BANQUE BANORIENT FRANCE
Banking with a personal touch

Information Security Awareness

Overview

Complementing the security measures used by Banque Banorient France, here are measures you can take to ensure the security of your financial and personal information

Online Banking Password

- Do not include personal info or predictable sequences in your password
- Use Password Managers to generate and store your password
- Use Upper letters, Numbers and Special Characters
- Use different passwords for different platforms
- Use Multi-Factor Authentication
- Do not use your internet banking when connected to public hotspots
- Banque Banorient France staff will never ask your password. Report it immediately to the bank

Phishing Emails

There are numerous types of phishing, but ultimately it is any type of attack by email that is designed to result in the recipient taking a specific course of action. This could be clicking a link that leads to a compromised website, opening a malware-laden attachment, or divulging valuable information such as usernames and passwords.

Signs to spot a Phishing Email

- An Unfamiliar tone or greeting
- Grammar and Spelling errors
- Inconsistencies in Email Addresses, Links & Domain Names
- Threats or a Sense of Urgency
- Suspicious Attachments
- Unusual Request
- Recipient Did Not Initiate the Conversation
- Request for Credentials, Payment Information or Other Personal Details
- Email Signature

Protecting yourself against Phishing and Fraudulent emails:

- Do not reply to emails asking for your personal banking information such as passwords, PIN (Personal Identification Number), Account number or any other financial information. Banque Banorient France would never ask for your personal details in such manner.

- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information
- If you are unsure whether an email request is legitimate, try to verify it by contacting the person in subject
- Do not click on links received from unknown senders
- Always call only on your client's known phone numbers for verification and not on the numbers mentioned in an email
- If you suspect that your personal details have been compromised, report it immediately to your bank
- Sometimes fraudsters impersonate people you know at work and ask you to redirect funds/payments to an account under their control, be vigilant and call the person for verification
- Always verify the Email Sender and do not trust the display name.

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 your 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.

BANQUE BANORIENT FRANCE
Banking with a personal touch

- 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