SECURITY QUESTIONS of BANKS and SOCIAL MEDIA

HAZAL KERVAN

111680026

ISTANBUL BILGI UNIVERSITY

SOCIAL SCIENCES INSTUTE

MEDIA AND COMMUNICATION SYSTEMS

THESIS SUPERVISOR: Yrd. Doç. Dr. Erkan SAKA

Bankacılık Güvenlik Soruları ve Sosyal Medya

Hazal KERVAN

111680026

Tez Danışmanı: Yrd. Doç. Dr. Ethem Selen

Jüri Üyesi: Prof. Dr. Rüştü Aydoğan Boşnak

Jüri Üyesi: Doç. Dr. Itır Erhart

Tezin Onaylandığı Tarih: 06.02.2017

Toplam Sayfa Sayısı: 63

Anahtar Kelimeler (Türkçe):	Anahtar Kelimeler (İngilizce):
1) Bankacılık	1) Banking
2) Güvenlik Soruları	2) Security Questions
3) Sosyal Medya	3) Social Media
4) Şifre İşlemleri	4) Password Procedures
5) Kimlik Doğrulama	5)Authentication

ÖZET

Teknolojinin hızla gelişmesi, günümüz kullanıcıların alışkanlıklarını büyük ölçüde değiştirmiştir. Kullanıcılar finansal işlemlerini Banka şubelerine bizzat giderek yapmak yerine; internet, mobil ve çağrı merkezi gibi alternatif bankacılık Channellarını tercih etmeye başlamışlardır. Diğer bir yandan sosyal medyanın hayatımıza girmesiyle internet kullanıcıları çeşitli mecralarda kendileri hakkında kişisel bilgileri paylaşmaya başlamışlardır.

"Bankacılık Güvenlik Soruları ve Sosyal Medya" başlıklı bu tezin kapsamında, bankacılık kullanıcı hesaplarının güvenliği sorgulanmıştır. Sosyal medyada yer alan bilgiler ile kullanıcıların finansal hesapları internet bankacılığı, mobil bankacılık veya telefon bankacılığı üzerinden yetkisiz erişimlere açık olup olmadığı araştırılmıştır. Bu bağlamda bankaların kimlik doğrulamada esas aldıkları güvenlik soruları incelenmiştir. Facebook, Linkedin ve Instagram örneklem olarak seçilerek, Bankalar tarafından yöneltilen güvenlik sorularına ilişkin cevaplarının sosyal medya Channellarında olup olmadığı, diğer bir deyişle güvenlik sorularının cevaplarının ne kadar erişilebilir olup olmadığı araştırılmıştır.

Çalışmanın teori SECTIONünde; Türkiye'de Bankacılık sektörü, sektörün hızla gelişimi, kullanıcıların Bankacılık Channelları kullanımına ilişkin yönelim ve kimlik doğrulama konuları incelenmiştir. Tezin ikinci SECTIONünde sosyal medya mecralarından Facebook, Linkedin ve Instagram kullanımları ve bu Channellarda yer alan kişisel bilgiler belirlenmiştir.

Çalışmanın araştırma SECTIONünde; Bankacılık alternatif dağıtım Channellarında örneklem olarak seçilen Bankalar tarafından hazırlanmış güvenlik soruları incelenmiştir. Bu bağlamda her bir banka için; internet bankacılığı New Password işlemleri süreci, telefon bankacılığı Channelı üzerinden yeni internet bankacılığı password işlemleri ve telefon bankacılığı Channelı üzerinden yeni kredi kartı password işlemleri ve mobil bankacılık Channelı üzerinden New

Password işlemi süreci incelenmiştir. İnceleme sonuçları sosyal medya Channellarında yer alan kişisel bilgiler ile eşleştirilerek bir model oluşturulmuştur.

Sonuç SECTIONünde, güvenlik sorularının yeterliliği, olası tehditler ve kullanıcıların gizli bilgiler konusunda bilinçlendirilmesi gerektiği değerlendirilmiştir.

Anahtar Kelimeler: Bankacılık, Güvenlik Soruları, Password İşlemleri, Sosyal Medya, Kimlik Doğrulama

ABSTRACT

Rapid development of technology has changed the habit of users highly. Instead of managing financial transactions by physically visiting Bank's branch offices; users have started to prefer alternative banking channels such as internet, mobile and call center. On the other hand, social media has adopted in daily life, internet users have started to share information about themselves in mutual platforms.

Within the scope of this "Thesis regarding to Security Questions of Banks and Social Media" headlined thesis, the security of banking user accounts are questioned. Considering the information in social media, unauthorized access to user's financial accounts on internet banking, mobile banking and call center are questioned. Thus, the security questions that Bank's are currently using for authentication are examined. Facebook, Linkedin and Instagram are chosen as sample to research whether the answers of the security questions provided by Banks could be found in social media channels. In other words, accessiblity of security questions are examined.

In theory part of the thesis, Banking sector in Turkey, rapid development of sector, tendency of usage of Banking channels and authentications are examined. In the second part of the thesis, usage of Facebook, Linkedin and Instagram and the personal information stored in these channels are clarified.

In the research part of the thesis, the security questions of the Banks that are chosen as sample are examined within the scope of alternative delivery channels. Therefore, for each bank, processes of new password for internet banking, new internet banking password process on call center and new credit card password on call center and nw password process on mobile banking applications are analyzed. As a result of analysis are matched with the personal information located on the social media channels, a model is obtained.

On the summary section, sufficiency of the security questions, possible threaths and the neccesity of raising awareness to customes is evaluated.

Key Words: Banking, Security Questions, Password Process, Social Media, Authentication

LIST OF ABBREVIATIONS

BRSA: Banking Regulation and Supervision Agency

CVV: CVV Code or security number that consists of the last 3 digits of the numbers that are generally printed on the white field available on the back of the credit cards.

Transaction Authentication Number: A code that consists of a series of alphabetic and/or numeric characters of a certain length, created for one-time use only when a customer to verify the transaction they wish to carry out once they have been recognised by the system by means of one of the identity verification methods, to state whether he approves the transaction that is about to be realized.

Deposit bank: The institutions that operate with the main purpose of accepting deposits and extending credit on their own behalf as well as the branches of overseas institutions of this nature in Turkey.

Participation bank: The institutions that operate with the main purpose of collecting funds by means of special current and participation accounts and extending credit, as well as the branches of overseas institutions of this nature in Turkey.

Development and investment bank: Other than accepting deposits or participation funds; the institutions that essentially operate to extend credit and/or perform the tasks assigned to them in special laws, as well as the branches of overseas institutions of this nature in Turkey.

SMS: The messaging service that involves sending a text message from one phone to another.

TBB: The Banks Association of Turkey

TRID: Turkish Republic Identity Number

CONTENTS

SECTION 1

SUBJECT of THESIS

1.1 SCOPE of THESIS

Social communication websites are not only limited with the function of communication. It also enables users to reach the information they require, and let informatics to spread in a rapid way. (Sönmez, 2013) In this direction, in an environment where private information of social media users are accessed, it is questioned that the accessibility of the answers of the security questions of banks and therefore whether they are in line with supportying user securtiy or not is examined. It will be researched that performing banking transactions via a person with the aim of fraud with the knowledge of information obtained from social media. Within the method of the summary; accessing private information on social media is limited with read only access. Hacking user acconts and performing fraud via using that accounts are not in the scope of this thesis.

1.2 BANKS CHOSEN AS SAMPLE

Within this thesis work, 5 banks are chosen as sample where 2 of them provides new generation banking service. The banks listed below are selected as sample.

- İş Bank- BANK A
- Garanti- BANK B
- ING – BANK C
- Finansbank(Enpara) -BANK D
- Teb (CepteTEB) – BANK E

1.3 PROCESSES CHOSEN AS SAMPLE

Within the scope of thesis “Security Questions of Banks and Social Media“, access of banking process will be analiyzed since any banking transaction (i.e. Money transfers, payment of credit cards, payment of bills and transfering Money to mobile phones) is available through that channel. The channels where a new password is obtained will be examined. This channels are clarified as internet banking, call center and mobile banking. It will be questioned that whether the answers of the security questions can be accessed on social media or not.

Ass a result of all this analysis work, the strenght of security questions of Turkish banking sector will be tested.

SECTION 2

BANKING SECTOR IN TURKEY

2.1 GENERAL INFORMATION

Wikipedia defines a Bank as an institution that extends credit to and protects deposit accounts of people and/or enterprises, as well as performing any and all kinds of capital, money and credit related transactions.

The Turkish banking sector has been through rough periods in parallel to various economic crisis experienced. The economic crisis of 2001 resulted in the transfer of many banks to the Savings Deposit Insurance Fund (SDIF).

Erdönmez stated that "A Strong Economic Transition Program' was put into action in Turkey in May 2001 for purposes of re-structuring the institutional sector, mitigating the effects of the crisis and reestablishing economic stability in the aftermath of the financial crisis experienced in the year 2001." The Banking Regulation and Supervision Agency (BRSA) was established on 31 August 2000 for purposes of protecting the rights and interests of the account owners. The purpose of BRSA is to implement the "Banking Sector Re-Structuring Program". For this reason, a system that would enable decision making on the regulations that the banks are subject to and the follow-up of decisions taken to strengthen the foundation of the economy, was developed. BRSA is an independent institution that is not subject to the orders or auditing of any other body.

According to BRSA data, the total assets of the banking sector reached TRY 2.48 trillion (USD 859 billion) as of June 2016. As of December 2015 the market is shared by a total of 50 banks, among which 32 are deposit collecting institutions, 13 development and investment banks and 5 are participation banks.

It is true that many services are provided to customers virtually by means of the technologies we currently employ. Some banks have started providing digital banking services on the basis of the convenience offered by current technologies. Branchless banking services constitute the basis of digital banking.

Digital banking is the structural organization whereby the banking transactions are performed via the internet or over the phone without the need to visit a branch (www.bankalar.org). In consideration of the fact that 60% of banking transactions are currently being handled outside the branches, investing in branchless banking is predicted to be quite advantageous. Banks arrange meetings with customers who apply for digital banking services at a time and place convenient to them to sign the service agreement and obtain transaction permission slips that they are subject to. Either during these meetings or later on via a courier service, the deposit account card or credit card is provided to the customer. The absence of any branch related expenses means banks don't need to charge any fees or can charge lower fees for banking services, thus increasing the popularity of this type of service.

2.2 BANKING CHANNELS

2.2.1 Internet Banking

Internet Banking has been defined as the "Banking Services Channel that ensures customer access to the services offered by the bank as well as the performance of their transactions via the internet" in the Principles Communique that was published by BRSA.

It has been stated in the book "Bankalarımız" (Our Banks), which was published by the Banks Association of Turkey (TBB) on the basis of 2015 year-end data, that 17.4 million people performed internet Banking transactions and 93% of these were retail customers.

An examination of the "Internet and Mobile Banking Statistics" report that was published in June 2016 by TBB reveals that 26,113 people have logged into internet banking at least once

in the last year. On the other hand the number of the active singular users that logged onto internet banking at least once in the last 3 months has been determined as 17,019.

	June 2015		**March 2016**		**June 2016**	
	Number of Transactions (Thousand)	**Transaction Volume (Million TRY)**	**Number of Transactions (Thousand)**	**Transaction Volume (Million TRY)**	**Number of Transactions (Thousand)**	**Transaction Volume (Million TRY)**
Money transfers	63,860	516,836	68,285	571,449	73,011	675,769
Payments	50,263	33,092	48,699	38,110	45,304	39,107
Investment transactions	11,305	155,299	10,743	156,415	10,879	156,304
Credit card transactions	11,862	17,792	12,303	17,778	11,965	18,167
Other financial transactions	3,471	30,610	3,801	32,614	3,766	41,426
Total	**140,760**	**753,630**	**143,831**	**816,366**	**144,925**	**930,772**

TABLE – TBB – Internet and Mobile Banking Statistics Report, June 2016

TABLE 1

The table provided in the report in regards to financial transactions performed through internet banking shows the total transaction volume as TRY 930,772 million, pointing to the fact that in our country, a significant transaction volume is being handled through alternative channels.

2.2.2 Mobile Banking

The need for mobile banking has arisen as mobile phones have become an integral part of our lives. Mobile banking involves the realization of banking transactions via smart phones channel. The institutional applications that are downloaded to smart phones enable users to have access to the system by using their user details, and conduct banking transactions conveniently and easily without paying a visit to their branch, in a manner similar to internet banking. Access to the bank's system through this application is possible by entering the customer number or TRID specific to the user matched with the correct password followed by the correct entry of the authentication number sent to the mobile phone number of the customer registered in the database of the Bank.

The distinguishing difference between mobile and internet banking is the mobile number that is considered to be the identity of the user. So much so that, the majority of the institutions allow customers that are trying to access their systems through mobile banking channel, to log in without an authentication number upon entry of the correct user name and password and verification of the mobile phone number used as belonging to the customer attempting the access through queries. In other words, the use of the correct user name and password has become sufficient to gain access to the mobile banking application.

