Online Security Recommendations

For your own protection, we remind you that occasionally, fake emails or malicious software can be used by fraudsters to extract customers' bank data. Please follow our below recommendations in order to prevent and detect the potential online fraud attempts.

A. Social Engineering threats

Social engineering is the art of manipulating, lying or influencing others to perform /not perform certain actions or disclose confidential information.
It is somehow similar to a trust winning trick or to a simple fraud. This term usually applies to those using tricks in order to collect information or to access the IT systems. In some cases, the attacker never comes face to face with the victim.
Find out below the most common types of social engineering.

What does "PHISHING"/ "SMSishing" mean?

In the IT field, **Phishing** means a form of criminal activity consisting in obtaining confidential data, such as the access credentials (username, password, Personal Identification Number, OTP) for financial applications or information related to the credit card, using techniques of manipulation of a person or an institution identity. A phishing attack normally consists in an attacker sending an electronic message, using instant messaging software (*e-mail*) – **PHISHING,** or telephone (*SMS message*) - **SMSishing**, wherein the user is advised to click on a link and/or to enter his access credentials (user name, password), card number, PIN codes, etc.

Beware of online FRAUD attempts though fake emails (Phishing) or SMS (SMSishing) like:

- An email or SMS urgently requesting you to update / validate your personal data or security credentials: in most cases this is a fraud attempt. Do NOT provide such info.
- Emails or SMSs where you identify grammatical or writing errors (wrong translation from other languages) are always fraud attempts.

A phishing example: You receive an e-mail wherein you are informed that you have won a trip abroad and all you need to do in order to receive the travel voucher is to enter (on a website similar to that of the bank) the following information to confirm the identity: your name, address and card data.

A SMSihing example: You receive a SMS message from an unknown number claiming to be your bank and inviting you to download a new version of the Mobile Banking application.
ATTENTION! Most probably in this case you will download and run a malware that could give the attacker the possibility to control and monitor your mobile phone, including being able to capture the access credentials for the legitimate Internet Banking application.

If you receive an email/SMS that appears to be sent by Vista Bank, please consider the following:

- The Bank will NEVER request by email, SMS or by clicking on a link, sensitive data such as: passwords, PIN codes, bank accounts, credit or debit card data, Token codes;
- The message from the Bank will NOT contain attached files that you did not request and will NOT ask you to click on any link that redirects you to any other Internet server / website than the Bank's official ones;
- The bank will NOT ask you to download the official Mobile Banking or eToken applications via a link sent by e-mail or SMS. The only official sources for our applications are the App Store and Google Play.

Announce Vista Bank Romania immediately:

If you have received a suspicious email/SMS that appears to be sent by Vista Bank, please c**ontact immediately the nearest Bank branch or call the Vista Bank Call Center (Phone: + 4021.222.33.10)** to verify the authenticity of the respective email. Also, send / forward (as an attachment) the suspicious email to the following address: abuse@vistabank.ro . **Under no circumstances call other phone numbers mentioned in suspicious emails.**

Where from do they have my e-mail address or telephone number?

Most time, this information is collected from public sources (e.g. announcement websites), but also from the databases made public following security breaches of the various online services where you provided the respective contact data. This information is frequently changed or resold by attackers in order to be used in "phishing" type attacks.

How do they know which bank I work with?

The attackers do not know this, but, if they send many messages, some of them will surely get to people working with the bank presented in the phishing message; if the people are not paying attention, they will provide the attackers with the information they are looking for.

What do I do if I receive a "suspicious" e-mail or SMS message?

It is best to directly delete the respective message, especially if it contains links or attachments. At the same time, whenever you have suspicions about the origin of a message (e-mail or SMS message), it is recommended to contact the bank on one of the official support channels (e.g. the telephone or e-mail indicated on the public website).

What is Vishing?

Vishing is a term coming from the **V**oice and ph**ishing** terms and it represents a deceit via phone call through which the user is fooled to provide sensitive information, the access credentials, card numbers or access code, with the purpose of impersonating the rightful user or to be used by the attacker in other social engineering attacks.

A vishing example: you receive a telephone call from a person claiming to be an employee of the bank announcing you that due to a security alert he must verify your card number, PIN code or card security code.

What can you do?

- DO NOT pass on your confidential data to others.
- The attacker can find out information about you on the Internet or social networks, in order to seem as credible as possible. Ask the caller for more details and let him know that you want to check the phone number directly with the Bank (via website or Call Center), after which you will return with a call. Don't give if he insists on the urgency of providing the data on the spot.

WHAT IS "CEO FRAUD" OR "BEC FRAUD"?

