Internet Bank security recommendations of Komercijalna Banka AD Skopje on prevention against identity fraud

"The chain is as much firm as is its weakest ring"

Dear Clients,

The need for proving you own identity is constituent part of the modern living. The world's trend of criminal acts which incorporate fraud of stolen or no existing identity is increasing. This document explains what you can do to prevent criminal attempt for identity theft and fraud, as well as advices that may help you in any hypothetical situation when you think to be victim of identity theft.

The Guidelines that may be downloaded at the Internet Bank site, provide security recommendations for the Internet Bank users, as summary of the best world's security practices.

NOTE: In case of any unusual operation of the Internet browser when using the Internet Bank of Komercijalna Banka, which may be as a result of any malicious programs installed on your computer (virus, trojan, spyware…), please immediately contact and inform our Help Desk thereof and follow the security recommendations you will be provided.

Internet Bank security recommendations of Komercijalna Banka AD Skopje on prevention against identity fraud

Content

Internet Bank users and their role in the security system

First, let us note that since the beginning of operation of the Internet Bank of Komercijlna Banka AD Skopje in 2001, the start of the pilot phase for carrying out payments in the domestic payment operations for legal entities in September 2004, as well the start of the mass production in October 2006 up to now, there has neither been any user (legal entity or individual) of the Internet Bank to report or become victim of unauthorized access to the information on the bank accounts at its disposal (personal accounts or accounts of the legal entity he/she is authorized to work with), nor any incident of unauthorized disposal of assets on the accounts through the Internet Bank.

Furthermore, the ethical hacking tests, which are periodically carried out by domestic and international companies specialized in the field of IT security, have not reported any weaknesses that may significantly threaten the Internet Bank security neither in the technologies selection and application nor in the processes and activities of the officers responsible for its development and maintenance.

Notwithstanding all continuous and synchronized efforts in the field of security undertaken by the Internet Bank Development Team together with the IT Security Team and the Officer responsible for the security of the IT system of the Bank, as well as other officers and units of the Bank, the security has always been a matter of perfectly balanced combination of top trained personnel, well informed and trained users, selection and application of safe and recognized technologies, as well as their permanent use through well defined procedures and protection measures recognized as best security practices.

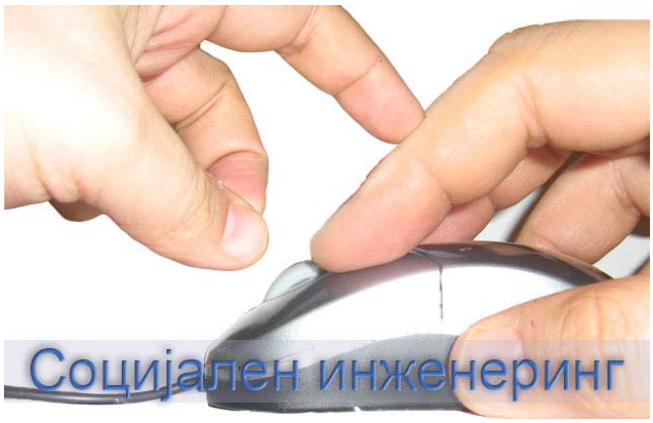
In order to continue with the tradition of safe use of the Internet Bank, this document is addressed to the most important ring in the Internet Bank security system chain, or those for whose protection it is implemented – our clients, without whom, regardless of the technical controls and processes implemented, the security system may be threaten if they do not pay attention to certain threats present when using Internet.

Identity theft and identity fraud

Identity theft means use and fraud of the identity of other person without its knowledge and consent. The cheater has to obtain access to your personal data or to steal your ID documents, regardless whether they are in paper form (ID card, passport) or they are your digital ID tokens, such as your username and password,

list or device for generation single-use codes, your digital certificate saved on your PC, CD or security token, the PIN for access to the digital certificate, etc. Identity fraud means unauthorized use or fraud of identity stolen in criminal activities for illegal acquiring of goods, services or financial assets.

Be always careful – Social Engeneering



Social engineering means sophisticated manipulation with the respective person by the cheater in order to obtain certain sensitive information from the victim, or to convince the victim to do different unauthorized activities.