2.2.3 Telephone Banking

All the banks in Turkey provide telephone banking services. Telephone banking is based on the use of a password determined by the customer to access his/her account information over the phone, and the use of prompts issued by the phone keys to perform the transaction (H. Siphai). Similar to mobile banking, the telephone banking channel enables the customer to perform his/her transactions without paying a visit to the branch. Banks share account information and

allow customers to complete transactions via telephone banking after verifying that the customers is in fact their customer.

2.3 IDENTITY VERIFICATION METHODS

2.3.1 Security Question

The institutions have designed processes to create new passwords in case the customer forgets previously provided information. In this context, the banks prepare security questions that focus on verifying the identity and confirming the status of the customer. The mother's maiden name is among the most frequently asked question. However, due to technological advancements and legal requirements, it is currently necessary to ask more than one question to verify the identity of the user.

2.3.2 Legislation

In 2007, BRSA issued a Principles Communique that would be essential in the management of banks' information systems. Banks are required to set up their information systems according to this communique. The principles pertaining to the identity verification of the customers receiving banking services are defined as per this communique. In the communique, identity verification is defined as the "mechanism that ensures the identity declared actually belongs to the person who makes the declaration". The principles pertaining to identity verification are stipulated in article 9.

Identity verification

ARTICLE 9-(1) *An identity verification system that is suitable for the transactions that are performed through information systems is established. The identity verification techniques used are decided according to the results of a risk evaluation conducted by senior management. The risk evaluation is performed in consideration of the type of transaction planned to be performed in the information systems (type, nature, if any, the financial and non-financial repercussions*

the transaction might have), the sensitivity of the data subject to the transaction and the ease of use of the identity verification technique.

In this article, the transactions performed by information systems cover all channels, other than branches, through which such transactions are handled. BRSA does not establish the rules pertaining to the identity verification process. It is essential that the related rules are determined in line with the decisions of senior management in each and every bank. Accordingly, each bank applies different rules. However, BRSA requires that the identity verification process is applied from the start to the end of the banking process initiated by the customer.

Article 9 - 3 focuses on the secure maintenance of customer information in the databases of the banks and will not be examined within the scope of this thesis.

The principles pertaining to internet banking identity verification are outlined in a separate article (Article 27) due to the fact that internet banking is the most used alternative distribution channel.

Identity verification

ARTICLE 27 -

(1) Regarding the internet banking services offered, the Bank must establish a reliable identity verification mechanism that is commensurate with the risk levels these services pose. And the bank must also develop a structure that does not allow its customers to use these services without first passing through the established identity verification mechanism.

(2) When determining the risk levels associated with this kind of service, at least the following needs to be considered:

a) Customer type,

b) Means provided to the customer to perform transactions,

c) Sensitivity of the information shared between the bank and customer,

d) Communication infrastructure used and

e) Transaction volume.

(3) The identity verification process regarding internet banking is performed for all parties involved, such as the bank, or customer that is the party to the transaction and if any, the support services entity.

(4) The identity verification mechanism applicable to the customers consists of at least 2 components independent of each other. These two components are chosen from two different groups of factors that customers "knew", "has" or that are a "biometric characteristic" of the customer. The factors customer "knew" could be the components such as the password/variable password, where as the ones customer "has" could be the single use password creation device or the password provided by means of the short messaging service for single use. The components must be completely specific to the customer and identity verification must not be complete and access to services must not be provided prior to the provision of the necessary information.

(14) In the systems to be installed and applications to be developed, the bank, regarding its systems and software, takes the necessary measures against all known attacks oriented to the possible seizure of identity verification information belonging to its customers and personnel.

In Article 27-4, the requirement that "the identity verification mechanism must consist of at least two components" is mentioned. BRSA considers these components in 3 different groups as follows: "Customer knew", "Customer has" and "biometric characteristic". The "customer knew" factor could be the password, the "customer has" factor could be devices like OTP that produce single use passwords or passwords provided via a text messaging service. The customer is prohibited from realizing a transaction or viewing the account prior to completing the identity verification process.

SECTION 3

USE OF SOCIAL MEDIA

3.1 GENERAL INFORMATION

Within the rapid technological changes occured in communication, the coverage zone of web has been expanded. With Web 2.0 technologic improvements has reached level of comprising many users. As Tim O'Reilly described, a trend of creating content via participation and cooperation of visitors has occurred. In other words, communication platforms, wikis and other communications tools started to take part in our lives. Therefore, a new communication genre in which single users use internet for virtual communication and Express themselves on this platforms has been initiated.

İşlek stated that new media has improved to access of information via new channells and users meet in a platform where they acccess data with social weds. Therefore, except from passive consumption provided via traditional media, there is an interaction within the social media. (Lister and others, 2009:21). At this point, it could be said that social bounds occurred within the interaction of single users with each others have started to shape the new internet. Pempek described social network sites as a community in which users join a community with user names(nicknames), share profiles with eachother, send general and/or private voice, photograph, messages, video for communication. As İşlek has stated, social network sites connects web users that share contents with each other with social network system.

In order to research current use od internet, a digital agency called We Are Social has published "Digital 2016" that is a global social media usage work. Statistics of Turkey that are subject to related report are exmined and it is clarified that 46,3 millon of 79,14 people are active social media users. Also, it is observed that 36 million users are accessing social media through mobile phones. In other words, it is observed that 58,5% of Turkish people are actively using

internet while 45,5% of Turkish people are actively using their mobile phones. Aditionally, when the fact of 77% of active internet users are online everyday is considered, it could be said that in parallel to the rapid tehnological changes, Turkish people ae adapting to the new communication methods. In the work " Social Media Report in Turkey" of Mehmet Kartal, via defining socail media as final step of information technlogies, he clarified that social media run through traditional media methods, and when percentages of social media usage is considered, it secured its position.

3.2 FACEBOOK

3.2.1 Usage of Facebook

Within Web 2.0, an era of single users are using internet for the purpose of virtual communication and expressing themsevles through platforms have been started. Throughout this platforms, Facebook which is built up in 2004 is the biggests social network building platform. It provides services of having friendship, uploading photos and videos, spreading instant status updates and sharng information of ther platforms. With this oppurtunities, users are contributing to this channel to grow via creating contents. Facebook enlarged itself within time and incoporte into Messenger, Instagram, Whatsup and Oculus VR.

At present time, when this one of the most popular social network Facebook's usage trend though the World is analyzed, it is observed that within the period of 2010-2014 there is an serious increase of %224,4 occurred. As a result of a research performed on 30.06.2016, it is observed that 49,5% of World population are clarified as internet users and half of this users are concluded to be Facebook users. When the active user amount is stated as 17 billion in Wikipedia. In "Digital 2016" report, Turkey's most used social media platform is clarified as Facebook with the ratio of 32%.

When usage statistics of Turkey by sex is analyzed, it is observed that 37% of the users are women. In related research Works, it is stated it in previous year, the ratio of women using internet was observed as 36%, therefore there is a minimum amount of change in this ratio.

The research of "Facebook Usage in Turkey" published by Şenel, the rations of intenert usage by age are given below.

- % 31.6--- 25-30,
- % 30.4--- 18-24,
- % 26.9--- 31-40,
- % 7.9----- 13-17,
- % 3.2------41-65

Şenel stated that "This research is in line with Facebook's own data. With the ratio of % 44, the biggest part of facebook usage belongs to the age group of 18-24."

3.2.2 Personal Information Stored in Facebook

Facebook, connects single users that share information on their personal lifes. Users should sign up this platform with a user name. Real-name policy is adopted in Facebook. Via providing the service of informing aganst fake accounts, related accounts are banned after the analysis of that accounts. This case could be consired as a compensative control mechanism in order to protect the security of accounts that are created via real person information. In other words, Facebook encourage users to choose their own name and surname as their nicknames.

On Facebook, people can be friends with the persons they know or not. After accepting the friendship request, due to the profile access limits, information that is shared by user are accessed in a read-only way. Users can tag their close environment (family, close friend, boyfriend/girlfriend, husband/wife) etc. as in their info part. Also, even tough users do not use

related tagging method, within the scope of the sharings, users relations with other users can be observed. For instance, fom the content of a post within the theme of mother's da or a valentine's day photo or a photo of siblings can give a clue of the degree.

With the surname law, it is legalized to use Maiden Name for women when they are married. Within the scope of this law,it is observed that women are using their both surnames on Facebook. Additionally, it is analyzed that divorced women are using their Maiden Names as their surname on Facebook. As of day, if those women have a child above age 18, it can be said that child's Maiden Name information can be obtained easily through Facebook. Therefore, it can be concluded that Maiden Name is an accessable information through Facebook.

Users may share the information of ther mobile phone numbers in general information section of Facebook. Also, it is observed that users that change their mobile phone numbers or lost the numbers on their phone book share the information of their mobile phone number on their Facebook Wall. Additionally, users may share the mobile phone number information via sending direct messages to other users.

3.3 LINKEDIN

3.3.1 Usage of Linkedin

On Wikipedia, Linkedin is described as "a Professional social network platforrm in which people in business can communicate with others and share informatics". Linkedin that built up in 2003, provides services on both internet and mobile channells. Currently, there are 433 trillion active users. (http://m.haberturk.com/ekonomi/teknoloji/haber/1255438-satista-sira-twittera-geldi) It is observed that, at the end of 2015, they have total income of 2,990.91 million dollar. (http://www.google.com/finance?q=NYSE:LNKD&fstype=ii).

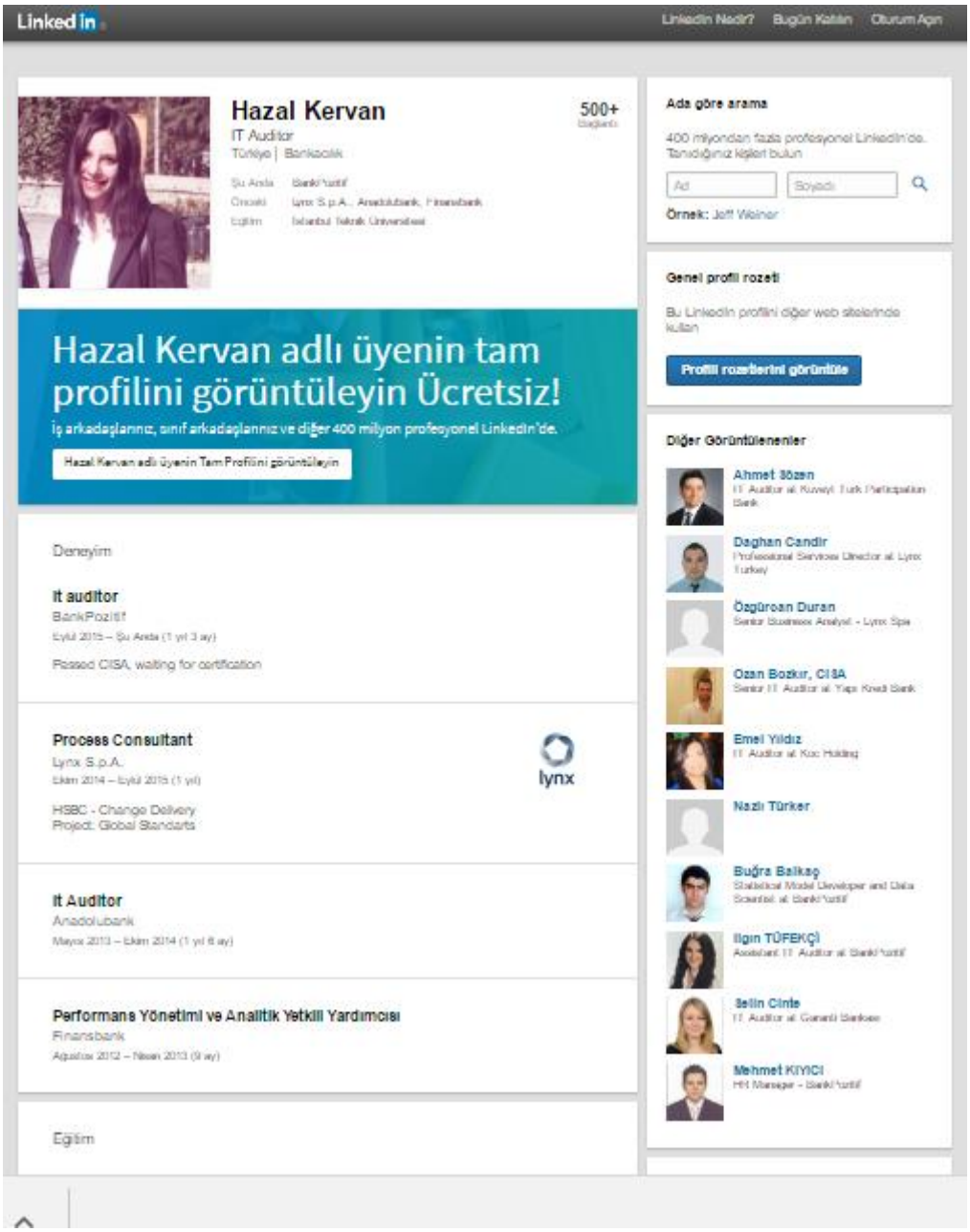
Social network provided by Linkedin is both used by persons and companies.Companies share the news of current news, changes and communicate with the users that work under the

company. Also, companies can share current job posts on their Linkedin pages. Single users can share detailed information of their CVs on their Linkedin page as in the detail of they wish. A CV template is provided by Linkedin in default settings and single users may add the information of their career, education and photos. Single users can connect with both the persons they know and the persons that they are willing to communicate. Also, they can vivew the detail of job postings and apply to them. Single users are joining to this platform via using their real names..

