Application of information technology to combat cyber fraud

Anna S. Zueva[1], Daria A. Musatova[1], Valentina V. Britvina[2], Alexey Yu. Sorokin[3] and Gulmira E. Nurgazina[4]

[1] Lomonosov Moscow State University, 1, Leninskie Gory, Moscow, 119991, Russia
[2] Moscow Polytechnic University, 38, st. Bolshaya Semyonovskaya, Moscow, 107023, Russian Federation
[3] Academy of Civil Protection of the Ministry of Emergency Situations of Russia, 1, Sokolovskaya, Khimki, 141435, Russian Federation
[4] Russian State Academy of Intellectual Property, 55 a, Miklukho-Maklaya street, Moscow, 117279, Russian Federation
zueva@audit.msu.ru

Abstract. This paper is devoted to the consideration of various types of cyber attacks. The purpose of this paper is to analyze NFC fraud, phishing web pages, PayPal fraud, fake call centers. To explore this topic, we studied the experience of Canada in the field of cyber attacks. The article also discusses the most important aspects of banking and government regulation in this area and methods of combating cyber attacks.

Keywords: carding, cyber scamming, cyber-attacks, fraud, payment systems, phishing, NFC fraud.

1 Introduction

In a modern society there is a powerful trend of consumption. People are economically active as never before and consume enormous amounts of goods and services. More than that, people tend to prefer plastic cards to cash. A technological progress constantly brings up new improvements to payment systems, and banks advertise them as a more secure and advanced alternatives to carrying cash around. To find out if it is right or wrong, we are going to analyze the world of plastic cards, digital payment systems and find all possible dangers that can await bank customers. The technological progress not only provides newer options of how people can make transactions but it also gives thieves an access to a new area where they can commit crimes and still keep their identities hidden. As Javelin Strategy & Research says, about $6.4 billion were stolen from peoples' credit cards by scammers in 2018 in USA, and the number tends to grow. More and more people each year become victims of hackers, scammers that can collect personal information, control others' bank accounts and perform illegal activities.

The technological progress not only provides newer options of how people can make transactions but it also gives thieves an access to a new area where they can commit crimes and still keep their identities hidden. As Javelin Strategy & Research says, about $6.4 billion were stolen from peoples' credit cards by scammers in 2018 in USA, and the number tends to grow. More and more people each year become victims of hackers, scammers that can collect personal information, control others' bank accounts and perform illegal activities.

2 Materials and methods

In the process of writing this article, the following methods were used: methods of analyzing the literature, analyzing regulatory documents, comparing the experience of different states in the observable area, specific legal and comparative legal methods.

3 Results

People may not know but there is a constant danger of their bankcards to be attacked by the criminals. There are many types of scamming, we are going to touch the most common ones in order to find a way of protecting your bank accounts.

1. NFC Fraud

Most of modern cards have a NFC chip, which allows to perform transactions without entering your card in the payment terminal. So called "Paywave" technology is accepted everywhere and people tend to use it. Modern smartphones can mimic bankcards by using the NFC as well. What NFC does, is that it allows to hold a bankcard near payment terminal and make a purchase without entering PIN or swiping a card if the price of the purchase is under a certain limit that differs in regions. [3]

Criminals use that technology to perform low-cost transactions with a payment terminal. They can simply place the terminal close to your wallet and perform a "purchase" without you even knowing it. This type of fraud is best performed in crowded places like subway stations or malls. [4]

To fight this kind of a scam, people can protect their money by storing all the bankcards that feature NFC chips in special wallets that block any type of signal. If you wrap your mobile phone or a credit card in tinfoil, you will see that no signal is being received, nor any signal is being delivered. These wallets work the same way but instead of wrapping your cards in pieces of aluminum, you can simply extract cards from the wallet when they are needed. [7]

2. Phishing webpages

Phishing websites are a very old trick that has been used by credit card scammers for ages. These websites ask you to enter the whole information about your bankcard including a card number, an expiration date, a CVV code and a PIN. [12] First and foremost, no other individual should know your PIN and even no bank employee can ask you to name it. If anyone asks your PIN code, you must be sure that someone tries to scam you. As Internet Crime Complaint Center (IC3) states, $48,241,748 was reportedly lost per victim due to phishing attacks in 2018 (2018 Internet Crime Report).

On the other hand, online stores will always ask your CVV code in order to perform a payment. Phishing sites are usually presented as online stores, the main goal is to trick you. Creators of such sites make a fake version of famous online stores, such as Amazon or Ebay, and make them look identical to the real ones. In order to track whether you are being redirected to a phishing site, you should check the URL of this particular website. Buyers must use authentic websites, which can be found in Google, Yahoo or Bing. These searching websites have a strict policy that restricts any cyber frauds and developers always update their websites in order to protect users from entering phishing webpages. Modern browsers have built-in scanning programs that will alert you if something suspicious is happening, they will not allow you to enter a scamming website.