Instead of trying to detect and use any eventual weaknesses of the IT technical controls and provide access by applying sophisticated hacking techniques and tools, the cheater would try to establish a relation of confidence with the victim, and misleading the victim regarding his identity, to steal sensitive information which would further be used in other criminal activities. Very often the farud presents itself by false identity, making fraud of the sender e-mail and using the logo of the company under which name he wants to present himself, but the social engineering may also use other more conventional means of communication, such as the telephone and mail.

Recommendations

You shoud never provide your personal data or financial information (such as your accounts numbers) to unknown persons that may contact you by e-mail, telephone or in written and under the name of companies that you never contacted before. You should also avoid providing information to any agencies that identify themselves as consultants, executors or marketing agencies of a company you have established business relations with, as you have no guarantee on the identity of the third party which require access to any sensitive information.

Have in mind the fact that such contacts by any third party (agency) in the name of the Bank are less probable. Pursuant to the Law on Personal Data Protection and the internal acts of the Bank, no contact information about you, such as your telephone number, e-mail address or your residence address must not be provided to any third party (agency, other company, etc.) without your written consent.

Pursuant to the Bank's IT Security Policy and the Guidelines on implementation of the IT Security Policy, neither any officer of the Bank nor any third party the Bank has concluded contract for cooperation, must never contact you, regardless of the reason therefore, and require from you to disclose any of the following digital tokens for identification and access to the Internet Bank services:

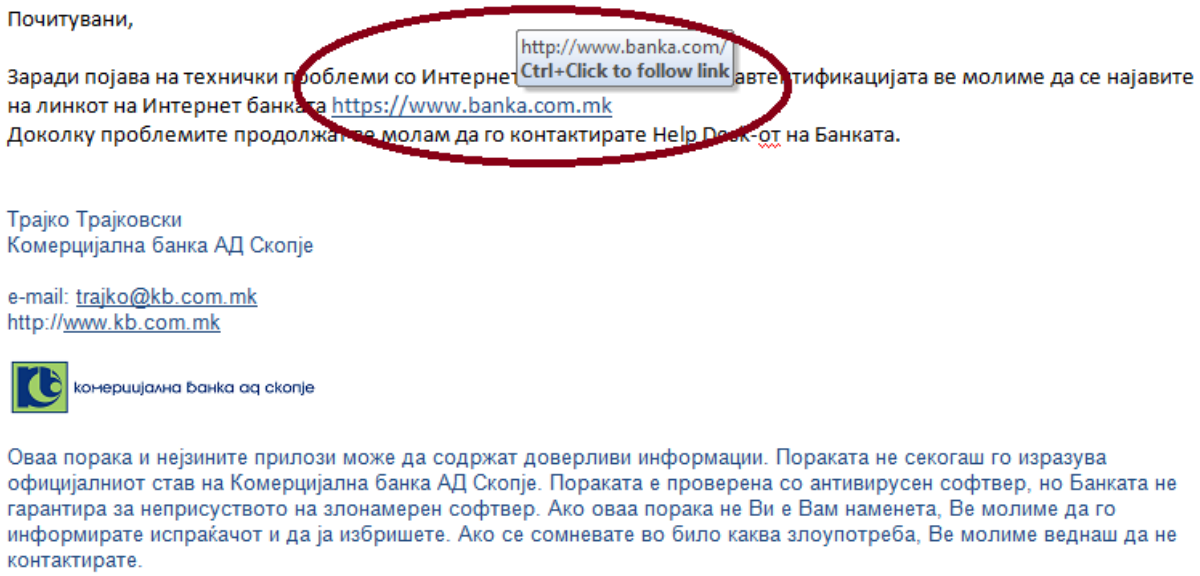
- your password;
- your digital certificate access PIN and
- list of single-use codes.

Regardless whether you are contacted by any third person by phone, e-mail or the person is trying to help you in recovery of any technical problem for which you have required help for, if any of the above listed incidents occur you should immediately terminate the communication with that person and inform the Bank's Help Desk thereof.