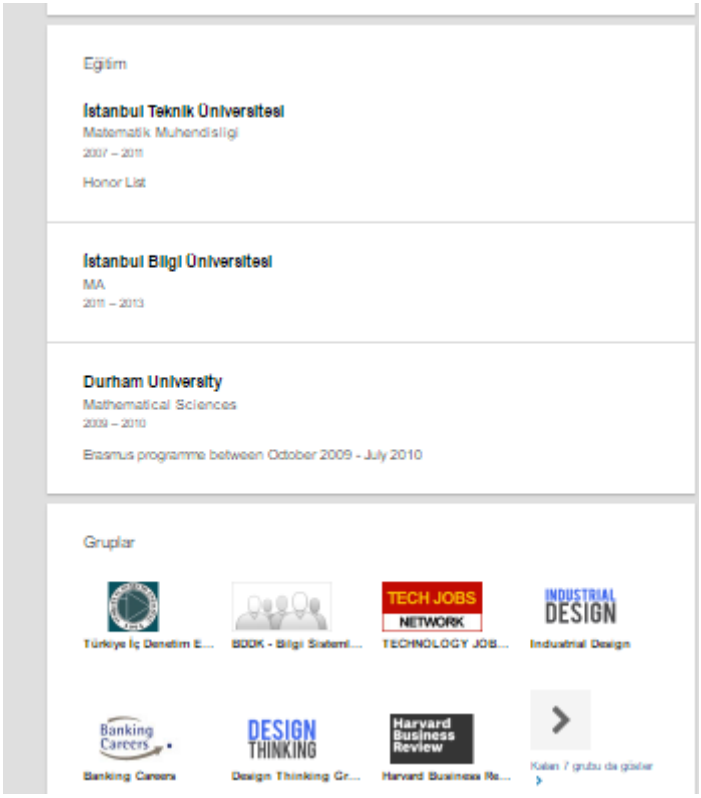
3.3.2 Personal Information Stored in Linkedin

Linkedin platform can be defined as business world's Facebook. Apart from Facebook, it is observed that usrs are in the habit of sharing Professional posts (promotion, searching for new job, current evaluations in their business field) instead of sharing posts from their Daily lifes. Additionally, users share the information of personal information such as their e-mails and mobile phone numbers.

Linkedin provide their services free of charge. However, they provide exclusive services for users that pay an amount. However, in basic, in order to see user information, there is no limitation of having an account in Linkedin. Any user willing to see a Linkedin profile can access the information simply searching "name surname linkedin" on Google. Sometimes, users may have similar names with other users. In that case, in order to recognise the user that is searched for, profile pictures or personal information (i.e. current comapny or the graduated school) are considered as severalizing information to find the searched user.


LinkedIn
LinkedIn Nedir?
Bugün Katılın
Oturum Açın
Hazal Kervan
IT Auditor
Türkiye | Bankacılık
500+
Ada göre arama
400 milyondan fazla profesyonel LinkedIn'de. Tanıdığınız kişileri bulun
Ad
Soyadı
Örnek: Jeff Weiner
Genel profil rozeti
Bu LinkedIn profilini diğer web sitelerinde kullan
Profili rozetlerini görüntüle
Hazal Kervan adlı üyenin tam profilini görüntüleyin Ücretsiz!
İş arkadaşlarınız, sınıf arkadaşlarınız ve diğer 400 milyon profesyonel LinkedIn'de.
Hazal Kervan adlı üyenin Tam Profilini görüntüleyin
Deneyim
It auditor
BankPozitif
Passed CISA, waiting for certification
Process Consultant
Lynx S.p.A.
HSBC - Change Delivery
Project: Global Standarts
lynx
It Auditor
Anadolubank
Performans Yönetimi ve Analitik Yetkili Yardımcısı
Finansbank
Eğitim
Diğer Görüntülenenler
Ahmet Sözen
Doğan Candır
Özgüroan Duran
Ozan Bozkır, CISA
Emel Yıldız
Nazlı Türker
Buğra Balkaş
Ilgın TÜFEKÇİ
Selin Cinte
Mehmet KIYICI

PICTURE 1



PICTURE 2

3.4 INSTAGRAM

3.4.1 Usage of Instagram

Instagram is a social network that provides the ability of sharing photos and videos on both internet and mobile channels. It is built up on 06.10.2010. It was invested by on April 2012 with 30 million active users and currently Instagram has 5000 million users. Facebook

3.4.2 Personal Information Stored in Instagram

Apart form Facebook and Linkedin, Instagram is a platform that users do not require to select their real names. Users can share informatics both via selecting either their own names or using nicknames. There is a fusntion of sharing the same informatics as in the same time on Facebook and/or twitter if asked.

On instagram application, the instagram profiles of the users that are in your phone book and user's Facebook friends are visable and if wanted, following requests can be sent to that users.

Users may use Instagram for personal and/or commercial purposes. Personal users share photos and/or videos of their Daily lifes with or without filters. Using of hashtags are smileys are available.

There is a possibility of accessing Maiden Name of users through Instagram. This case is only valid for if the user shares a media with the content of family and user's mother may be tagged or commented on the media. Maiden Name can be easily accessed if mother and the user using different surnames on their accounts.

3.5 PERSONAL INFORMATION CAN BE ACCESSED THROUGH SOCIAL MEDIA

Within the scope of security questions of banks, the information might be obtained through social media channels are examined and stated in the table below.

	Mobile Phone Number	**Maiden Name**	**Name of Mother**	**Name of Father**	**ZBirth Date**	**Birth Place**
Facebook	+	+	+	+	+	+
Linkedin	+	-	-	-	+	-
Instagram	-	+	+	+	-	-

TABLE 2

Additionally, due to the content of the shared information, a knowledge of user's kinsmeni family, pets and workplace can be obtained. Within the scope of this thesis, in terms of security questions whether this informations are required or not will be examined.

SECTION 4

SECURİTY QUESTIONS OF BANKS

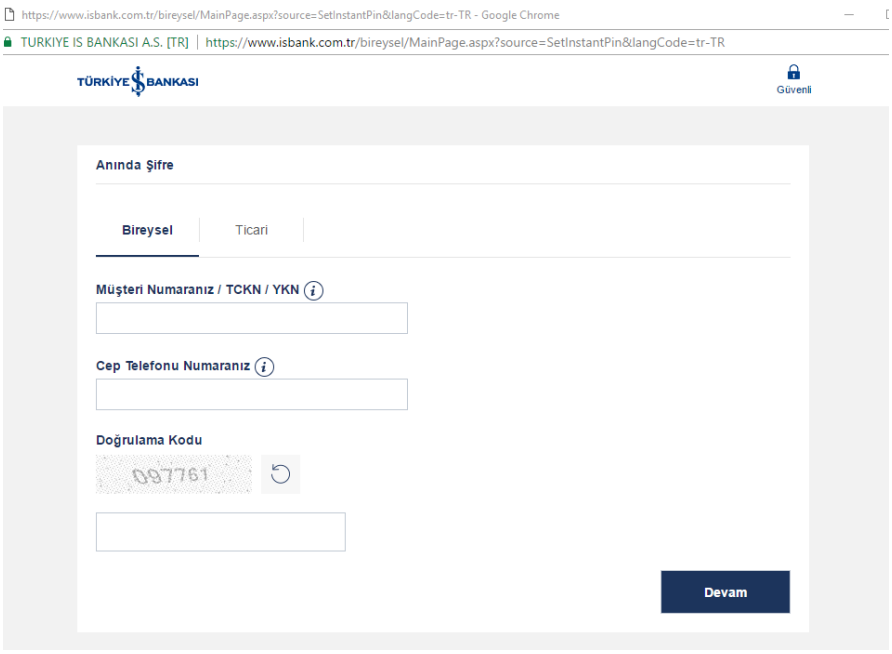
4.1 SCOPE

Within this thesis work, 5 banks are chosen as sample where 2 of them provides new generation banking service. The banks listed below are selected as sample. For each bank, security questions of new password process on internet banking, mobile banking and call center are examined.

4.2 SECURITY QUESTIONS OF BANK A

4.2.1 New Password Process on Internet Banking Channel

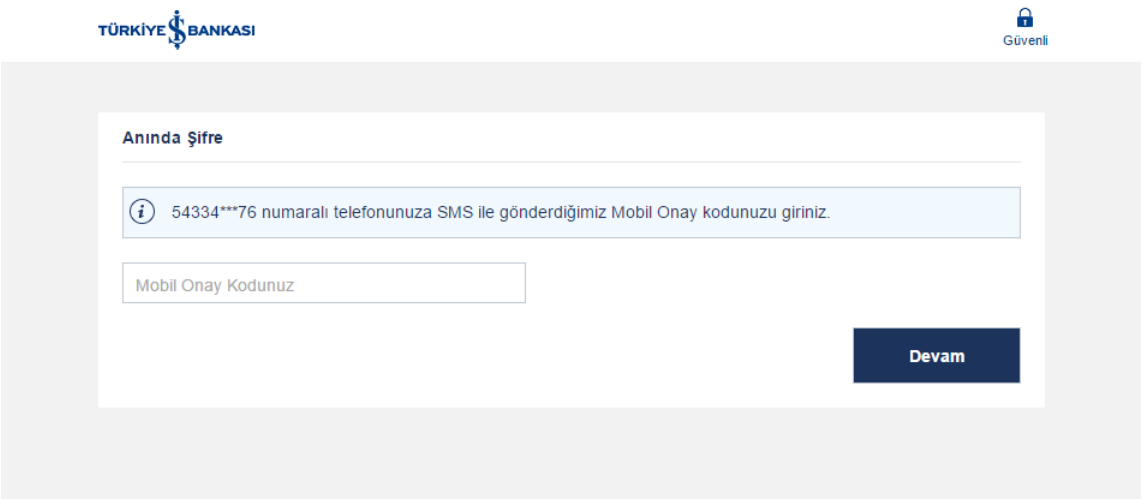
For Bank A, "Immediate Password – Forgot My Password" section on their web site is clicked and related questions asked (TRID, Mobile Phone Number, Verification Code) are presented in Picture 3.



PICTURE 3

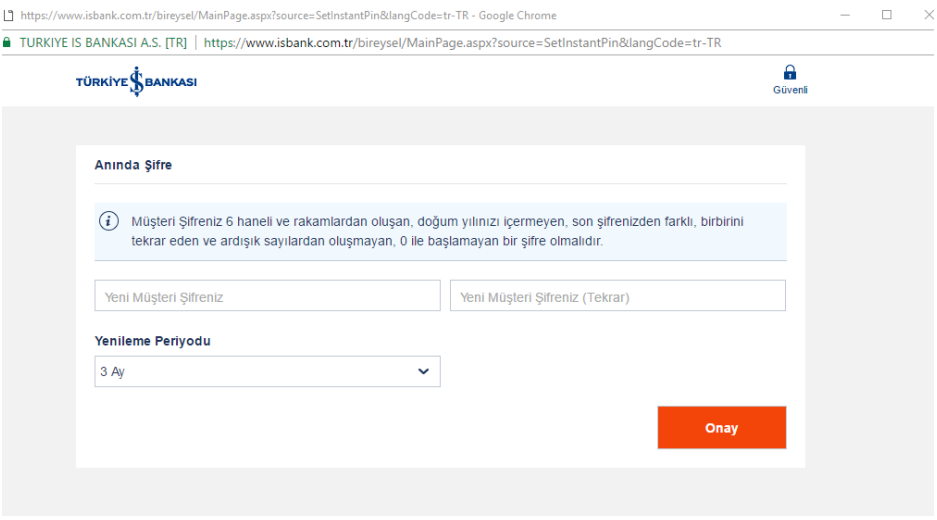
For retail customers that are in the scope of thesis, customer numer or TRID or citizen number for foreign customers are asked and addtionally, mobile phone number that recorded in Bank's database and verification code to check whether a robot is trying to access any information or not are asked.

When those informations are validated, a SMS code asked that is sent to customer's mobile phone as shown in Picture 4.