Another type of attack classified as Social Engineering is "CEO Fraud" or "Business Email Compromise (BEC)". Through this deceit the attacker manages to compromise the e-mail server of a company or to create an e-mail box similar to the official one, eventually by changing a letter, zero (0) figure instead of the O letter.

The attacker uses this false identity in order to inform by e-mail the business partners of the company about the change of the invoice payment accounts. Usually, the person who is impersonated is the Chief Executive Officer of the company or the Chief Financial Officer. In the sent e-mail, the financial manager specifies that, from now on, the payments to the company would be made to a new account, account that is at the attacker disposal. The business partners, without suspecting the fraud and making additional verifications, makes the payment into the indicated account. Thus, the attacker gains possession of the money.

In order to prevent such situations, we recommend you:

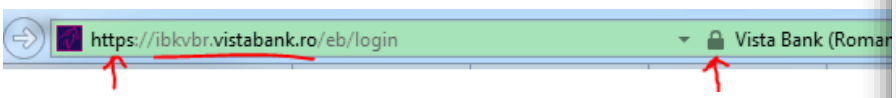
- to avoid, as much as possible, to use unprotected electronic correspondence to exchange information of sensitive commercial or of confidential nature (IBAN codes, passwords, payment details, etc.);
- always use Antivirus software for the protection of your computers;
- Do NOT make payments to new accounts that you have not used before, based on instructions received by e-mail and without first verifying the validity of these accounts with your partners, by means of other communication channels not related to the e-mail. The offenders count on the lack of this verification, therefore, if you check, you will successfully counter-attack the attempted fraud. Do NOT verify the data by e-mail or, under no circumstances, through the contact channels suggested in the suspicious e-mail – we advise you to directly contact your partners, by secure and known channels (telephone/fax numbers that you used before in the past);
- In the event you made a payment to a wrong account, urgently contact your bank to find out if blocking proceedings /return of the involved amounts are still possible.

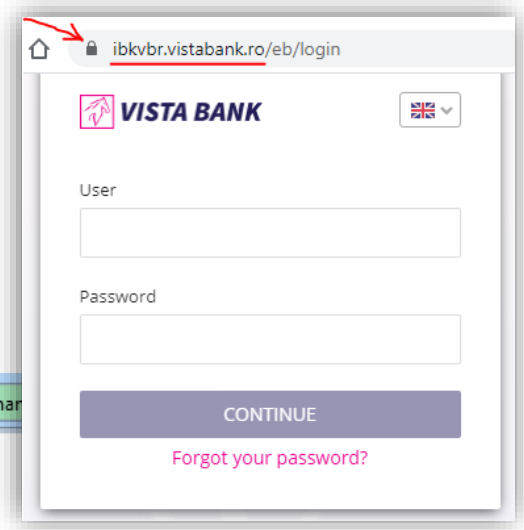
In case you consider you have been a victim of an online fraud attempt, we also encourage you to notify as soon as possible the local Police, as well as CERT-RO (by calling 1911 or by email to: alerts@cert.ro).

B. Security recommendation for Online Banking services

Always access our **Internet Banking** service from Vista Bank Romania official website: https://www.vistabank.ro. Make sure that during login/ authentication you are on Vista Bank Romania official Internet Banking website: **https://ibkvbr.vistabank.ro/eb/**

Check if the site address is correct, if it is preceded by **https: //,** and if the symbol of a **closed padlock** is displayed to the right or left of the site's web address, depending on the browser used, as in the examples below:





Make sure you install the Vista Bank Romania official Mobile Banking application only from the following trusted locations / official application stores:

- (for **Android** from Google Play): https://play.google.com/store/apps/details?id=en.vista.mobile&gl=EN
- (for **iOS** from Apple Store): https://apps.apple.com/bm/app/vista-mobile-banking/id1477309312

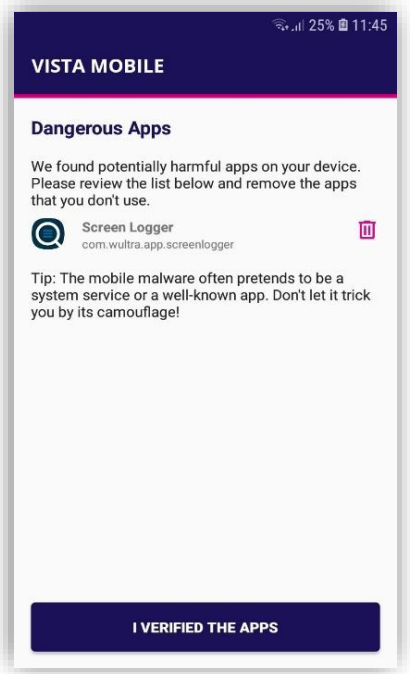
Make sure you install the Vista Bank Romania official eToken application only from the following trusted locations / official application stores:

- (for **Android** from Google Play): https://play.google.com/store/apps/details?id=com.vistaetoken&gl=EN
- (for **iOS** from Apple Store): https://apps.apple.com/bm/app/vista-etoken/id1477189905

Update Mobile Banking and eToken when new versions are available in Google Play (for Android) or Apple Store (for iOS), as new versions bring improvements and can fix bugs or vulnerabilities.

