

## **General Security advices**

### **Overview:**

In order to create risk and fraud awareness in our clients and to ensure protection of their personal banking information, below are some security advices from our bank. The main objective is to educate our clients on how they can prevent themselves from falling victim of fraud and deception.

### **Online Banking Password**

- Change your online banking password frequently, memorize it and avoid writing it in obvious places
- Avoid easy passwords like your name, date of birth, your telephone nos. etc
- Passwords should be a combination of upper case, lower case and numbers
- Do not use your internet banking in public places like internet cafes, Libraries etc
- Never declare your password to anyone who claims to be a staff of BLOM BANK FRANCE. Immediately report such matter to the bank

### **Fraudulent emails:**

- Do not reply emails that request your personal banking information such as passwords, PIN (Personal Identification Number), Account number or any other financial information. BLOM BANK FRANCE never requests clients for such information via emails.
- If you receive any unusual email from your suppliers which trigger suspicion, please confirm that email by calling your known contact before remitting funds to the account details mentioned by the supplier in email
- Suspicion grounds could be :
  - If the supplier contacts the client through unauthorized or unknown email address.
  - For any reason, if the supplier changes the banking details and requests for payment to be transferred to bank account other than the usual bank account.
  - If you receive invoice or payment request via email from a particular supplier who had never communicated payment matters on emails.
  - If the supplier offers unexpected discount and insist on urgent payment and also demand for copy of bank advice or transaction reference number of payment for follow-up with his bank.
  - If the supplier demands for payment in EURO for banks operating in United States or payment in USD for banks in European region.
  - If any unknown third party contacts you for payment to your immediate supplier.
  - If the email from the supplier has several spelling and grammatical errors in the body of "official looking" email.
  - If the color or size of the text is different than the usual style of email used by supplier.

- The fraudulent email with above suspicious contents may also contain supplier's company logo and official layouts that had been used by original supplier as legitimate communication.

#### **ATM Security:**

- Never disclose your Personal Identification Number (PIN) to anyone
- Change your PIN regularly or if you think it may have been compromised, change it immediately
- Operate the ATM with close distance and ensure your key pad is hidden with your hand or body
- Ensure that other individuals at ATM queue keep acceptable distance from you. Quit your transaction and leave the ATM immediately if you feel unsafe or you are suspicious of individuals near the ATM. Come back later or use another ATM.
- Never accept help from strangers when using ATM and always be wary of strangers asking for help. While one distracts you and the other steals your card and money
- Do not be in a hurry during transaction and carefully secure your card and cash in your wallet, handbag or pocket before leaving the ATM. Do not count your cash in front of the ATM
- If your card is jammed, retained or lost, report this immediately to the bank
- Know your daily withdrawal limit and reduce it if necessary
- Report lost or stolen ATM Cards as soon as you discover they are missing

#### **Cheque Security Measures:**

- Request for a new cheque book(s) should be made only by using the form attached in your cheque book or by submitting a letter to the bank signed by the authorized signatory.
- Count the cheque leaves immediately on receipt of a new cheque book to ensure that no leaf is missing or duplicated in the book.
- Ensure to keep your cheque book under lock and key. The safekeeping of the cheque book is of prime importance and the responsibility of the owner
- Notify the Bank in writing immediately if a cheque is lost or stolen along with the acknowledgment of reporting such loss or theft to Police, in order to stop payment of the cheque.
- Unused cheques should be returned to the Bank when the account is closed.
- Do not sign blank cheques. Always fill in the date, the name of the receiver and the amount before signing the cheque.
- Take care to write the cheque without any gaps from the printed area in spaces provided to write the payee name, amount in words and figures
- Always draw a line through any unused space
- Any mistake made in writing the cheque should be altered by neatly striking it out and confirmed by your full signature against it
- To prevent unauthorized encashment of the cheque, use crossing whenever possible.
- Never sign in multiple places unless authenticating a change.
- When you cancel a cheque, write "CANCEL" across the face of the cheque