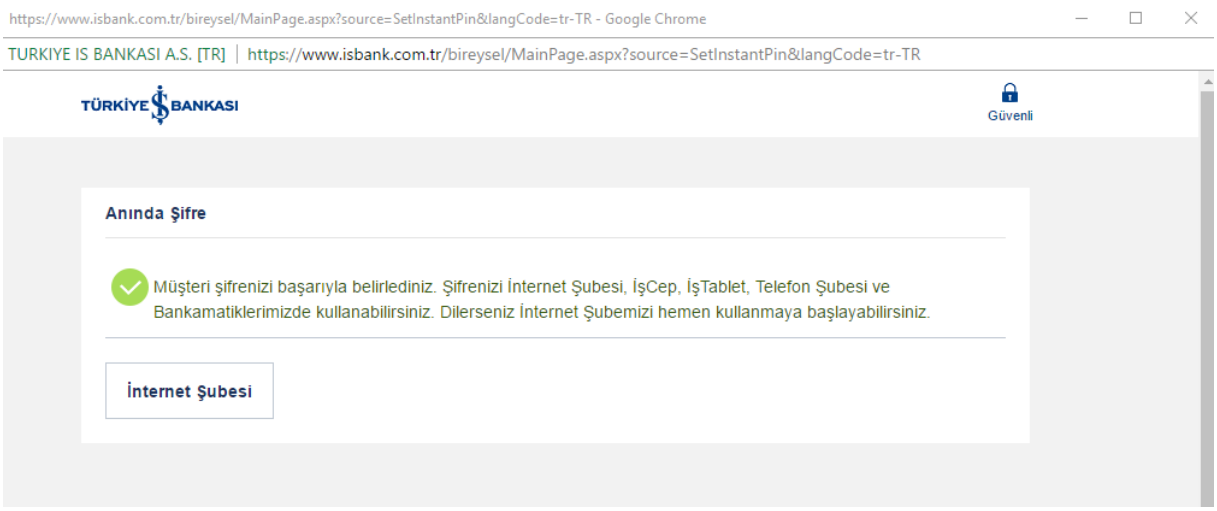
PICTURE 4

When SMS code is validated, it is seen that new password is created, as shown in Picture 5.



PICTURE 5

After clearifying password, the information of usage of this password on intertnet, mobile and call center channels is obtained. Additionally, a SMS sent to cutsomer's mobile phone with the information of a change in password had been occurred.



PICTURE 6

The password model of BANK A's internet banking channel is analyzed as; (TRID + Mobile Phone Number +Authentication Number) + SMS = New Password.

4.2.2 New Password Process on Call Center Channel

The number stated in BANK A's internet web site is called, and the menu of obtaining new password is selected. It is observed that BANK A asks the information below for all call center menus.

-Customer number – password

-Credit Card Number – password of card

-Account number – password of plastic card

Via selecting customer representive menü, a new internet banking password is asked. In related field, customer number is asked. Without validatin this information, other questions are not

asked. Since that information can not be obtained through social media channels, this process is left out of scope.

4.2.3 New Password Process on Mobile Banking Channel

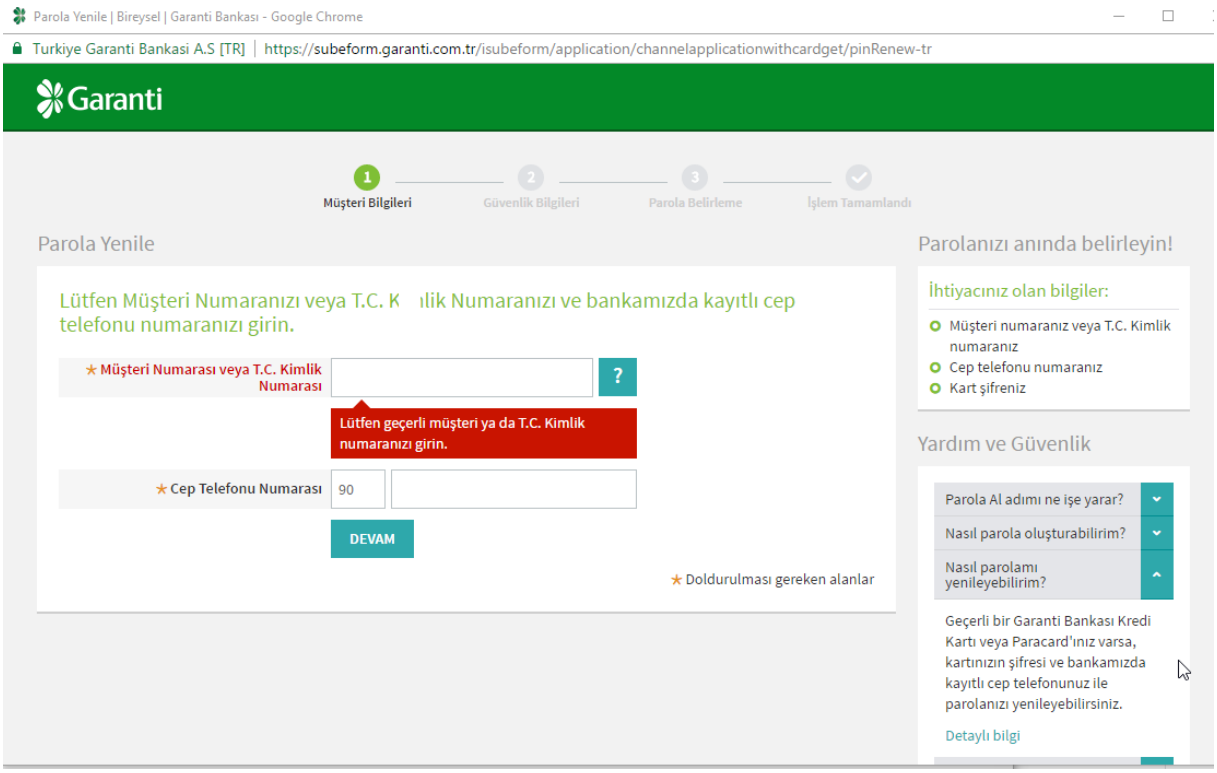
Mobile banking application of BANK A is downloaded on smart phone and new password process is examined via clicking “Forgot my password” field.

In new password process, customer’s TRID and mobile phone number information are required to be validated on the first screen. Later, an authentcation message to customer’s mobile phone number that is stored in Bank’s database is sent. After validating the authentication number, with the validation of information of card number, card’s epire date, security code (CVV) and password of card, creation of new password is seen as available.

4.3 SECURITY QUESTIONS OF BANK B

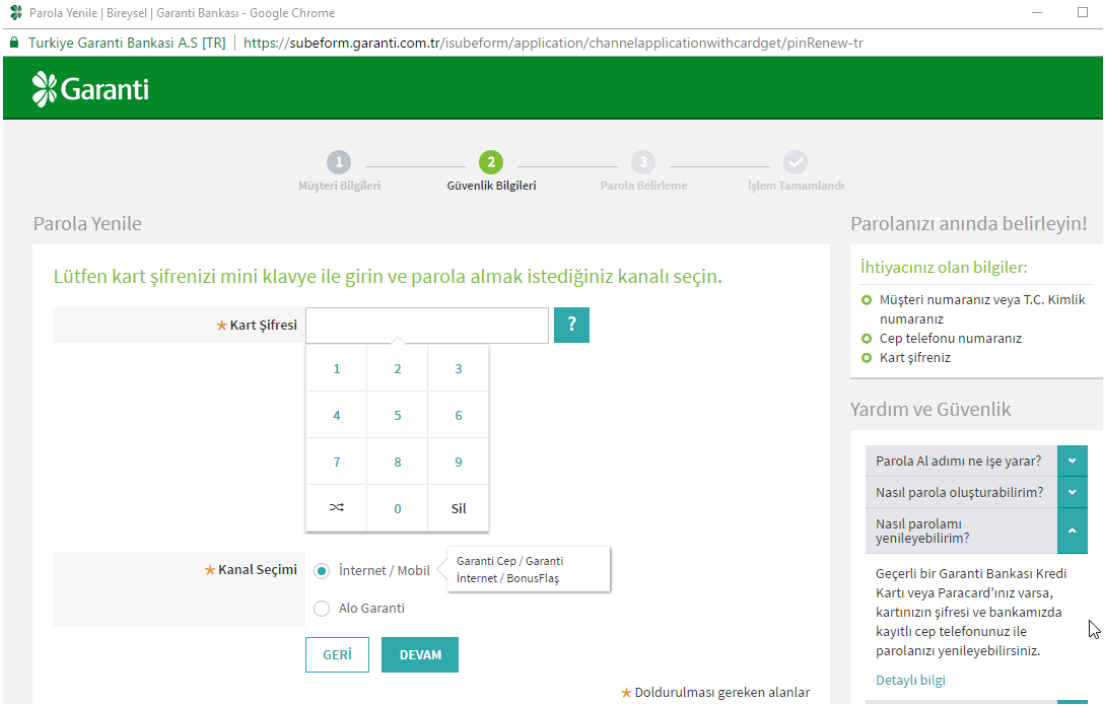
4.3.1 New Password Process on Internet Banking Channel

For Bank B, “Immediate Password – Forgot My Password” section on their web site is clicked then it is seen that questions of customer number or TRID and mobile phone number information is asked as stated in Picture 7.



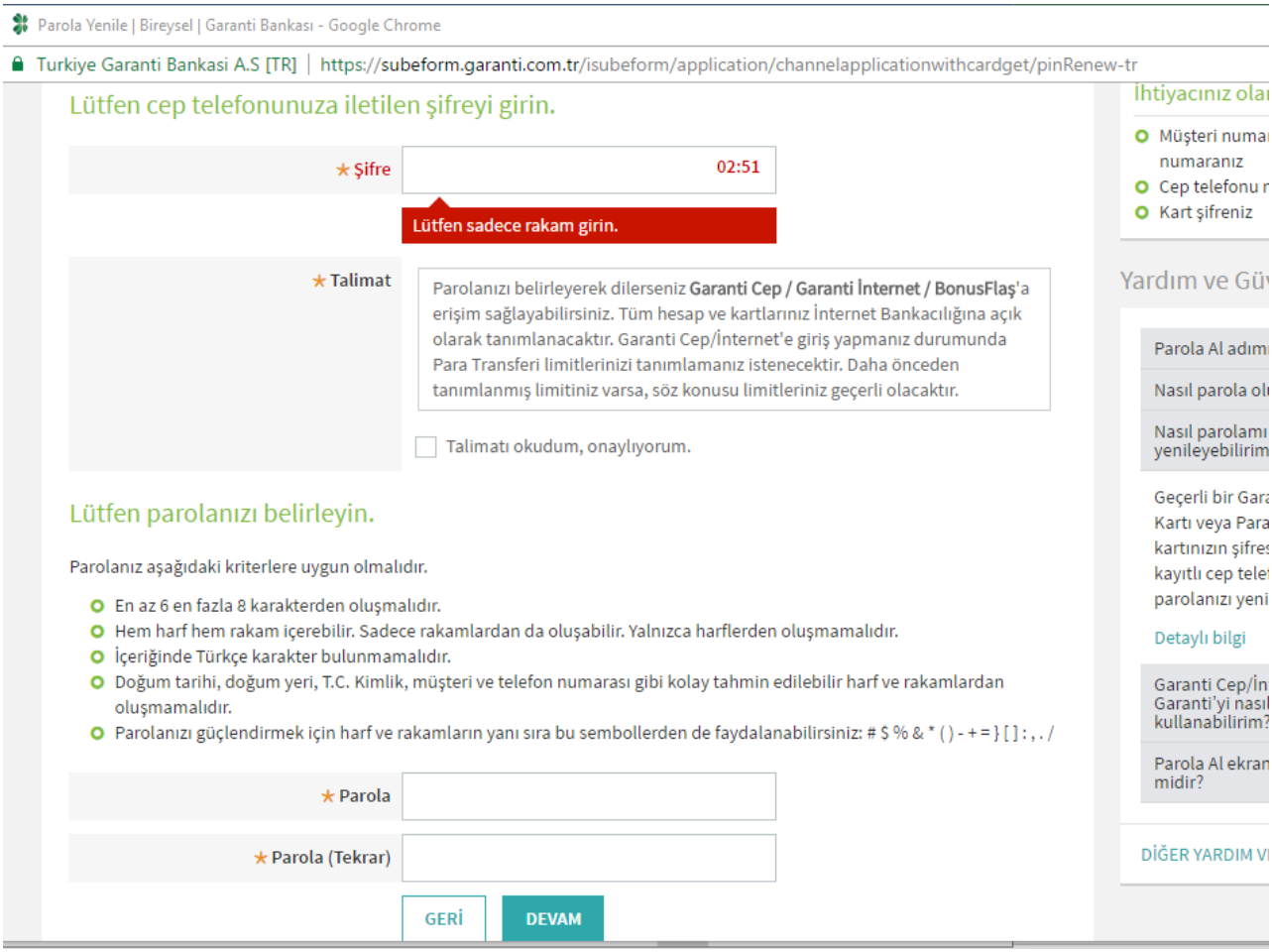
PICTURE 7

When the right information is filled, it is seen that the information of password of card is asked with channel information (Picture 8).



