**(4) Early Warning Against the Crime of Hacking in Trade**

There is an increase in the amount of crime of hacking in trade disputes between Egyptian and Chinese companies recently. In order to prevent hackers from committing crime and protect the benefit of both Egyptian and Chinese companies, we would like to share with you some usual practice of the Hackers, and warn the Egyptian businessmen of the situation of a possible hacker’s trick, so you could be more careful in some critical stages to prevent yourself from being victim of the hacker.

Usually, the Hacker enters into the email address of the Chinese company and get to know some background information of the business, after the down payment is made, by the time for the Egyptian company to pay the balance and purchase the document, the Hacker would send emails from the mail address pretended as Chinese company’s mail address, saying that the bank account from the contact is under auditing and could not receive money, requesting the Egyptian company to change bank account, and remit the money to a new bank account in a different city, sometimes in Hong Kong, or even in overseas countries. As there is no strict control on the name of the account beneficiary in some overseas banks, the hacker can still use the Chinese company’s name as the beneficiary of his account to get the trust of the victim.

To convince the Egyptian partner, the Hacker will make similar Proforma Invoice with amended bank account information, with same imitated signature and stamp, then he will follow up with the Egyptian businessmen closely and push the client to make the remittance as early as possible. Once the remittance arrives to his account, he will close the account immediately after he withdraws the payment, and it will be very difficult to trace it because they usually use fake information to open the account. Holidays are good time for hackers to make the deal because there is lack of communication between the two companies.

Some Egyptian businessmen would then believe that the Chinese partner is playing the trick with them to make them pay twice, but in fact, the Egyptian side has much more control in preventing the hacker from committing the crime if they can fulfill the following:

1. To regulate the trade practice, sign good contract, specify the bank account information in the contract or Proforma Invoice. **Be alert in any request of changing bank account when being asked to do so, and check it by different channels,** because each registered Chinese company has only one bank account related to its business license, always make sure that the money is remitted to the bank account whose beneficiary is exactly the company name, and the bank address is in the same city of the company registration location.
2. Keep close contact with the Chinese company and verify important information through various channels, not only by email, but also by telephone and fax. Inform the Chinese company immediately after you make any remittance, so both of you could have time to react if crime of hacking occurs, and ask the bank to freeze the account for further investigation.
3. Be careful in checking the revised Proforma Invoice, there must be some slight difference in word size and typeface, especially the imitation of the company stamp and signature made by the Hacker.
4. Hacker problem can happen between companies who are new to each other, as well as long time cooperation partners, between new partners because they do not have the experience of usual practice of the other party, between old partners because they trust each other, and do not give a second thought to their emails and requests.

So always be careful and have the sense of Hacker in mind, and do business cautiously, you can avoid this problem through your own experience and effort.

Economic and Commercial Counselor’s Office

Embassy of P.R.China in Cairo

Nov. 11, 2014