Topic III: Measures against Unlawful Money Transfers Related to Internet Banking

Recently, unlawful money transfers related to Internet banking have rapidly increased. The police are carrying out thorough crackdowns, and public relations and awareness activities to prevent victimization.

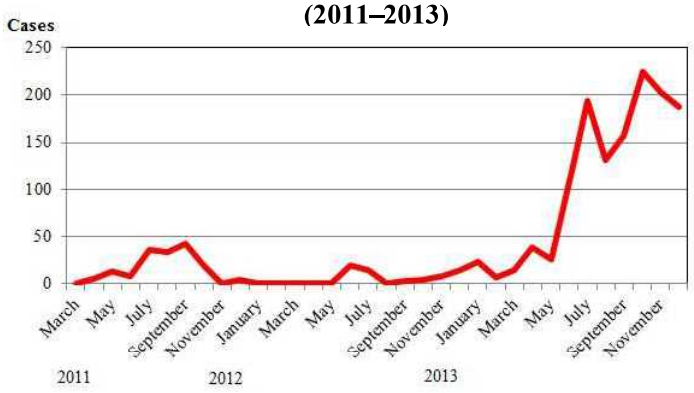
There has been a rapid increase in crimes where Internet banking ID and passwords are unlawfully obtained and utilized to illegally transfer money into another person's account. Since this kind of crime can harm the safety of and shake confidence in Internet banking, the police are conducting thorough crackdowns, preventive activities in collaboration with financial institutions and other entities, and public relations and awareness activities for users.

(1) Occurrences of Unlawful Money Transfers Related to Internet Banking

I. A Sudden Increase in Occurrences

In 2011, the amount of damage incurred by unlawful money transfers totaled approximately 308 million yen. While it dropped to approximately 48 million yen in 2012, financial loss rapidly increased in 2013 and significantly grew to approximately 1.406 billion yen. The situation is grave, with occurrences especially climbing since June of the same year, with over 100 cases each month.

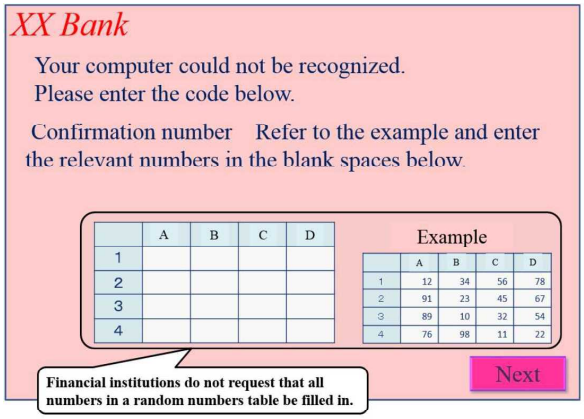
Trends in the number of unlawful money transfer through Internet banking by month (2011–2013)



II. Modus Operandi of Unlawful Acquisition of Identification Codes Such as ID and Passwords

Phishing sites and computer viruses are known to be used as means for acquiring other people's identification codes, such as ID and passwords. In regard to the latter, from around October 2012 not only have there been computer viruses that unlawfully obtain ID and passwords when connecting to legitimate Internet banking sites, but there have also been instances of financial loss incurred through computer viruses that fraudulently display screens asking users to fill out a random numbers table required to authenticate trades. This type of fraud has rapidly increased in 2013. Some computer viruses unlawfully obtain ID and passwords for email accounts, and there has also been financial loss incurred by obtaining one-time passwords* 1 appearing in emails.

Unlawful screen display due to computer virus (illustration)



III. The Process by which Funds Are Unlawfully Transferred

Accounts into which money has been unlawfully transferred are held by Chinese citizens in approximately 70% of instances and Japanese citizens in approximately 20% of instances. In addition, approximately 70% of all cases of unlawfully transferred funds are those where payment is made by a person different from the holder of the account into which money is unlawfully transferred, and money is transmitted overseas through a fund transfer business operator through withdrawals made by the holder of the account into which money was unlawfully transferred.

*1: This is an authentication password used for purposes such as Internet banking. The character string comprising the password changes for each time of authentication, ensuring that the password cannot be utilized the next time the website is accessed even if the identification code is stolen.

Case 1: In September 2011, a man (age 32) and an accomplice from China utilized an unlawfully obtained ID and password of another individual to illegally remit 5 million yen into his own savings account. By October 2012, both men were arrested for crimes including computer fraud and violation of the Unauthorized Computer Access Act (Act on the Prohibition of Unauthorized Computer Access). (Saitama Prefecture)

Case 2: In October 2013, a man from the Philippines (age 32) offered information for a fee that was required to receive cash unlawfully transferred to his own savings account and remitted overseas through a fund transfer business operator. In January 2014, the same man was arrested for violation of the Act on Prevention of Transfer of Criminal Proceeds (compensated transfer using an exchange transaction card, etc.). (Aichi Prefecture)

(2) Countermeasures against Unlawful Money Transfers Related to Internet Banking

I. Arrests of Persons Contributing to Unlawful Money Transfers

In 2013, the police arrested a total of 68 persons who opened an account with the fraudulent intent of allowing it to be utilized by another person, bought and sold accounts, withdrew unlawfully remitted funds, collected cash, and gave instruction on such unlawful actions related to unlawful money transfers.

II. Swift Investigation through Collaboration with Prefectural Police

Because in many cases, the addresses of holders of accounts from which funds are remitted, the addresses of holders of accounts into which funds are remitted, and the locations of cash withdrawals span several jurisdictions, it is important to share information on damages and collaborate among prefectural police from the time the perpetration of a crime is confirmed. Therefore, the National Police Agency actively promotes integrated/joint investigations among prefectural police. With the aim of speeding up the initial investigative stage, a Special Cybercrime Taskforce was established at the Metropolitan Police Department in July 2013 to provide relevant prefectural police with results of investigations conducted in Tokyo, where the head offices of financial institutions are concentrated.

III. Requesting Financial Institutions and Other Entities to Strengthen Security Capacity

The police are requesting financial institutions to strengthen security capacity for Internet banking, offering account information for freezing accounts abused in unlawful fund transfers and information on holders of frozen accounts, and advocating more stringent scrutiny of overseas remittances to fund transfer business operators. By doing so, some financial institutions have strengthened security capabilities through measures such as the utilization of a variable password generator (token) that enables the use of one-time passwords without email.

In addition, police are carrying out measures that include exchanging information with businesses offering antivirus software to detect botnets*2 abused in unlawful money transfers, and collaborating with telecommunications carriers and other entities to warn users of computers that incorporate these botnets.

Variable password generator (token) (image)

IV. Public Relations and Awareness Activity Conducted in Collaboration with Businesses

The police are collaborating with financial institutions to warn users about, and develop their knowledge of, the various modus operandi by which identification codes such as ID and passwords are unlawfully acquired.

In addition, since there have been cases where exchange students and technical interns have bought or sold accounts used in illegal remittance and have withdrawn funds, the police are working with the universities and businesses where such foreigners belong to, for awareness activity.

*2 Computers infected with a computer virus (bot) that operates based on commands from an attacker, or a network composed of a command server that sends commands from an attacker to these computers.