PICTURE 8

When the information asked is analyzed in details, it is observed that the password asked is related with any password information of any card of Bank B.



PICTURE 9

After fullfiliing the right verification code sent to the mobile phone number, the password is decided. It is seen that internet banking password model of Bank B is set as (TRID + Mobile Phone Number) + (Password of card) + (SMS) = New Password.

4.3.2 New Password Process on Call Center Channel

New internet banking password process of Bank's call center channel is analyzed. In the related menü, the information of card number and password of card are asked. Since these informations are the ones that can not be obtained directly from any social media channel, Bank B's call center process will be left out of scope.

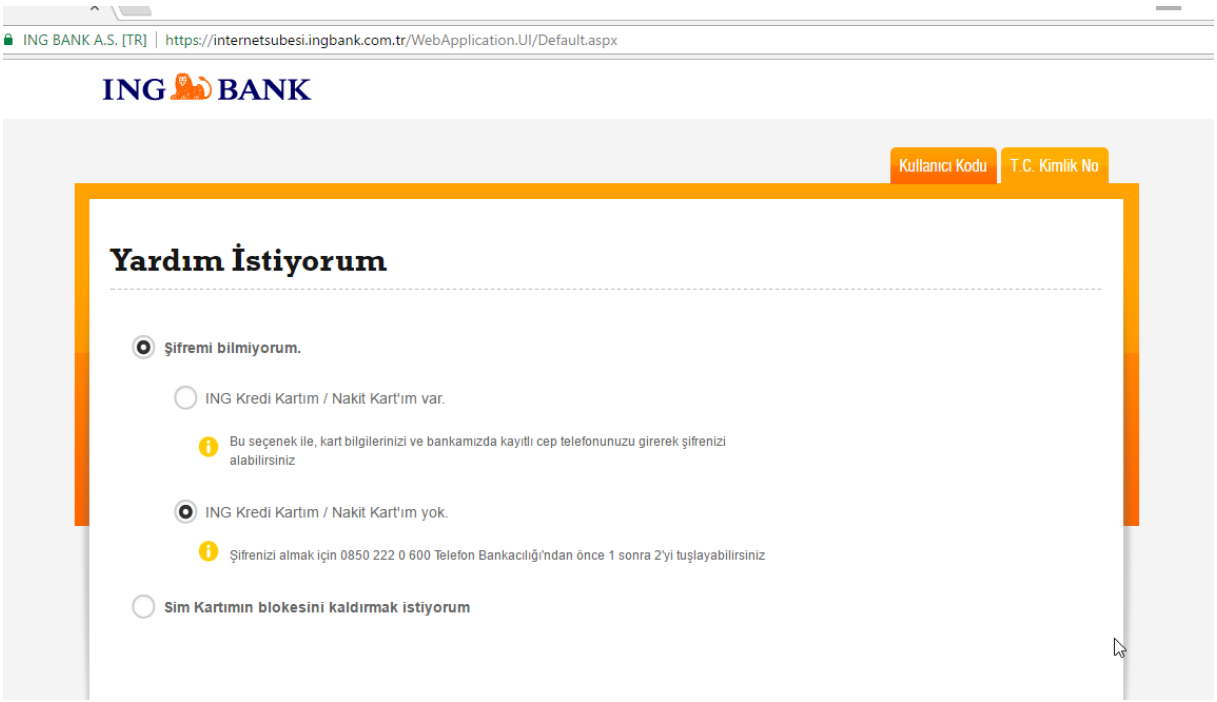
4.3.3 New Password Process on Mobile Banking Channel

Mobile banking application of BANK B is downloaded on a smart phone to analyze the new password process. It is seen on the first screen that TRID and mobile phone number informations are asked to be validated. After that, it is observed that validation of password of Bank's any card is asked. When the right information is entered, it is seen that new password is created with the verification code that is sent to customer's mobile phone which was saved to Bank's database previously.

4.4 SECURITY QUESTIONS OF BANK C

4.4.1 New Password Process on Internet Banking Channel

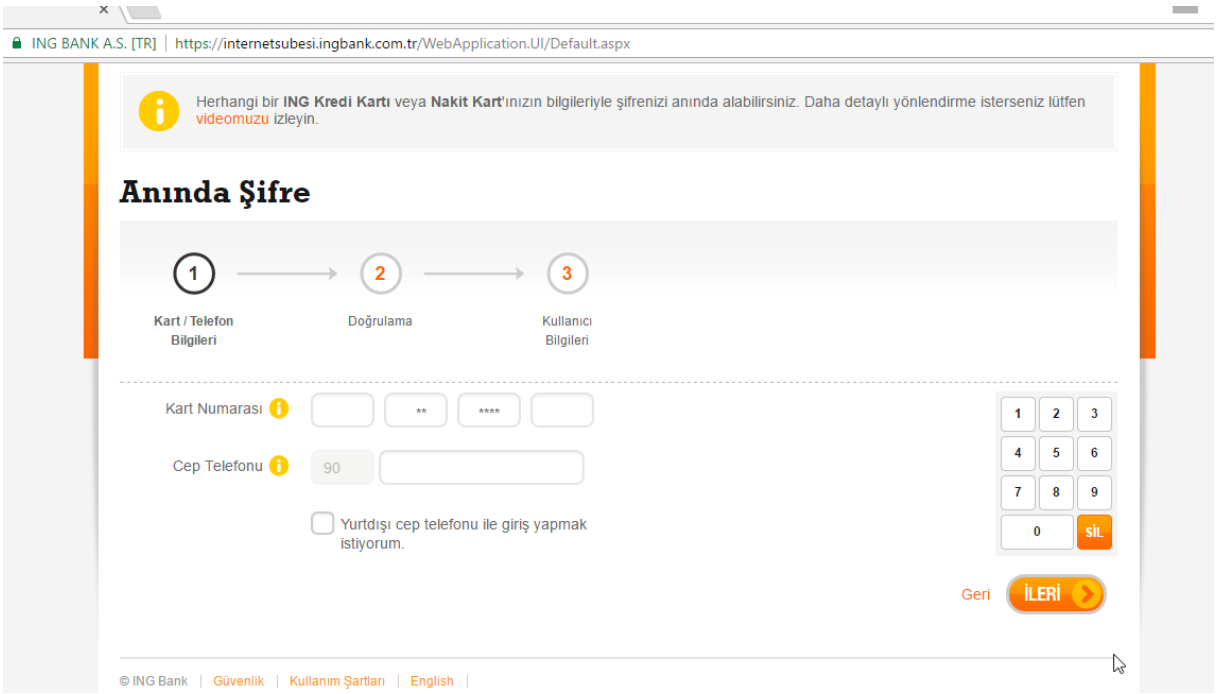
It is observed for Bank C that when "I need help" button in the official website is clicked the screen showed up is presented in Picture 10.



PICTURE 10

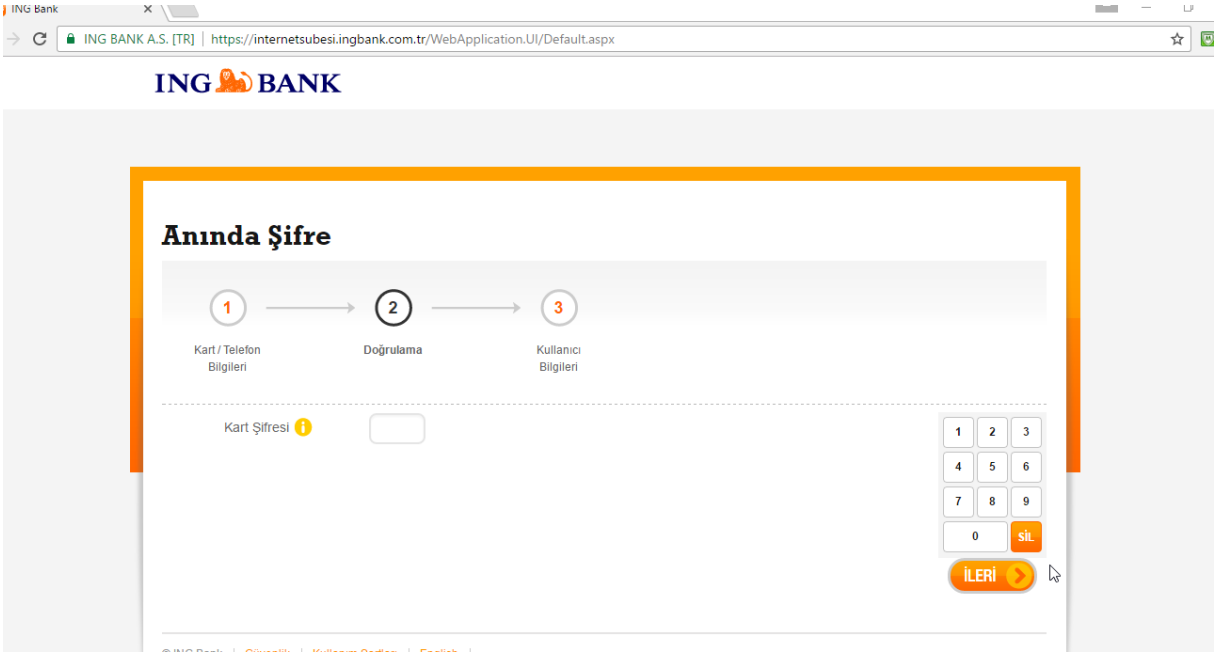
It is observed that when customer of Bank C forgot the password, there are 2 different method is followed by BANK C. There are different processes desgined for the cases customer either will to use credit card information or plastic debit card. For the case of when customer does not have any card of Bank, it is seen that customer is transffered to call center channel. Within the scope of the thesis, both options are analyzed.

-When customers have a card, it is seen that Bank C first asks the information of card number and mobile phone number (Picture 11).



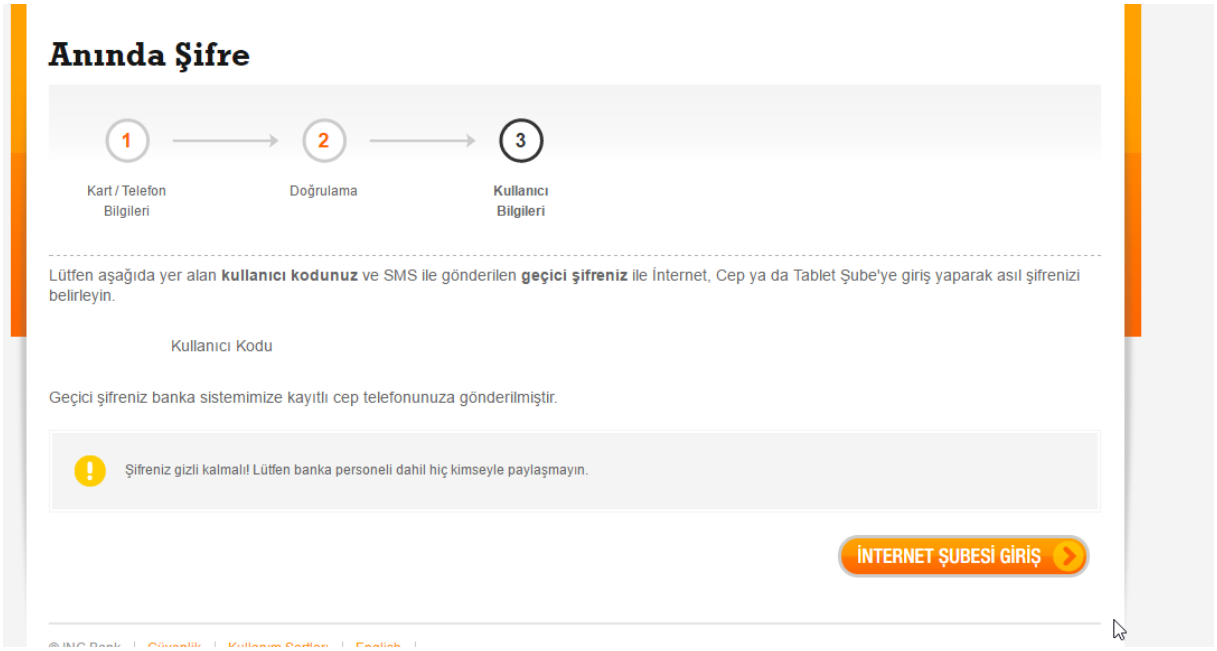
PICTURE 11

When the informations required in Picture 11 are validated, it is seen that passwoord of customer's card is asked (Picture 12).



PICTURE 12

When the informations required in Picture 12 are validated, it is observed that a temporary password is created and sent directly to customer's mobile phone (Picture 13).