Phishing

Phishing is well fabricated fraud aimed for gathering sensitive information, usually digital tokens for personal identification, such as usernames and passwords, cards PINs and PINs for access to the digital certificates, where the fraud is camouflaged in order to look like any trustworthy entity in the electronic communication the user is used to work with (example, web site that looks like the Internet Bank of Komercijalna Banka AD Skopje).

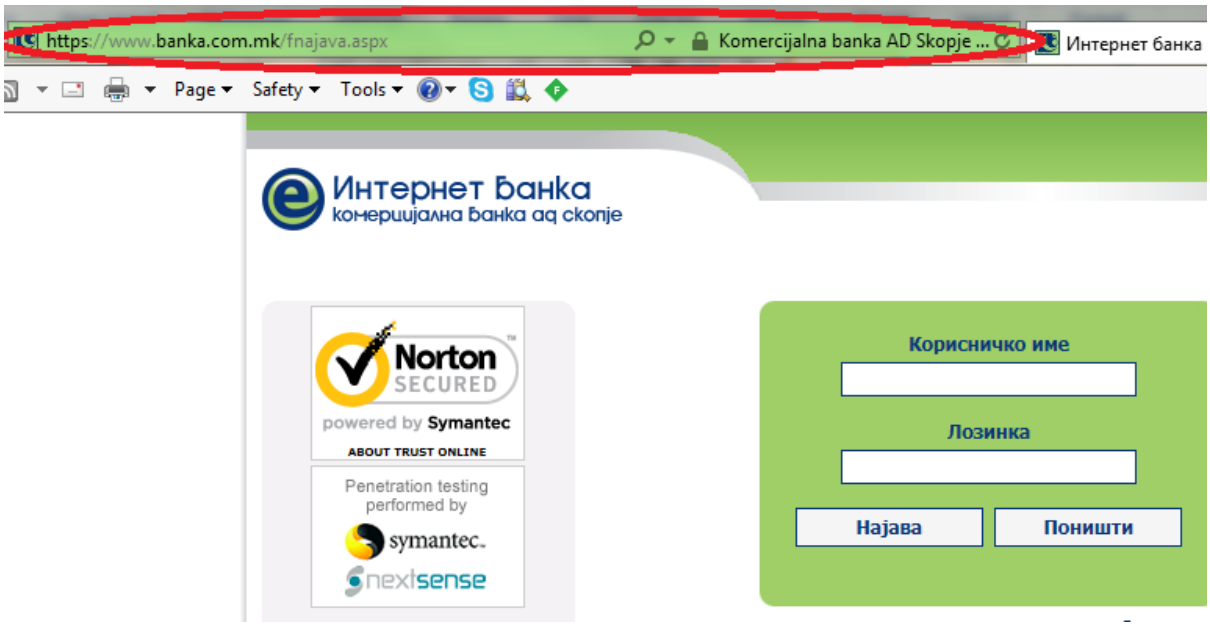
Phishing by means of e-mail messages
A classical attempt for fraud, which combines the social engineering and the phishing would be as follows:

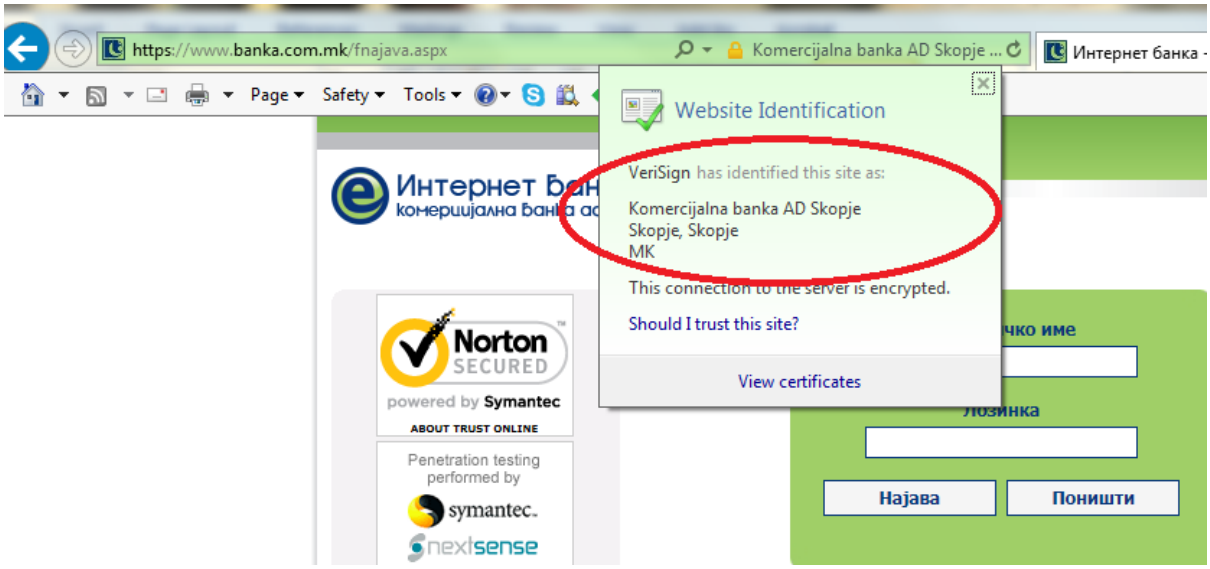


If you move the cursor closer to the link, you will notice that the link leads you to another address that is different from https://www.banka.com.mk (http://www.banka.com). Usually, the replica sites are not secured by valid server certificate and use ordinary uncrypted http connection (the crypted ones are usually https), but it may not always be the case. The victim that will click on the link will be directed on a web site which is very much alike the original one of the Bank, but does not have the same function. If we consider the details of the address toolbar, we can see the differences:

Internet Bank of Komercijalna Banka The fake copy of the Internet Bank AD Skopje (pay attention to the lock, site where user accounts and which when clicked on provides a passwords are stolen (in this case certificate that you are linked to the the link is different and there is no original site) lock icon)

If the user tries to log in and writes down the correct username and password on the fake copy of the Internet Bank site, without beign aware of, the victim provides its digital tokens to the fraud, who latter may use to get sensitive financial information of the user in a unauthorized manner.


https://www.banka.com.mk/fnajava.aspx
Komercijalna banka AD Skopje ...
Интернет банка
Page
Safety
Tools
Интернет банка
комерцијална банка ад скопје
Norton
SECURED
powered by Symantec
ABOUT TRUST ONLINE
Penetration testing performed by
symantec.
nextsense
Корисничко име
Лозинка
Најава
Поништи


https://www.banka.com.mk/fnajava.aspx
Komercijalna banka AD Skopje ...
Интернет банка
Page
Safety
Tools
Website Identification
VeriSign has identified this site as:
Komercijalna banka AD Skopje
Skopje, Skopje
MK
This connection to the server is encrypted.
Should I trust this site?
View certificates
Norton
SECURED
powered by Symantec
ABOUT TRUST ONLINE
Penetration testing performed by
symantec.
nextsense
Најава
Поништи

Phishing by means of malicious add on-s on the Internet browser (Man in the middle of the browser attack)

More sophisticated way of phishing is the use of malicious add on-s for the Internet browser of the user (Internet Explorer, Firefox Mozilla, Google Chrome) which is usually installed on the user's work station as useful add on its Internet browser. It is not a rare case when Plug-in or Add on are installed without the knowledge and approval of the user, usually when browsing particular malicious site and using the internal weaknesses of the operating system and Internet browser. The malicious add on shall read the browsing of the Internet sites and immediately after detecting HTTPS connection or log in windows in form of modal pop-up window, shall disclose the following message:

We do not recognize the computer you are using.

To continue with Online Banking, please provide the information requested below.

Confirm Your Identity

Instructions: Provide your Card Security Code and as much additional security information as you can. Your entries must match the information on the account record and will be used solely to confirm your identity.

Card Number :

[ ]

Card Security Code (required): Turn to the BACK of your card and look in the white panel where you signed your card. Type the last 3 digits of the code.

[ ]

Expiration Date: month/year

[01 \/] / [2010 \/]

ATM PIN:

[ ]

[Continue]

The original Internet Bank site is in the back of the newly disclosed window but this modal window is not part of this site. The malicious program uses the user's confidence in the Internet Bank site trying to mislead the user that the data required by the new window are part of the same site.