More than that, users should never enter links that could be sent to their e-mail addresses by suspicious accounts that they have never seen before, nor they should never click on advertisement pictures in order not to be scammed.

These easy tips will protect users from losing their money, thankfully, program developers always enhance and update their products in order to protect people that are not experienced enough or not even aware of such type of a scam.

3. PayPal scam

Many internet users, buyers and sellers, use such services like PayPal, Shopify or TranferWise. These technologies, particularly PayPal as the first ever and the most popular, allow you to transfer money, make payments via a website that has your bankcard attached to it. PayPal is a payment system that allows you to make safe transactions in a short time. It became popular at the time when worldwide transaction would take days or even weeks to send money from one bank account to another with enormous fees and losses on currency conversion. [9-11]

More than that, PayPal allows you to make full money return if you stumble upon a scammer while buying a good from an online auction. Ebay was growing rapidly and as it's popularity rose, PayPal became the only possible way of guaranteeing a safe purchase. If a particular good does not ship in time or if it is broken, Ebay will cancel the payment and return it back to you. [8]

Because of its popularity, PayPal scams started to be a common problem among people [1]. Any criminal could access your PayPal account if he previously got information about your e-mail address. Criminals can use your e-mail to change PayPal's password and block the access to your funds. Later, they would easily perform online purchases by using your identity and sell brand new goods to extract cash.

PayPal, being aware of this problem, started using two-factor authentication, which requires you to enter a newly generated code that was sent to your second e-mail address or your mobile phone. This safety feature was so good that most of other IT-companies have adopted it in order to secure their customers' private information [2].

In order not to become a victim of such illegal actions, people should never send their logins, passwords or e-mails that can give criminals any possibility to hack accounts and use others' savings. The only information that users can give publicity to is their unique nickname, which is needed to send money when a transaction is being made. This nickname corresponds to an account that has your delivery address and a bank account that will receive or send funds.

4. Fake call centers

In 2019 CBC Television published a very deep investigation on how Canadian bank customers can face a massive scam with low-interest credit cards. This story has started after CBC News journalists received a database that featured all the personal information of more than 3,000 Canadians including full names, birth dates, home addresses, credit card numbers, PINs and CVVs. As an investigation went on, journalist got the main idea of this fraud – scammers steal identities, not a credit card number. If scammers know enough information about you, they are able to make hundreds of new credit cards and get enormous revenues by using your identity.

Scammers, in order to collect data, make phone calls and present themselves as bank employee. These fake employees present you an option to lower credit card's interest rate by making one payment that can vary from $500 up to $5,000. As the phone call continues, scammers ask a customer to verify his personal data. It is known as the low-interest or rate reduction scam.

The victims of the fraud are often people who are full of debts. Such acting of a fake bank employee can easily attract them because they wish to find any possible way of minimizing their debts.

Speaking about scammers, there are illegal call centers in Pakistan that simply go through Yellow Pages and make calls to everyone. The reason why Canada attracts these scammers is countries' legislation and banks' safety policy.

Even if people reject to pay for this fee or do not give any personal information, it is already enough for criminals to collect the data. Scammers can use your mobile phone number and mimic it with another SIM card. Then they download bank's application or use official website to login under a stolen identity. Scammers can easily get the missing information about an individual by calling bank's office or using an official chat.

If a criminal did not succeed in withdrawing funds from the initial credit card, he is most likely to sell a list of people with all their personal information via Darknet. Darknet is a special part of internet that could not be accessed through well-known browsers like Safari, Internet Explorer or Google Chrome. To enter Darknet, you should install a special browser called Tor in order to look through illegal auctions that sell things like drugs, handguns, pornography and stolen credit card numbers. A special thing about Darknet is that a user cannot be tracked because of a special security system that hides user's IP-address and his location. All transaction in these auctions are made with crypto currency that cannot be tracked as well; buyers and sellers of illegal content and goods keep their identities completely anonymous.

The main problem why Canadians are in danger and why Canada is one of the most frequent requests in Darknet auctions is because Canadian government does not allow a credit freeze. What credit freeze is, it is an ability to block an access to the credit report. By blocking an access to the credit report, no information can be passed over and so no credit will be issued. This procedure is the most effective way to stop identity thefts. 50 of 51 states in the United States, except a state of Michigan, have a credit freeze law. Sad to say but Canada provides no option for people to make a credit freeze, thus bank accounts and identities of Canadians are still in a great danger. As Canadian Anti-Fraud Centre states, about $20,000,000 were lost to identity fraud in 2018.