PICTURE 13

In line with this observation, it is analyzed that the model of Bank C as follows:

(Card number + Mobile Phone Number) + Password of card = Temporary Password (SMS)

4.4.2 New Password Process on Call Center Channel

-When customers do not have any card of Bank C, it is seen that call center channel is the only option for creating a new password. New password section is selected on call center menü. In the related menü "I do not remember my credit card password" menu is selected since the thesis is in scope of social engineering. A customer representative is transferred after selecting that option.

Customer representative asked the queestions stated below for the new passoword for internet banking.

-**2 letters of maiden name** (the order of the letters are selecteed randomly via system)

-**Birth Date**

After validating the informaation stated above, it is seen that a code is sent to customer's mobile phone. When the code is validated by customer's representative, a new passowrd is created on call center channel.

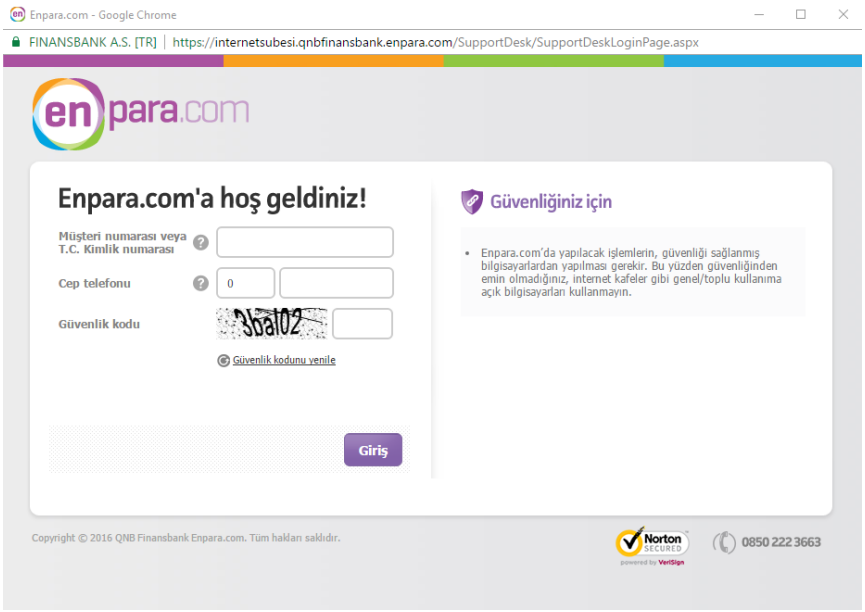
4.4.3 New Password Process on Mobile Banking Channel

Mobile banking application of BANK C is downloaded on a smart phone to analyze the new password process. It is seen on the first screen that the informations of first 6 and last 4 number of card and mobile phone number and password of card are asked. After validating the required informations, it is seen that new password as in the format of text messsage is sent to customer's mobile phone which was saved to Bank's database previously.

4.5 SECURITY QUESTIONS OF BANK D

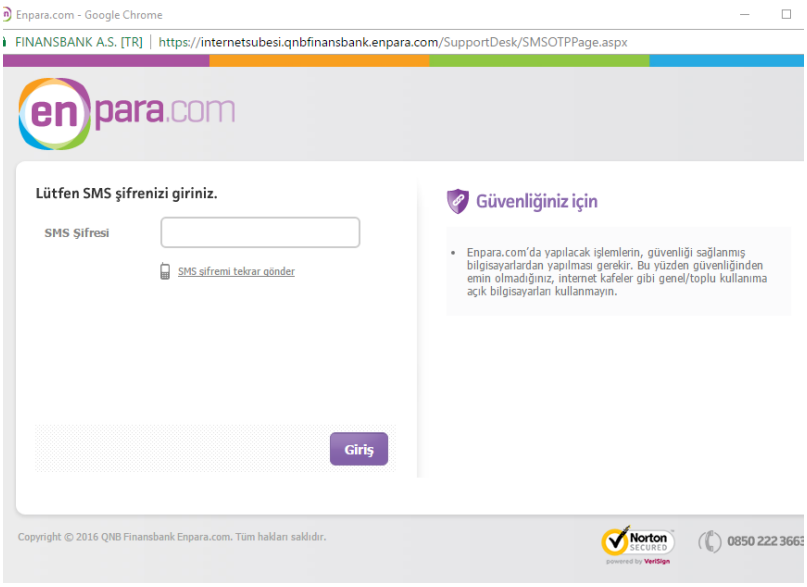
4.5.1 New Password Process on Internet Banking Channel

On the web-site of Bank D, “I do not remember my information” section is clicked. It is seen that customer’s either customer number or TRID and mobile phone number informations are asked with the verification code on the screen (Picture 14).



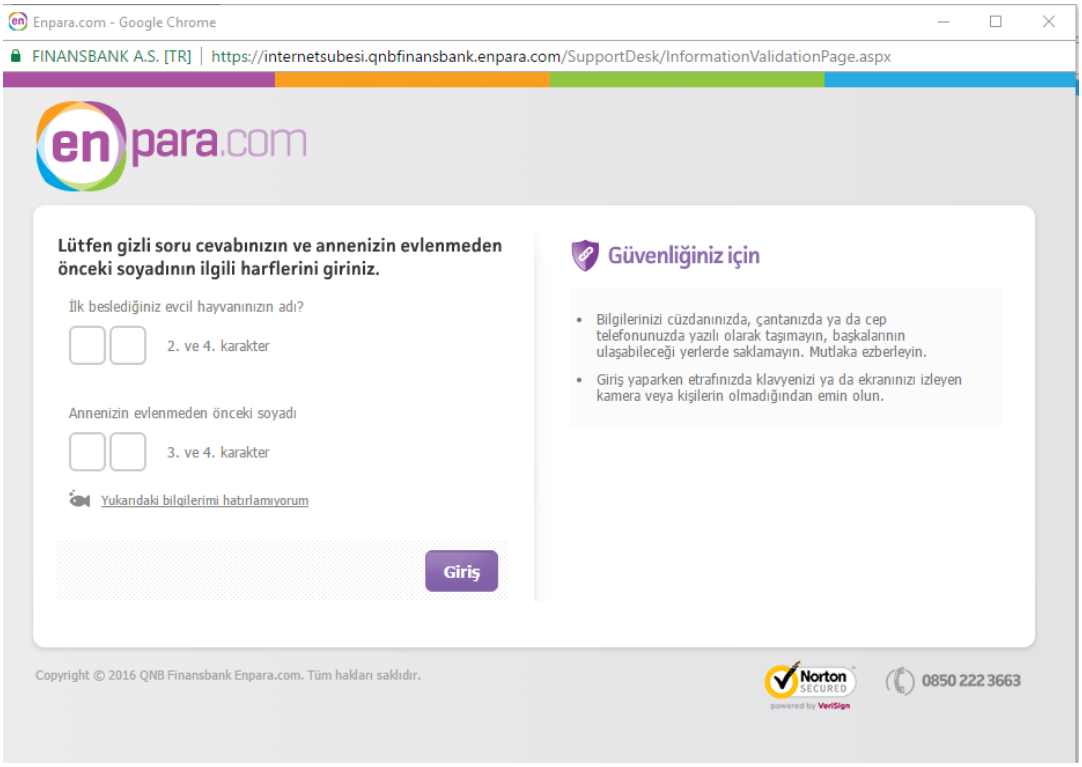
PICTURE 14

When the related fields entered correctly, it is seen that a verification code is sent to customer’s mobile phone (Picture 15).

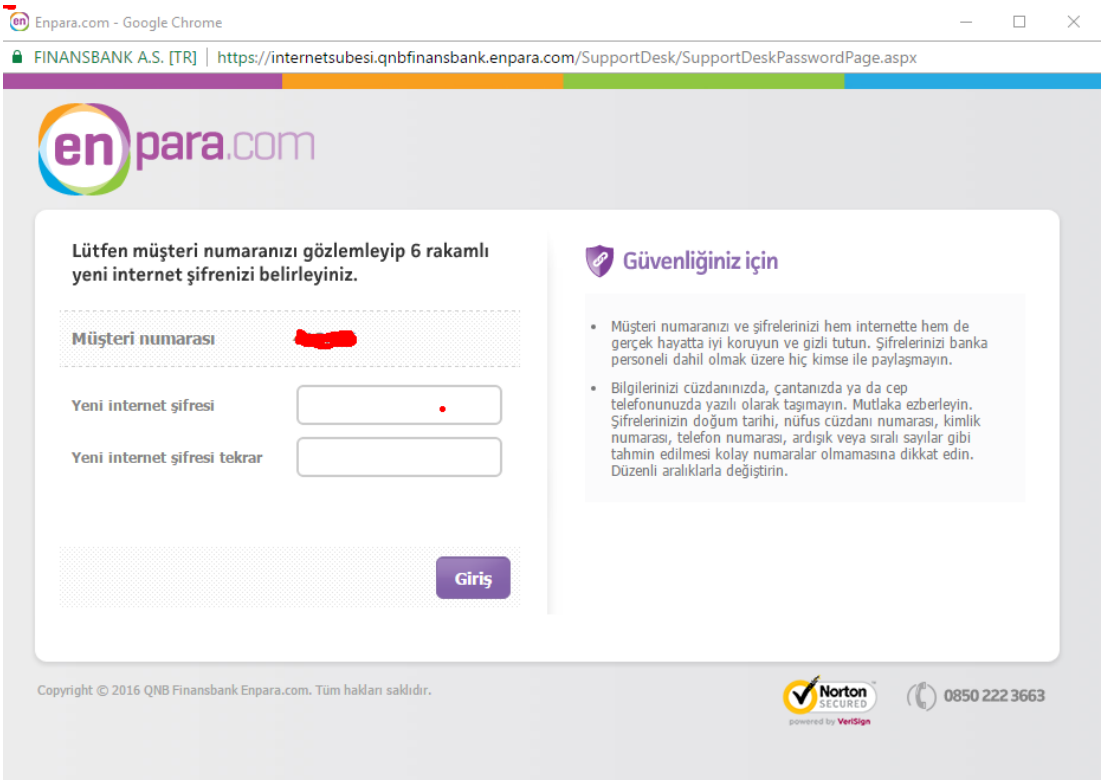


PICTURE 15

After validating the verification code it is seen that one of the security questions that the custome chose(here, that question was pop-up as first pet) and maiden name was asked (Picture 16).



PICTURE 16



PICTURE 17

As a result of this examination, it is analyzed that the model of new password process of internet banking is set up as follows; (TRID + Mobile Phone Number +Verification Code) + (SMS) + (Name of first pet+ Maiden Name) = New Password

4.5.2 New Password Process on Call Center Channel

In order to obtain a new password on call center channel of BANK D, a meeting with customer representative is required. It is observed that in order to create a new password, customer should give the right information set of father name, birth date and serial number on the identity card. It is analyzed that, Bank D has no validation rule in terms of "what customer has".

4.5.3 New Password Process on Mobile Banking Channel

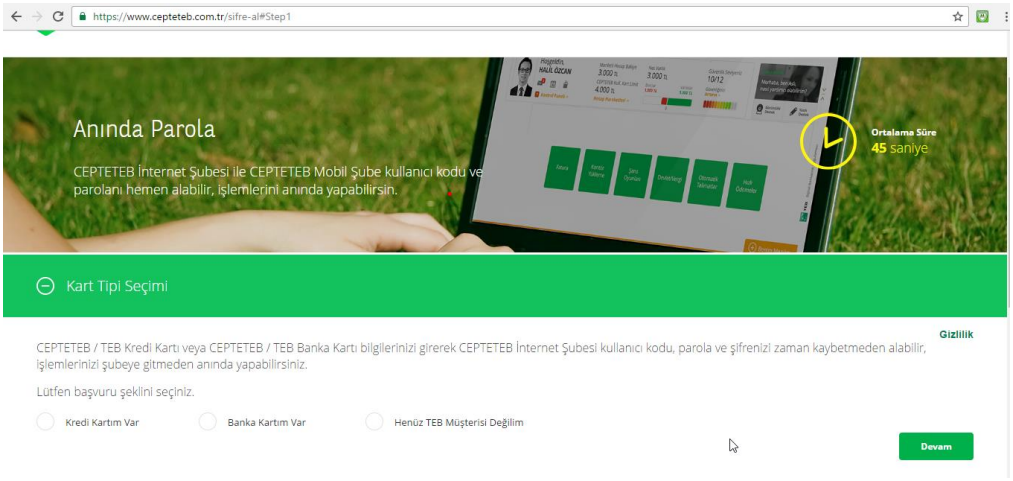
Mobile banking application of BANK D is downloaded on a smart phone to analyze the new password process. It is seen that the bank directs customer to internet banking channel through

the mobile application. It is observed that the processes of mobile banking channel and internet banking channel are designed as the same.

