Warning on Financial Swindles

Never give your confidential payment information to anyone. China Merchants Bank have received several questions about the legitimacy of certain solicitations received by post or email. These letters or emails hold out the promise of large sums of money in exchange for payment of advance fees, transaction costs, customs duties, etc. In some cases, the recipient is informed that he/she has won a lottery. The letters and emails also state that the financial or other transactions have been initiated by companies registered in China or other Asian or European countries.

"NEVER give your confidential payment information to anyone!"

We wish to make it absolutely clear that, in all probability, such requests are fraudulent and are related to a well-known financial swindle which first appeared in West Africa in the 1980s. The swindle is now so widespread that national and international law enforcement authorities refer to it as “Nigerian bank fraud”, “Nigerian advance fee fraud” and “419 fraud”.

Suggestions that a lottery has been won fall into a separate category although the method of operation is comparable and the fraud is perpetrated by the same swindlers.

Several features the schemes share are listed below:

- a sum of money (or a product), of lawful or unlawful origin, from a lottery, an investment plan, oil, a bequest, real estate, a bankruptcy, etc., will be made available upon receipt of an advance payment of fees associated with the release of the money (or product);
- to initiate the transaction, the recipient must contact an official of the company registered in China (or in another Asian or European country);
- the official must be contacted on a mobile telephone number in China; please notes that the identification of a mobile phone number may not be evident for a non-Chinese residence;
- attempts to verify the company name and address in a business directory or with the local Chamber of Commerce all fail;
- an invitation to travel to China (or any other Asian or European country) is generally extended in order to complete the transaction and pay the advance fee.

Phishing

A new variation on this type of scam is “phishing”. Phishing is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords, credit card numbers and Social Security numbers.

Phishing isn't new -- it's a type of scam that has been around for years and in fact predates computers. Malicious crackers did it over the phone for years and called it social engineering. What is new is its contemporary delivery vehicle -- spam and faked Web pages.

Phishing (sometimes called carding or brand spoofing) uses e-mail messages that purport to come from legitimate businesses that one might have dealings with banks such as Citibank or Visa; online organizations such as eBay and PayPal; shipping companies such as FedEx and UPS; Internet service providers such as AOL, MSN, Yahoo and EarthLink; online retailers such as Best Buy; and insurance agencies. The messages may look quite authentic, featuring corporate logos and formats similar to the ones used for legitimate messages. Typically, they ask for verification of certain information, such as account numbers and passwords, allegedly for auditing purposes. And because these e-mails look so official, up to 20% of unsuspecting recipients may respond to them, resulting in financial losses, identity theft and other fraudulent activity against them.

The police receive many reports of this nature. Because of the methods used by these swindlers (Internet, mobile telephone numbers, fake addresses and names, bank accounts which only exist for a matter of days), in most cases it is extremely difficult to track down the perpetrators or recover the victims' money.