Appshielding and Malwarelytics – additional security features implemented by Vista Bank for protecting your mobile banking apps

The **Vista Mobile Banking** and **Vista eToken** applications integrate the **Appshielding** security feature. The new feature allows the two applications to better protect themselves against a wide range of sophisticated cyber-attacks, such as malware attacks, vulnerabilities related to rooting / jailbreak, debugger connection, Code or Framework injection, application repackaging and app integrity breaches, malicious screen readers or untrusted keyboards, overlay attacks, Man-in-the-App and Man-in-the-Middle scenarios, sensitive embedded key protection (white-box crypto). Whenever a suspicious activity occurs, Appshielding responds by taking necessary protection countermeasures, preventing attackers from modifying the mobile app both during runtime and at rest.



Vista Mobile Banking for Android version, integrates the **Malwarelytics Antivirus** – a security feature that protects both the Vista Bank mobile apps and your entire mobile device.
When opening the Vista Mobile Banking application, Android version, in case any malicious active applications (mobile malware) are detected on your phone or tablet, you will be notified of their existence. From the same screen you have the option to uninstall them immediately, by clicking on the trash can icon.

Token / eToken Safety (who generates the "Unique Password"/OTP):

- Always keep the Token or the device on which the eToken app is installed with you and do not allow it to be accessible to others;
- Do not disclose to anyone the "Unique Password"/OTP generated by Token;
- In case your Token or the device on which the eToken app is installed is lost/stolen, immediately notify the Bank to deactivate that token.

Password security:

- Use only strong passwords (at least 8 characters long, small, numeric, and special characters) and avoid words found in the dictionary, consecutive letters or numbers, or names of people or birthdays (or other public information available on social networks);
- Do not use the same passwords as those used on other websites (such as Social Networks, Personal Emails, etc.);
- Do not share the password with others;
- Periodically change the passwords.

C. General security recommendations for online

Security Tips for your Computer:

- Periodically scan the computer to protect against viruses and other malware using a daily updated Antivirus software.
- Use an account/user for the operating system that does not have administrator rights (so viruses can't be easily installed);
- Avoid default installations for application, choose custom installations, and do not install Toolbars or dangerous Extensions in the Internet browser;
- Update periodically your operating system and make sure you are using a recent, stable browser, while the Java application and PDF reader are updated to the latest versions;
- Lock your computer when you leave it unattended;
- Do not use computers you don't own (at the Internet Café, hotel, airport or "friends") when making bank transactions, as they may already contain malicious programs (intentionally or unintentionally installed) that can steal your authentication data or / and bank data.

Secure use of Smartphones and Tablets:

- Restrict the access to your phone/tablet using a PIN code, password or fingerprint;
- Install only good reputable applications with many downloads and positive reviews;
- Use an Antivirus to scan installed applications;
- Update both your phone operating system and your applications;
- Do not "Jailbreak"/"Root" your phone/tablet.

Safely browsing on the Internet:

- Avoid accessing links from emails that redirect you to other sites that can possibly imitate the bank's website (as there is a risk of entering your username, password, Token or PIN on a False/Clone website which will steal authentication data for malicious reuse).
- Enter/Write yourself the bank's website directly into the browser.
- Learn to recognize if you are accessing a secure website: the « **https://** » connection and a valid website certificate. If the browser warns you that the website certificate does not match the server, it is advisable not to continue.
- Disable password saving into browsers (especially auto-saving of passwords).
- Enable the pop-up blocker option.
- Do NOT download files from torrent sites or pirated applications. These files can hide the malicious software that is installed on the computer without informing the user.
- Do NOT click "Agree" or "OK" to close a window. Instead, click on "X" in the corner of the window or press Alt + F4 on the keyboard.

Using Wireless Networks (WiFi):

- Avoid plugging your laptop or smartphone into an unsecured network. Free Wi-Fi networks are extremely vulnerable if they are not secure.
- When connecting to an unsecured network, any person within the reach of the access point may "see" the transmitted information.
- Do not leave your home router unsecure and do not use WEP technology. It can be accessed in seconds because of this protocol vulnerabilities. Use only WPA2, configure a longer key and change the wireless network SSID. Otherwise, you are susceptible to rainbow-table attacks.