4.6 SECURITY QUESTIONS OF BANK E

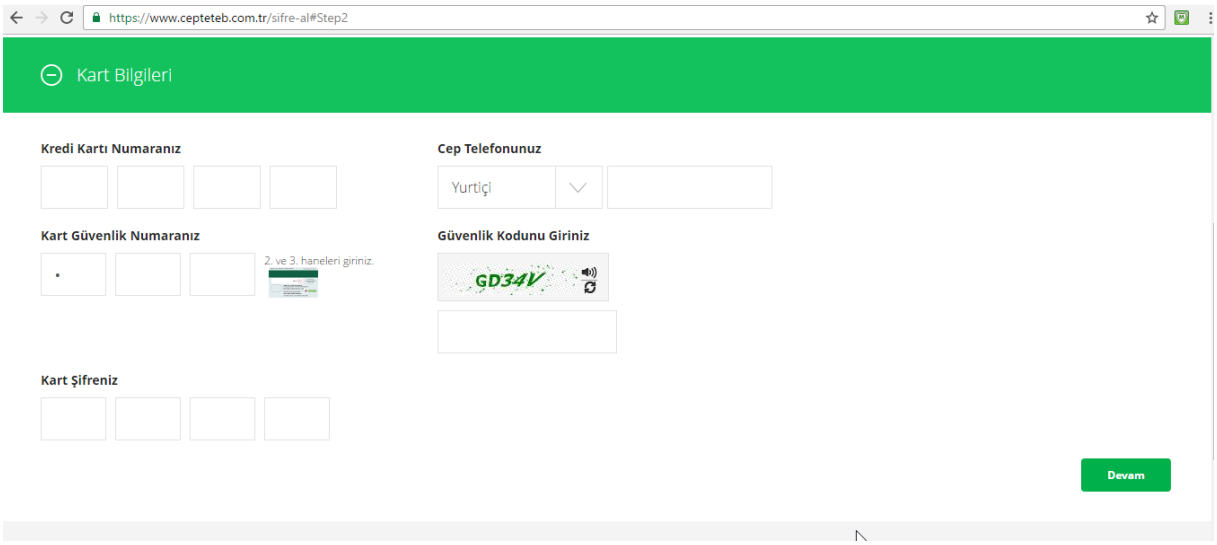
4.6.1 New Password Process on Internet Banking Channel

It is observed for Bank E that when "New Password" button in the official website is clicked the screen showed up is presented in Picture 18. It is seen that Bank E has 3 different methods for the customers that has credit card, debit card or the person is not yet bank's customer (Picture 18).



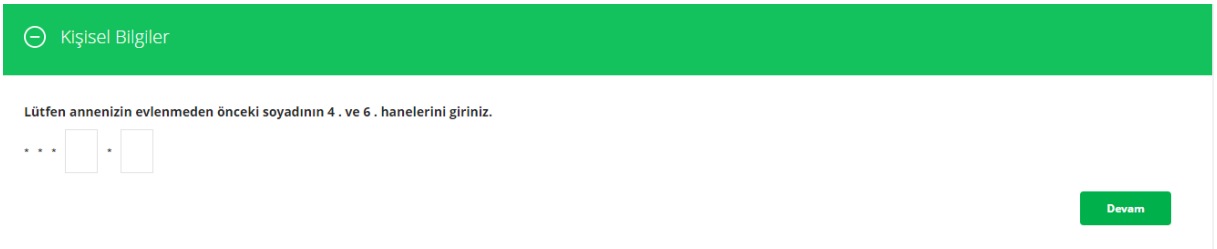
PICTURE 18

When "I have credit card" link is clicked, it is seen that the information of customer's credit card number, security code, mobile phone number and password of card is required (Picture 19).



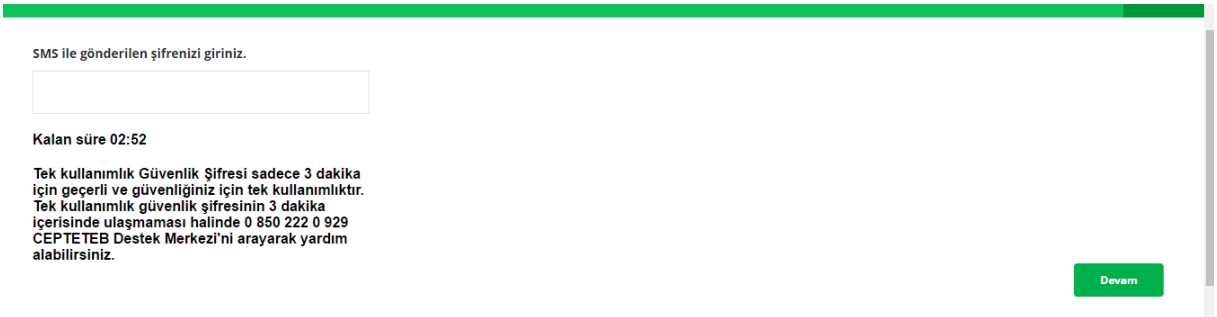
PICTURE 19

When the related informations are validated, it is seen that maiden name of customer is asked by Bank E (Picture 20).



PICTURE 20

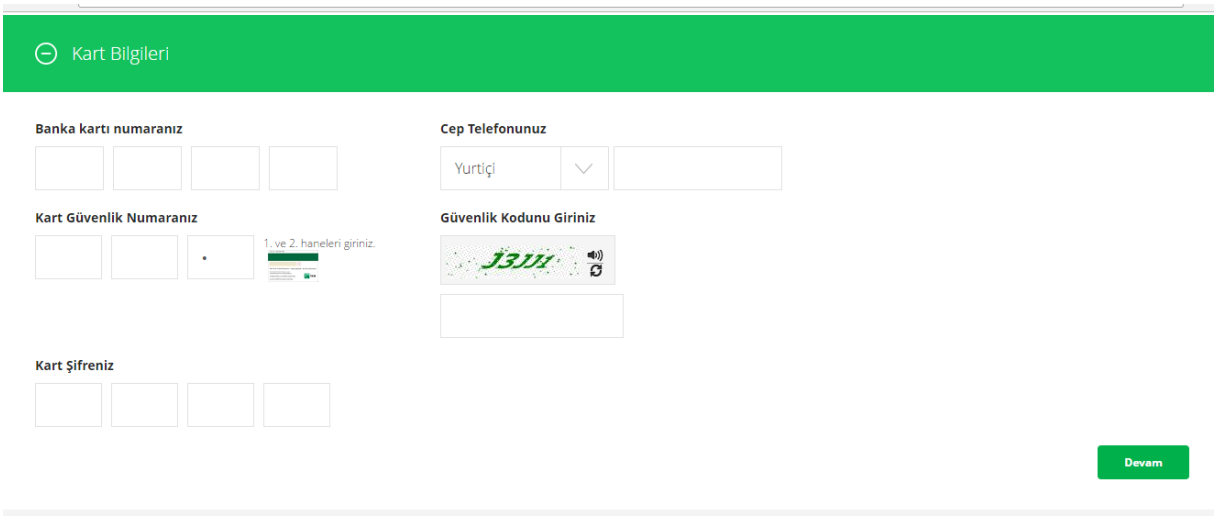
When the maiden name fields are validated, it is seen that a verification code is sent to customer's mobile phone as text message and this verification code is asked by Bank E (Picture 21).



PICTURE 21

After validating the code, it is observed that new password information of internet banking is sent to customer's mobile phone as text message.

On "New Password" menü, when "I have debit card" section is clicked is it observed that same questions are asked with the credit card process with a difference of debit card informations are asked rather than credit card (Picture 22).



PICTURE 22

When "I am not Bank's Customer" section is clicked, it is observed that due dilligence process is initiated for the customer.

As a result of this analysis, it is observed that the process of new password on internet banking channel is set up as follows:

(Card number+ Card- Security Number + Mobile Phone Number + Password of card + Verification Code) + (Maiden Name) + (SMS) = New Password

4.6.2 New Password Process on Call Center Channel

The menu of creating new password of internet banking on call center channel is selected. It is observed that customer representative requires to validate the information of customer's birth date, father's name, birth place and mobile phone number. It is seen that new password is sent directly to customer's mobile phone as text message.

4.6.3 New Password Process on Mobile Banking Channel

Mobile banking application of BANK E is downloaded on a smart phone to analyze the new password process. As a result of the examination, it is seen that the model is set up as below:

-Customer's debit card number, password of debit card, CVV, mobile phone number,

or

- Customer's credit card number, password of credit card, CVV, mobile phone number,

After validating the information set stated above, it is seen that 2 random letters of maiden name is asked. After than, it is seen that a verification code is sent to customer's mobile phone. When that information is validated it is observed that new password is sent to customer's mobile phone as text message.

SECTION 5

ANAYSIS AND MODELLING

5.1 NEW PASSWORD PROCESS ON INTERNET BANKING CHANNEL

In direction of the work, security question model of internet banking channel of the banks that are chosen as sample are clarified as below. It is observed that if the question set in paranthesis was not answered correctly, system does not allow to pass to other questions.

ABANK- (TRID + Mobile Phone Number + Authentication Number) + SMS = New Password

BBANK – (TRID + Mobile Phone Number) + (Password of card) + (SMS) = New Password

CBANK- (Card number + Mobile Phone Number) + Password of card = Temporary Password (SMS)

DBANK – (TRID + Mobile Phone Number +Authentication Number) + (SMS) + (Name of first pet+ Maiden Name) = New Password

EBANK - (Card number+ Card- Security Number + Mobile Phone Number + Password of card + Authentication Number) + (Maiden Name) + (SMS) = New Password

As seen in the model, it is observed for all banks that apart from the information of customer, a tool that customer has is used as a security authentication method via sending text messages to customer's mobile phone.

A – Customer knew + Customer has = New Password

B – 2 x (Customer knew) + Customer has = New Password

C – 2 x (Customer knew) = SMS to the tool that customer has

D - 2 x (Customer knew) + Customer has = New Password

E - 2 x (Customer knew) + Customer has = New Password

For all banks that are chosen as sample, using a tool that customer has apart from only focusing on what customer knows has strengthen the security process. However, it is also seen that the process has absolute dependency of customer's mobile phones.

Matching up of the information can be obtained through socail media channels and security questions of banks are stated in the table below.

Channel	**TRID**	**Mobile Phone Number**	**Card number**	**Password of card**	**Card-Security Number**	**First Pet**	**Maiden name**	**SMS**
ABANK	+	+						+
BBANK	+	+		+				+
CBANK	+	+		+				+
DBANK	+	+				+	+	+
EBANK	+	+	+	+	+		+	+
Social Media Channel	-	Linkedin, Facebook	-	-	-	Facebook, Instagram	Facebook, Instagram	-

TABLE 3

As a result of our examination, it is observed that there is no process in which the answers of the security questions might be obtained from social media channel. It is seen that TRID information whh can not be obtained from any socail media channel has a critic impostance in the security processes. Similarly, it is determined that for some of the banks credit card

information that can not be obtained from any social media channel is a critical information in new password processes.

As seen in the model, sending SMSs to customer's mobile phone that is recorded in Bank's database is very important. In this direction, it is seen that security of mobile phones shall be cared both physically and in terms of software issues.

5.2 NEW PASSWORD PROCESS ON CALL CENTER CHANNEL

In direction of the work, security question model of call center channel of the banks that are chosen as sample are clarified as below. It is observed that if the question set in paranthesis was not answered correctly, system does not allow to pass to other questions.

ABANK – Since this bank requires customer number and that information could not be obtained from any socail media channel, call center process of Bank A has left out of scope.

BBANK – Card number+ Password of Card

CBANK - (Maiden name) + (Birth Date) + (SMS code) = New Password

DBANK – Name of Father + Birth Date + Serial Number of Identification Card =Password

EBANK – Birth Year +Name of Father + Name of Mother + Birth Place + Mobile Phone Number) = Password sends as a tex message to custome's cell phone

When these information are analyzed, principles listed below are observed.

A- Customer knew (out of scope)

B- Customer knew password of card -since it is the initial condition will be left out of scope.

C- 2x(Customer knew) + Customer has = New Password

D- Customer knew = New Password

E- 5x(Customer knew) =SMS Password sent to channel of "Customer has"

As seen in the model, apart from BANK C, all bank require information of not only what customer knew. Also, there is an additionaly security authentication method via sending text messages to customer's mobile phones.

Matching up of the information can be obtained through socail media channels and security questions of banks are stated in the table below.

Channel	Customer Number	Card number	Password of Card	Maiden Name	Birth Date	Serial Number of Identification Card	Name of Father	Name of Mother	Birth Place	Mobile Phone Number	SMS
ABANK	+										
BBANK		+	+								
CBANK				+	+						+
DBANK					+	+	+				
EBANK					+		+	+	+	+	+
Social Media Channel	-	-	-	Facebook Instagram	Facebook Linkedin	-	Facebook Instagram	Facebook Instagram	Facebook	Facebook Linkedin	-
Identification Information	-	-	-	-	+	+	+	+	+	-	-

TABLE 4

When the Table 4 is analyzed, for new password process on call center channel; it is observed for Bank C that apart fro the SMS message information, the answers of the security questions

might be obtained from social media channels. For Bank D, it is seen that answers of questions might be obtained from social media except from the question regarding to serial number information. Additionally, if some person steals a customer's information in identification paper, it is seen that there is no need to obtain additional information on social media. It is observed that since there is no control desgined regaring to the what customer have weakining the security process. For Bank E, it is observed that the answers of the security uestions might be obtained through social media channels. Also, if some person steals a customer's information in identification paper, with having the mobile phone number information, there is a possibility to pass the questions. However, since there is a validation of SMS code control added to the process, it became hard to beat the process.

