Bank Audi
Private Bank

Guidelines for the Prevention against Email-based Cybercrimes Designed for People and Non-Financial Institutions

This guide is targeted at providing a brief overview on the indicators of cybercrimes and the means of prevention, such as:

1. Indicators on Email-based Cybercrimes

Email-based Cybercrimes may take various forms and you should be aware of, including but not limited to, the following indicators, which may help detect these acts:

- A difference detected in the email address of the "Supplier", in which a letter, number, symbol or sign is changed, for example the letter "g" is replaced with the letter "q".
- An email attributed to the "Supplier" through which the sender claims that the "Supplier's" account number has been changed for unconvincing reasons and arguments, which include for example checks conducted by the controls or tax authorities on the "Supplier's" accounts, or the deterioration of the relationship with the former bank because of the high bank commissions.
- An email containing instructions to send transfers to an account held abroad under a name deemed close or similar to the "Supplier's" name while using a different account number than the "Supplier's" account number, which is adopted according to the documents held by the individual or the concerned company.
- An email attributed to the "Supplier" through which the sender asks you to abstain from contacting the "Supplier" by phone in order to confirm any changes or amendments made to the name of the Beneficiary Bank, Beneficiary Financial Institution or the Beneficiary Financial Intermediary Institution or any changes or amendments made to the Beneficiary's name or account number.
- An email attributed to a Bank, Financial Institution or a Financial Intermediary Institution through which the sender claims that the Bank, Financial Institution or the Financial Intermediary Institution is in the process of updating the file of one of its customers and is requesting specific information for that matter.
- An email attributed to the "Supplier" involving many unusual or flagrant spelling mistakes.
- An email attributed to the "Supplier" involving phrasing and a language different from the previous correspondences.
- The letters and numbers used in the invoice attached in the suspicious email are inconsistent in terms of form, size and color.
- The transfer request attached in the suspicious email contains a signature similar to the "Supplier's" signature.
- An email attributed to the "Supplier" and addressed generally to the recipient company instead of the employee who usually receives from the "Supplier" the instructions to be implemented.
- An email different from the email attributed to the "Supplier".
- An email attributed to the "Supplier" containing instructions, which are different from the previous ones.
- An email attributed to the "Supplier", addressed to the individual/company and at a third party unrelated to the transfer request.
- The address of the "Supplier" is located in a country different from the country in which the Beneficiary Bank, Beneficiary Financial Institution or the Beneficiary Financial Intermediary Institution operates.
- An email attributed to the "Supplier" or to another person through which the sender requests information about the bank and financial accounts and/or any other sensitive information.
- An email containing a link to a website, which requests financial or personal information.

2. Policies and Preventive Measures Against Cybercrimes

The following preventive steps must be followed:

- Determining many means of communication by which the customer can contact all of his "Suppliers" to confirm the instructions received from them before their implementation (phone number, fax number, email, name of the person to contact).

APB-Cybecrime-Jan 2019 (Eng)

- Contacting the "Supplier" by phone on the numbers specified by the latter, which are recorded in the individual/company's records and not on the numbers included in the email to ascertain the transfer components related to the name of the Beneficiary Bank, Beneficiary Financial Institution or the Beneficiary Financial Intermediary Institution as well as the Beneficiary's name and account number and the attached documents.

- Abstaining from providing the "Supplier" or any other party, through email, with any financial information related to the name of the Bank, Financial Institution or the Financial Intermediary Institution with which the individual/company does business and the account number, balance and its ongoing transactions.

- Being mindful of the phone calls or emails requesting financial information for updating personal and financial files of the individual/company.

- Abstaining from replying to any correspondence sent to you by email by clicking on "Reply". Instead, click on "Forward" to select the email address from the "Mailing List" as the Sender's name appearing on the email may not actually be theirs but may be attributed to one of the hackers who has created a similar email. In addition, any falsification in the email address can be detected by opening the "Reply" window (without using it) and confirming the identity of the email sender.

- Confirming all the details of the email address and being mindful of any email with a suspicious and unreliable source similar to the "Supplier's" email.

- When sending emails to many people, you should add the email addresses in the "BCC" section to hide them from others who may want to hack it.

- If you were not able to contact the "Supplier" by any of the means of communication agreed upon, you must abstain from requesting the Bank, Financial Institution or the Financial Intermediary Institution to make the transfer until you confirm the veracity of the instructions received or sent through email.

- Being aware that the Bank may abstain from executing the transfer or implementing any other instructions if it cannot contact the individual/company by any of the means of communication agreed upon in order to confirm the transfer request received via email.

- It is necessary to use two electronic accounts at least:
  - The first account shall be used for all the correspondences related to money transfers with the Bank, Financial Institution or the Financial Intermediary Institution; this email address must not be indicated on the Business Card.
  - The second account shall be used for the social media sites.

- Abstaining from using a unified password for more than one email or website. In addition, you must use a strong password, change it constantly and activate the Two-Step Verification Sign-in feature. The password should not include, for example, the following:
  - Simple combinations of the keyboard patterns, series of numbers and letters or duplicated letters, such as (qwerty, abcdef, 1234, AAAa)
  - Words typed backwards, such as (sdrawkcab=backwards)
  - Short, uncompleted or wrongly written words, such as (Helo)
  - Consecutive short words, such as (Catcat)
  - Words preceded or followed by one code, such as (Apple3, %hello)
  - Personal information, such as (Date of birth, name, surname)

Being mindful of received correspondences, which include suspicious attachments, such as (scr, dll, cox, com, exe, bat, vbs, dif, shs, pif) as they might include malwares.

- Updating the browser used on electronic devices on a regular basis.

- Using and updating an original antivirus program constantly.

- Updating the Recent Activity feature of the email. If you have concerns regarding this activity, you need to change the password immediately.

- Being mindful of browsing the email through public Wifi.
- Retaining information stored in the Mail Server for more than three months, if possible.
- Abstaining from shipping goods to the importing company abroad before confirming the veracity of the payment instructions by phone using one of the means of communication agreed upon.
- Making sure that the insurance policies cover the risks related to the execution of financial and banking transactions through email.
- Being mindful of emails containing a Real Time Transfer request.

3. Corrective Action

When you identify, detect or report a criminal act through electronic means, you should take quick and effective measures including at least the following:

- Immediately inform and provide the concerned Bank, Financial Institution or the Financial Intermediary Institution with all the relevant information to take necessary actions.
- Contact the "Supplier" on their approved numbers in order to inform them that criminal acts took place or were attempted through electronic means and to draw their attention to the need for calling their customers by phone and informing them that they may have been subject to electronic piracy acts.
- File a complaint before the competent judicial authorities and retain all the digital evidences.
- Change the password immediately.
- Make sure to retain the ongoing email correspondences without canceling or amending them, given the possibility of using them in any investigations.
- It is advisable to review all the transactions with the "Supplier" in order to ensure that they did not face any other criminal acts by electronic means in the past, and to inform the relevant Bank, Financial Institution or Financial Intermediary Institution about the results of this review.