4 Discussion

In order to fight cyber scamming, banks and government should cooperate and create a two-sided strategy how to minimize credit card and identity frauds. In 2018 IC3 observed and estimated about $2.7 billion losses because of cybercrime in USA only. If we collect the worldwide value of money stolen via different scamming methods, the numbers will be shocking [6].

Internet should be strictly controlled by the Secret Services because it is a area where scammers are allowed to openly buy and sell illegal goods without being afraid of being caught. Many countries still do not have laws that will punish hacking and scamming which allows criminals to switch between banks and customers they hunt. The best example of that will be Canadian imperfect law system that allows scammers from Pakistan to rob and trick people.

Huge IT-corporations like Google and Apple are very strict when it comes to their customers' privacy. These corporations often help American government in solving security problems and provide advanced technologies that were developed to protect American citizens' privacy. More than that, Apple or Google have enough influence to state about flawed laws and bring ideas of fixing them in order to eliminate a new fraud scheme for cybercriminals.

FBI has created its own cyber security departments, which work with online store operations, ID frauds and data breaches.

Such banks like Bank of America, Chase or Citi have enough influence and expertise to give advice about law improvements. In 2018 Center for Strategic and International Studies (CSIS) concluded that an economic damage to the global economy due to cybercrime was close to $600 billion. In order to have a stable economic market, banks and government should fight cyber scamming together.

In 2015 banks presented a new chip technology called EMV. It was designed to make bankcard more secure and to fight cloning. 4 years later, an amount of counterfeit operations fell drastically from $3.6 billion in 2015 to $1.7 billion in 2018.[5]

On the other hand, an example of Canadian epidemic of identity fraud shows that banks have to adjust and develop their security services in order to stop cybercrime. Negligence could not be allowed to continue and banks should value their customers' privacy over everything.

5 Conclusion

As we have previously discussed, there is a relevant problem of cybercrime in our society. The technological progress not only brings user-friendly applications and gadgets but it also gives birth to new and devious ways of stealing money and valuable information.

In order to protect their personal information and savings, people need to be more careful with their mobile devices, e-mails they receive and different calls they receive.

To let people know about the global scope of cybercrime, banks and government should engage mass media like radio stations, TV channels, newspapers, web bloggers with a mission to tell people about their insecurity.

Banks should develop and introduce more secure products to create a safer environment for customers and bankcard users. We all should remember that when money gets out of legal circulation, we will all suffer from it. Prices of goods and services will increase rapidly, while our disposable incomes will decrease. More than that, there will be a constant chance of losing all your savings because of personal information leakage or your own carelessness.

Our protection should stop being reactive, we cannot act and fix laws or security systems only after a crime is being committed.

Never the less, basic examples that have reviewed will definitely protect bank accounts and minimize the level of cyber frauds. Scamming is a serious problem that should never be dismissed and every individual should be familiar with it.

References

1. Fundera 2019 research, https://www.fundera.com/resources/cash-vs-credit-card-spending-statistics.
2. Forbes 2018 research, https://www.forbes.com/sites/tomgroenfeldt/2019/03/18/credit-card-fraud-is-down-but-account-fraud-which-directly-hurts-consumers-remains-high/#5442522020bf.
3. Coskun, V., Ozdenizci, B., Ok, K.: A survey on Near Field Communication (NFC) Technology. Wireless Personal Communications, 71(3), 2259-2294 (2013).
4. Turban, E., King, D., Lee, JK., Liang, TP., Turban, DC.: Electronic Commerce Payment Systems. Electronic Commerce. Springer Texts in Business and Economics. Springer, Cham., 519-557 (2015).
5. 2018 Internet Crime, https://www.thesslstore.com/blog/20-phishing-statistics-to-keep-you-from-getting-hooked-in-2019.
6. 2018 IC3, https://www.digitalshadows.com/blog-and-research/fbi-ic3-cybercrime-surges-in-2018-causing-2-7-billion-in-losses/.
7. EMV Chips, https://www.creditcards.com/emv-chip.
8. Identity and credit card frauds, https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.
9. Visa, https://en.wikipedia.org/wiki/Visa_Inc.
10. American Express, https://en.wikipedia.org/wiki/American_Express.
11. MasterCard, https://en.wikipedia.org/wiki/Mastercard.
12. Mobile Phishing Attacks and Mitigation Techniques. Journal of Information Security, http://www.scirp.org/journal/jis/.