Regardng to the analysis, it it observed that the information on the identification papers are crucial information in the security process.

5.3 NEW PASSWORD PROCESS OF MOBILE BANKING CHANNEL

In direction of the work, security question model of mobile banking channel of the banks that are chosen as sample are clarified as below. It is observed that if the question set in paranthesis was not answered correctly, system does not allow to pass to other questions.

ABANK – (TRID + Mobile Phone Number) + SMS Authentication Number + (Card number + Card Year + CVV + Card Password)= New Password

BBANK - (TRID + Mobile Phone Number) + (Any card password) + (SMS Authentication Number) = New Password

CBANK – (Credit card information + Mobile Phone Number + Password of card) = SMS Password

DBANK – Since Bank D leads customer who forgot their mobile banking password to internet banking channel, this process is left out of scope.

EBANK – (Card number + Password of card + CVV + Mobile Phone Number) + Maiden Name + SMS Authentication Number = SMS Password

When the information above are analyzed;

ABANK – (Customer knew) + Customer has = New Password

BBANK – Customer knew + Customer has = New Password

CBANK – Customer knew = New Password

EBANK – Customer knew + Customer has = New password sent to what customer has

Channel	**TRID**	**Card number**	**Card Password**	**Card Year**	**Card CVV**	**Maiden Name**	**Mobile Phone Number**	**SMS**
ABANK	+	+	+	+	+		+	+
BBANK	+		+				+	+
CBANK		+	+				+	+
DBANK								
EBANK		+	+		+	+	+	
Social Media Channel	-	-	-	-	-	Facebook Instagram	Facebook Linkedin	-

TABLE 5

When the model of creating new passsword process of mobile banking channel is examined, it is determined that all banks require the information of card of customer. It is seen that related information strengthen the security of the process.

SECTION 6

CONCULUSION

In direction to the work performed within the scope of "Security Questions of Banks and Social Media", new password process is built up on the information of what customer knew and text messaged sent to the customer's mobile cell phone that is recorded on Bank's database. It is determined that just with the information gathered from social media channels, it is impossible to access alternative distiribution channels (i.e. internet banking, call center, mobile banking). However, it is observed that the information stored in social media are critical information in terms of the security questions, therefore, companies that design the security processes should bare in mind this fack and design additional controls in their security validation processes.

It is determined that for new password process of internet banking, asking password of credit card strenghts the process. It is seen in internet baking password model that TRID and credit card information are asked as security questions and these informations can not be gathered from social media channels. Users should pay attention while they are sharing their TRID information since it is a critical information in security processes.

Similarly, it is determined that information in customer's identification papers are critical information in the process. While analyzing new password process of call center, it is seen that one of the banks in scope creates a new password after validating father name, birth date and serial number stated in identification paper of customer. In this direction, there is possibilty to gather new password of customer by a person who obtains the information in identification papers. Since in our daily lifes, photocopies of identification papers are shared with many institutions or when entering some building identification papers are taken in terms of security, it is determined as risky. Therefore, citizens may share driving license instead when baring in

mind the criticality of the informations. Similarly, comapnies may add addtional security questions control to their processes. It is thought that a validation through a channel that customer has will strenght the process.

Sinceprocess of security questions of internet banking channel are in line with legal regulation of norm of communics, it is observed that when attacker could not have the mobile phone of customer, it is impossible to get a new password and perform banking transactions. Additionally, it is determined that sending verification codes and/or sending new password to the mobile phone of customer that is recorded in Bank's database strenghts the process. In this direction, it made it hard both for attackers to leak into customer's banking accounts and letting customer know about a new password process is running if customer is unaware of this action. For every single process, it is seen that there is an absolute dependency to verification codes that are sent to customer's mobile phones. Even tough leaking into customer's acconts is not possible with only information gathered from social media channels, the risks regarding to the mobile phones should not be missed. It should be considered that validation codes might be stolen either with some special hacking attacks desgined for mobile phones or stolen cell phones or easdropping of cell phones.

Users should be careful to mobile attacks. There are attacks designed o capture the received SMS that came to customer's mobile phone. An awarenes shall be created to users regarding to Midnight Raid Attacks capture received SMS information. Attackers sent a link to user's mobile phones and after clicking this link a hazardous malware is downloaded to the device. Therefore, attacker gains all of the recevied information.

As a result of the work performed, it is determined that security questions of new password processes are strenght enough. It is concluded that security control processes of the banks that are chosen as sample could set a good example and model to both local banks and banks in abroad. Also, when rapid changes in technology are considered, an awareness should be raised

to customers. Customers shall know what information is critical or not. Therefore while customers sharing their information, they can reconsider to share the information due to its criticality. Additionally, as stated in Norm of Comminics – Clause 5 as "Customers should be informed on the topics of what services are given within the scope of internet banking and conditions of access ad requirements of security", this duty should be done scrupulously by banks. Furthermore, institutions and organizations in sectors other than banking should design their security procedures va baring mind the risk of the informations stored in social media.

REFERENCES

MAİDEN NAMEOY, Vedat, (2015), İNTERNET BAĞIMLILIĞI ve SOSYAL AĞ KULLANIM DÜZEYLERİNİN FEN LİSESİ ÖĞRENCİLERİNİN DEMOGRAFİK ÖZELLİKLERİNE GÖRE DEĞİŞİMİ ve AKADEMİK BAŞARILARINA ETKİSİ", Asos Journal, Akademik Sosyal Araştırmalar Dergisi, Yıl: 3, Sayı: 19, Aralık2015, s. 365-383

BARIŞ, Fatih M., (2013), "SOSYAL AĞ VE E-PORTFOLYO ENTEGRASYONU: FACEBOOK ÖRNEĞİ", Eğitim ve Öğretim Araştırmaları Dergisi Journal of Research in Education and Teaching Mayıs 2013 Cilt:2 Sayı:2 Makale No:14 ISSN: 2146-9199

BALSÖZ, Fatma Müge, (2004), BANKACILIKTA DEĞİŞEN PAZARLAMA ANLAYIŞI BANKACILIK SEKTÖRÜNDE BİR UYGULAMA , Ankara, http://acikarsiv.ankara.edu.tr/browse/333/

BDDK, "BANKALARDA BİLGİ SİSTEMLERİ YÖNETİMİNDE ESAS ALINACAK İLKELERE İLİŞKİN TEBLİĞ" (2007) https://www.bddk.org.tr/WebSitesi/turkce/Mevzuat/Bankacilik_Kanununa_Iliskin_Duzenlemeler/9491ilkelerteblig.pdf

Bankalar.org, (2016), "Şubesiz Dijital Bankacılık Nedir?", http://www.bankalar.org/bilgi-merkezi/subesiz-dijital-bankacilik-nedir/

BIKTIM, Ecevit. "Mobile Phone Numbernu Ele Geçiren SMS" (2009) https://forum.shiftdelete.net/threads/cep-telefonunu-ele-geciren-sms.79739/

ÇİVİ, Gülçin, (2014), "INTERSECT Kullanıcı Kimlik Doğrulama ve Onaylama Sistemi", GIDB Dergi, Sayı:1, İstanbul

ERDÖNMEZ, Pelin Ataman, (2003), "Türkiye'de 2001 Yılındaki Mali Kriz Sonrasında

Kurumsal Sektörde Yeniden Yapılandırma", Bankacılar Dergisi, Sayı 47

YILMAZ, Eyüp, (2000), Türkiye'de Kredi Kartı Uygulaması ve Ekonomik Etkileri. İstanbul: Türkmen Kitabevi, 2000:124.

FACEBOOK, "Güncel Facebook Türkiye İstatistikleri" (2011) - https://www.facebook.com/notes/promoqube/g%C3%BCncel-facebook-t%C3%BCrkiye-istatistikleri/230108337030128/

FROMMER, Dan, (2010), "Here's How To Use Instagram", http://www.businessinsider.com/instagram-2010-11

İŞLEK, Mahmut Sadi, (2012), "SOSYAL MEDYANIN TÜKETİCİ DAVRANIŞLARINA ETKİLERİ: TÜRKİYE'DEKİ SOSYAL MEDYA KULLANICILARI ÜZERİNE BİR ARAŞTIRMA", Karaman

KARTAL, Mehmet, (2013) "Türkiye'de Sosyal Medya Raporu", http://www.iletisimvediplomasi.com/mehmet-kartal-turkiyede-sosyal-medya-raporu/

KAZANCI, Tarık, (2014), "Mobil Bankacılıkta Güvenlik Sorularının Analizi", İstanbul Üniversitesi, İstanbul

KOERHOST, Ruud H.G (2013)., "Personal Information Disclosure on Online Social Networks", Enschede

Lister, M., Dovey, J., Giddings, S., Grant, I., ve Keiran, K. (2009). New Media: A Critical Introduction. Newyork: Routledge Publishing

OKUMUŞ, Abdullah, BOZBAY Zehra, DAĞLI, Recep Murat, (2007) "BANKA MÜŞTERİLERİNİN İNTERNET BANKACILIĞINA İLİŞKİN TUTUMLARININ İNCELENMESİ", http://iibf.erciyes.edu.tr/dergi/sayi36/007_okumus-bozbay-dagli.pdf

O'Reilly, Tim, (2005), "Design Patterns and Business Models for the Next Generation of Software", http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html

ORHAN, Aydın, (2011), "Kimlik Doğrulama - Faktörler ve Bileşenleri", https://www.bilgiguvenligi.gov.tr/kimlik-yonetimi/kimlik-dogrulama-faktorler-ve-bilesenleri.html

PALA, Emre (2010), "Banka Müşterilerinin İnternet Bankacılığı ile İlgili Tutumlarına Yönelik Bir Pilot Araştırma",Yönetim ve Ekonomi, Cilt:17, Sayı:2, Manisa

PEMPEK, T.A., Yermolayeva, M.A. & Calvert, S.L. (2009). College students' social networking experiences on Facebook. Journal of Applied Developmental Psychology, 30 (3), 227-238.

SANCAK, Mahmut, "Satışta Sıra Twitter'a Geldi" Habertürk 18 Haziran 2016 http://m.haberturk.com/ekonomi/teknoloji/haber/1255438-satista-sira-twittera-geldi

SİPAHİ, İbrahim. "Elektronik Hizmet ve Müşteri Temsilciliği" (2013) http://ibrahimhsipahi.blogcu.com/elektronik-hizmet-ve-musteri-temsilciligi/13862257

SÖNMEZ, Bilge, (2013), Sosyal Medya ve Ortaöğretim Öğretmenlerinin Facebook Kullanım Alışkanlıkları. (Yayınlanmamış yüksek lisans tezi). Akdeniz Üniversitesi, Sosyal Bilimler Enstitüsü, Antalya

ŞENEL, Gülüm, (NA), "Türkiye'de Facebook Kullanımı Araştırması", http://inet-tr.org.tr/inetconf14/bildiri/4.pdf, İstanbul Bilim Üniversitesi

TBB, "Türkiye'de Bankacılık Sektörü 2011-2015 Aralık" (2016) - https://www.tbb.org.tr/Content/Upload/Dokuman/6291/Turkiye'de_Bankacilik_Sektoru_2011-2015_Aralik.pdf

TBB, (2009), “Türkiye’de Kredi Kartı Uygulaması”, Yayın no: 263

TBB, “Bankalarımız 2015” (2016) - https://www.tbb.org.tr/Content/Upload/istatistikiraporlar/ekler/773/Bankalarimiz_2015-tum_kitap.pdf

TBB, (2016), “Bankacılık Sektörü Ocak Haziran 2016”, https://www.tbb.org.tr/Content/Upload/Dokuman/7396/TBB_BN_120816.pdf

TBB, (2016), “Bankacılık Sektöründe Şube ve Personel Sayılarına İlişkin Bilgi Notu”, https://www.tbb.org.tr/Content/Upload/Dokuman/7345/TBB_sube_personel_bilgi_notu_100316.pdf

We are social, (2016), “Digital 2016”, http://wearesocial.com/uk/special-reports/digital-in-2016

Wikipedia, “Facebook real-name policy controversy” (2016) https://en.wikipedia.org/wiki/Facebook_real-name_policy_controversy

Wikipedia, (2016), “Linkedin” https://tr.wikipedia.org/wiki/LinkedIn 22 Aralık 2016

Wikipedia, (2016), “Instagram”, https://tr.wikipedia.org/wiki/Instagram