When analyzing the content of this input form, many illogical items may be noted, which suggest that it is attempt for fraud:

1. The message is written in English. The official messages and notes of the Bank directed to its resident users are in Macedonian.

2. The message insists on providing sensitive data for the “aledged” additional identification. We would like to point out that the Bank is already making two-factor identification by your password and list of single-use codes or the token and PIN for access thereto. These tokens are sufficient for your identification for the Internet Bank. ***Even more, the Bank would never require any such sensitive information through its web site or by an e-mail message.***

Recommendations:

You should never use the links from third sites to be linked to the Internet Bank site. Write the URL address https://www.banka.com.mk on the Internet browser and make a shortcut thereof or add it to your Favorites. For any further use, just click the shortcut or the link in the Favorites. Any other opening of Internet Bank site through the links provided by e-mail or disclosed on third sites, regardless whether they are Internet newspapers, social networking sites (Facebook, My Space, etc.) blogs or similar, imposes the risk of being caught in the frauds networks and theft of your digital identity.

Notwithstanding of the reliability of the site you are currently communicating with and the manner of that communication (Internet Bank site, e-mail message, etc.), please do not respond to and ignore the requests for providing the following sensitive information:

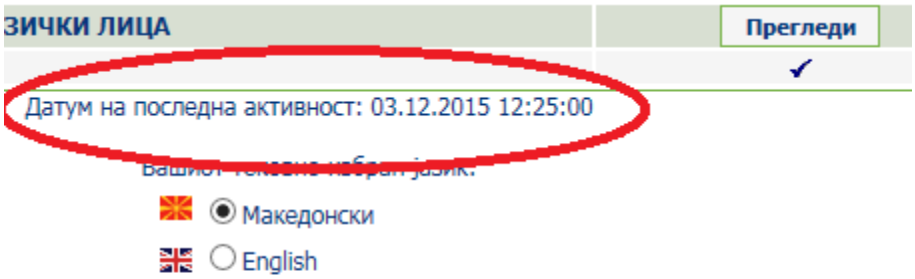
- Payment cards numbers

- POS or ATM authorization PIN
- Security 3-numbers code on the back of the card for authorization of the payments in e-trade through Internet.

    - Your Personal Registered No. or other sensitive personal data for which there are special standards for their protection and exchange prescribed by the Personal Data Protection Agency.

Act quickly and rational – detection and procedures in case of identity theft

Upon each successful log in to Internet Bank, the time of your last activity is permanently registered. You can see it on the site of your user profile and compare it with the last authorized access to the Internet Bank you know of.



If you notice date and time that do not correspond to your last access, immediately change your password and inform the Internet Bank Help Desk thereof, where the activities traces shall clear the details on any eventual unauthorized access to your financial data.

Make regular controls of the statement of your accounts, and in case you notice any debit transactions for which you are not sure to have been authorized by you or they do not correspond to the products and services purchased by you, please contact the Bank's Help Desk immediately and ask for further instructions.

In case you lose the document with your username and password recorded thereon, try to log in on the Internet Bank and change your password immediately. If you have problems in logging in on the Internet Bank, you should notify the Help Desk thereof and require the access to the Internet Bank by your user name to be temporary blocked. Upon your first following appearance at the Bank and identification by a valid identification document (ID card or passport), you will be issued new password, which should be changed after the first log-in, and you will be provided access to the Internet Bank.

If your list of codes or security token are lost or stolen, you should immediately inform the Bank's Help Desk thereof and require the access to the Internet Bank by your user name to be temporary blocked.

In all cases listed above, it is important for the activities to be performed under the following order:

- Contact the Bank's Help Desk and, if necessary, require the access to the Internet Bank by your user name to be temporary blocked.
- Furthermore, upon undertaking the above stated protective measures, you have the right to report the event to the Police, as well as to the Personal Data Protection Agency where official investigation against the doers of the criminal act shall be initiated.

Security failures and recommendations for their avoidance

- ✓ If you are logged in on the Internet Bank, never leave the computer unlocked and with the security token inserted in the USB port, or do not leave your list of single-use codes on your desk. If you do so, and especially where there are many people frequently moving around, you are opening the door to the potential fraud to access your finances.

