criminal offender has obtained victim's bank cards. The majority of credit card frauds are related to paying for fuel when a credit card has been stolen, for example from an employer. In case of debit card frauds the victim is often the criminal offender's relative or acquaintance who has taken from the victim's wallet the victim's bank card together with PIN Code and has withdrawn money from the account from the nearest ATM. Often, a victim's wallet has been stolen on the street, in store or in a public transport vehicle and after that cash has been withdrawn from ATM.

A total of 91 mobile phone frauds were registered (69 on the basis of § 213 and 22 on the basis of § 209). Stolen or borrowed mobile phone has been used for calling the special tariffs telephone numbers, sending SMSs or, for example, for loading money on one's account in the www.rate.ee environment (in this environment only a code sent to a telephone number has to be entered in the Internet and money shall be received on the account).

A total of 137 Internet auction or purchase environment frauds were registered (only on the basis of § 209). In addition to the www.osta.ee environment, frauds have also occurred in the www.okidoki.ee and www.sendioksjon.ee auction environment where a victim has found the desired goods and pays the seller for the purchase by means of Internet bank, although in reality the seller will not send the buyer any goods. In order to avoid such frauds, for example, a deposit payment offered in the www.osta.ee environment should be used or payment for goods should be effected upon the receipt of goods. In case of frauds committed in the Internet purchase environment the goods in the advertisement are being paid for in advance, however, the goods are not received; the goods are computers, laptops, clothes, jewellery, theatre tickets, etc.