BANQUE
LIBANO-FRANÇAISE

Prevention-guide against cybercrime via e-mails

1- Prevention guide against cybercrime via e-mails dedicated to individuals and non-financial institutions

Financial cybercrime is an act or attempt to commit a local or cross border crime by individuals or organized groups for the purpose of violating bank accounts or financial and personal information, through the use of various electronic and technical means. This form of crime includes, for example, fraud, theft, misappropriation, extortion, sabotage or espionage by electronic means.

2- Preventive policies and procedures against criminal acts

2.1 The following preventive steps are required during business operations:

- Use several means of communication with the provider in order to ensure that the instructions are understood before implementation of financial transactions (phone number, fax number, email address, the name of the person to contact, etc.).
- Communicate by telephone with the provider, by using the approved account numbers and not the numbers mentioned by e-mail to confirm the transfer instructions, i.e. the beneficiary bank, the name of the beneficiary, its account number and the validity of the documents attached and necessary for operations.
- Avoid providing the supplier or any other third party with private financial information (name of the bank, account number and balance, transactions in progress, etc.) by e-mail.
- Put the bank transfer process on hold until the confirmation of the instructions mentioned or sent by e-mail is obtained, in case it is not possible to contact the provider by the appropriate and approved communication means.
- Take note that the banking establishment will refrain from executing the transfer or any other operation when it is not possible to contact its customer by the approved means to confirm the request to carry out the operations mentioned by e-mail.
- Ensure the validity of payment instructions by telephone using appropriate and approved means before shipping goods to importing companies abroad.
- Make sure that insurance policies cover risks related to the implementation of financial and banking transactions by e-mail.

2.2 We also recommend adopting the following preventive measures in the context of e-mail operations on a daily basis: Use at least two e-mail accounts; the first is dedicated to all correspondence concerning bank transfers. This account should not be mentioned on your business card. The second is dedicated to the use of social networking sites.

- Do not answer the correspondence received by e-mail by clicking on the "Reply" option. You should give preference to the "Forward" option. This allows you to select the response address from the mailing list, because the sender's name appearing in the e-mail may not really be the name of a reliable contact, but that of hackers who would use a similar e-mail account. Any manipulation of the e-mail account address can also be detected by opening the option window (reply) (without using it) and verify the identity of the sender of the email.
- When you send an e-mail to several recipients, it is necessary to put their emails in the BCC box so that the addresses of your interlocutors can not be seen by all the recipients of your mailing list to avoid any attempt of hacking.
- Avoid using the same password for multiple e-mail accounts or online sites. You must use a strong password, change it regularly and activate, when possible, a 2-step verification procedure. Your password should not contain:
  - Simple templates on the keyboard, a series of numbers and repeated letters, or repeated letters (i.e. AAAa, 1234, abcdef, qwerty)
  - Reverse wording (i.e. sdrawkcab = backwards)
  - Short, incomplete or incorrectly written words (i.e. helo)

E-FORM/SEC/CYBER_CRIME/ENG/6-2017

- Short consecutive words (i.e. catcat)
- Words preceded or followed by a symbol (i.e. apple3, %hello)
- Personal information (i.e. date of birth, first name, name)

- Pay attention to the e-mails received with suspicious suffixed attachments (i.e. «.exe», «.cox», «.com», «.dll», «.scr», «.pif», «.shs », «.dif», «.vbs», «.bat»), because they may likely contain malicious programs.
- Update regularly the web browsers software used on your electronic devices.
- Use genuine anti-virus software and update it permanently.
- Enable recent activity tracking option for your e-mail account, and in case of doubt related to suspicious activity, change immediately the password of this account.
- Avoid consulting your e-mails when you are connected to public WIFI networks mainly when the messages are related to financial operations with your bank.
- If possible, keep the information stored on your mail server for more than 3 months.
- Be suspicious of e-mail messages in which you are asked to make a real-time transfer.

3- Remediation measures in case of discovery of an act or an attempt of hacking

When a criminal act or an attempt of a criminal act by electronic means is detected, the bank in charge of the transfer operation should be informed immediately and promptly provided with any relevant information to take appropriate measures. It is also important to:

3.1 Communicate with the supplier about its account numbers to inform him about a criminal act or an attempt of a criminal act through electronic means, in order to draw his attention to the need to contact his customers by telephone to inform them about a possible exposure to risks of electronic piracy.

3.2 File a complaint to authorities and keep all digital proofs and correspondences exchanged by e-mail without any deletion or modification so it can be used during investigations.

3.3 Change passwords immediately.

3.4 Review all the transactions done with the supplier to ensure that there has not been a prior exposure to criminal acts through electronic means and inform the bank of this review.

Click here to read the full guide.