- ✓ When you leave the computer for a certain period of time, you must lock the workstation and take the list of single-use codes or the security token with you. Have in mind that the security token shall only once require your PIN for access to your private key and shall automatically log out your session after 15 – 20 minutes of inactive status or after pulling out from the USB port.

- ✓ Never write down your username and password or PIN for access to the digital certificate on a piece of paper in your wallet or on the address book of your mobile phone. The practice shows that wallets and mobile phones are mostly subject to stealing.
- ✓ If you doubt that you may remember the password or the PIN, you may write them down on a paper and lock it in your office desk or at home. Try to keep different things on different places to prevent any loss or theft which may provide unauthorized access.

- ✓ When creating the password, never use any of the standard passwords that may be assumed by any criminal (P@ssw0rd, admin, 1234567890, user, operator, Administrator, master key, sysadm, manager ….). Avoid using whole words, names or dates that can easily be related to your private life (date of birth of your child, name of your beloved, etc.).

- ✓ The password should comprise at least 8 characters, each containing characters of at least three of the four groups of characters, selected by your free choice:

- small letters
- capital letters
- numbers
- special signs

- ✓ Do not use the one given password more than 90 days. Do not change your password additionally several times in a row in order to avoid the rule according to which it should not be a part of the history of the three recently used passwords.
- ✓ In order to remember your password easily you can define your own rule according to which you would create future passwords.
- ✓ Do not log in on the Internet Bank on a computer for public use (e.g. Internet cafes) or a computer serviced by unidentified persons. You can never be sure that on the above indicated computers there are not hidden installations of malware applications which steal the user accounts and passwords notwithstanding whether they are acquired due to non-existing or bad anti-virus protection or maybe they are installed deliberately by the person servicing them.

- ✓ Access the Internet Bank from your own portable computer, computer given for work at your post or your home computer. If still you have already logged in on the Internet Bank from a potentially unsafe and compromised computer, use the first occasion and change your password from your home or your personal portable computer.

- ✓ Do not leave your computer without regular updated anti-virus protection and active firewall. Avoid installation of anti-virus from an unknown brand since such applications most often after the installation falsely alarm the user on allegedly found virus and request additional payment for its full removal. Sometimes such false anti-virus solutions might install malware applications additionally (Trojans, spywares, key-loggers etc.) or lead you on sites with phishing in progress....

  Its recommendable to use anti-virus protection of some of the known brands (Symantec, Nod32, Kaspersky, BitDefender, AVG, Panda, Avast) and the issue should be a full protection Internet package in which, besides the protection from viruses you also get protection from other types of malware programs (spyware, adware, Trojans), blocking of malware JavaScript's when browsing the Internet sites, continuous updating of addresses of malicious sites and their blocking, outbound and inbound firewall protection etc. Sometimes proper combination of several protection software packages can provide much higher security level, however, take care not to slow down your computer and not to cause conflicts between applications.

- ✓ Regardless of the operating system you use, surfing by an Internet browser during a session in which you are logged in as a privileged user (member of the Local Administrators group with the Windows platform) is dangerous.
- ✓ You need to create a user account on your computer that does not belong to any privileged group and use it during surfing on Internet and use the sessions with a privileged user only if necessary when you want to install a new application or when you perform activities of periodical maintenance of your computer. One of the worst things that you might do is to use a pirate version of the operating system. Apart from the fact that use of such illegal copies is punishable, additional problem is that very often such copies are distributed with previously installed malicious programs. Some of them (Rootkits) use techniques of invisibility and bypass of system calls so that later on they cannot be detected and removed with any anti-virus application. In addition, the pirate software most often includes the need of exercising a crack (application by means of which the protection from unlicensed use is broken) whose activation almost regularly provides some new sophisticated version of Trojans or Rootkit. Apart from taking the risk of theft of sensitive information and destruction of your files, at the same time you take the risk that your compromised computer without your knowledge is controlled remotely by various criminal structures and be used for activation of DDoS (Distributed Denial of Service) attacks on the site of a company. In such case your IP address shall be recorded as incriminating and you take the risk of being accused for any possible damage that might occur.
- ✓ Use licensed software. If you cannot afford it, look for an alternative in the open source applications.