PROTECTION FROM FRAUD As part of our Consumer Education and Awareness Program under the guidance of Central Bank of the UAE, we at BANQUE BANORIENT FRANCE, take the security of your accounts very seriously. While we continuously upgrade our online security features to ensure you are always protected, it is also important that you understand your role and obligations to ensure the safety of your information regarding online / mobile banking, ATMs, and Debit cards.	**الوقاية من عمليات الإحتيال :** كجزء من نظام و معايير حماية المستهلك المعمم من قبل مصرف الامارات العربية المتحدة المركزي، اننا في بنك بانورينت فرنسا ، نأخذ مسألة حماية حساباتكم بمنتهى الجدية ، ولذلك نقوم باستمرار بتحديث وتطوير أنظمة الحماية لضمان الحماية اللازمة لكم ، كما يهمنا ان نلقت انتباهكم الى ضرورة دوركم الهام والتزامكم باتخاذ التدابير اللازمة لضمان حماية معلوماتكم المتعلقة بعملياتكم من خلال تطبيقات الهاتف , العمليات الالكترونية على الموقع ، جهاز الصراف الآلي وبطاقات الخصم المباشر.
• **Beware of Links.** Banks will never send you a text or email that asks you to click a link. If you receive this type of message, do not respond – just delete it and call our bank to confirm we did not send it.	• **احذر من الروابط الإلكترونية Links**, ان البنك لن يرسل اليكم اي نص أو بريد الكتروني أو الطلب اليكم الضغط على أية روابط الكترونية Links. وفي حال استلامكم أي نص أو رسالة من هذا النوع ، لا تستجب لها – فقط قم بالغائها وبادر بالاتصال بنا للتأكيد على اننا لم نقم بارسالها.
• **Protect your Confidential Information.** The bank will never ask for your account number, name, address, or password in an email or text message. It will only be asked for verification of your identity when you call our call center support directly.	• **قم بحماية معلوماتك معلوماتك السرية** ، ان البنك لن يسألك من خلال رسالة أو بريد الكتروني عن رقم حسابك ، اسمك ، عنوانك أو كلمة السر الخاصة بك ، حيث انه يتم التأكد من هويتك خلال اتصالك المباشر بمركز الإتصال.

• **Watch for Misspelled Words.** It is very common to find typos in a fraudulent text or email. If you find one in the message, you know it is a fraud!	• **انتبه للكلمات المتضمنة أخطاء إملائية** ، ان الشائع عموماً في رسائل الإحتيال أو الرسائل الإلكترونية تضمنها أخطاء إملائية واضحة ، في حال ملاحظتك لها في أية رسالة ، اعلم بأنها عملية احتيال.
• You should always be aware of the security when using an ATM and should always follow these general tips to ensure your personal information is kept safe:	• عليك الحذر والإنتباه دائماً لاحتياطات الأمان الواجب اتباعها عند استخدامك أجهزة الصراف الآلي وعليك باستمرار اتباع المعلومات والنصائح العامة التالية لضمان حماية معلوماتك الشخصية وبقائها آمنة :
i. Never disclose your Personal Identification Number (PIN) to anyone.	i. لا تطلع أياً كان على رقم التعريف الشخصي (PIN) الخاص بك.
ii. Never write your PIN or Password on your ATM cards.	ii. لا تكتب رقم التعريف الشخصي (PIN) الخاص بك على بطاقات الصراف الآلي.
iii. Memorize your PIN or Password.	iii. احفظ رقم التعريف الشخصي (PIN) وكلمة المرور الخاصة بك.
iv. In case of stolen or lost card or any suspicious transaction on your account, contact immediately the helpline 0097143160317 and inform your branch.	iv. في حال سرقة أو فقدان أي بطاقة او اشتباهك بأية عملية تمت في حسابك ، قم بالاتصال فوراً برقم المساعدة التالي : 0097143160317 وقم بإبلاغ فرعك بذلك.
v. Be aware of shoulder surfing while entering PIN at ATM or POS terminals	v. انتبه لمحاولات إستراق النظر من خلف الكتف أثناء إدخال رقم التعريف الشخصي (PIN) الخاص بك على جهاز الصراف الآلي أو أجهزة قراءة البطاقات لدى منافذ البيع.

• **Always Confirm Funds Transfers:** Before sending a request to bank for funds transfer, always confirm with the beneficiary of funds over the phone. Do not rely only on bank details received on emails from the beneficiary.	• **قم بالتأكد باستمرار من تحويلات الأموال** : قبل ارسال طلب الى البنك لتحويل أية أموال ، قم بالتأكيد على ذلك دائماً مع المستفيد من الحوالة من خلال إتصال هانفي به ، لا تعتمد فقط على بيانات البنك التي استلمها المستفيد على البريد الإلكتروني.
• Always maintain strong passwords for Online and Mobile Banking. Avoid using simple passwords such as your name and numbers associated with you such as date of birth etc.	• عليك باستمرار تكوين كلمات سر قوية للتعاملات المصرفية التي تقوم بها الكترونياً أو من خلال تطبيقات الهواتف الذكية. وتجنب استخدام كلمات بسيطة كاسمك مع أرقام ذات صلة بك كتاريخ ميلادك .. الخ.
• Keep your cheque books and loose cheques in safe place and never sign a blank cheque. Blank cheques are vulnerable to misuse or fraudulent activities.	• احتفظ بدفتر شيكاتك او الشيكات المتناثرة في مكان آمن ولا تقم مطلقاً بتوقيع شيكات على بياض ، حيث ان تلك الشيكات عرضة للإستخدام في عمليات الإحتيال أو إساءة الإستخدام.
• The bank will not be responsible if the customer share password or ATM and Debit Card PIN with the third party,	• ان البنك لن يكون مسؤولاً في حال قيام العميل بمشاركة كلمة السر أو رقم التعريف الشخصي الخاص بالصراف الآلي أو بطاقات الخصم المباشر مع أي طرف آخر.
Cyber Frauds: **Strong Passwords and MFA:**	**الإحتيال الرقمي :** **رقم سري قوي ومتعدد عوامل التحقق**
• Use strong, unique passwords for online banking accounts. • Enable multi-factor authentication whenever available.	• استخدم رقم سري قوي ، فريد في كافة تعاملاتك المصرفية عبر الانترنت • اعتمد اسلوب التحقق المتعدد العوامل كلما كانت متاحة لديك.

Secure Devices and Networks: • Keep devices (computers, smartphones, tablets) updated with the latest security software. • Use reputable antivirus and anti-malware software. • Avoid using public Wi-Fi for online banking. • Be careful of downloading applications from untrusted sources. **Monitor Accounts Regularly:** • Regularly review account statements and transaction history for any unauthorized activity. • Set up alerts for account activity, such as large transactions or unusual logins. • Report any suspicious activity to the bank immediately. **Protect Personal Information:** • Be cautious about sharing personal information online or over the phone. • Shred or securely dispose of documents containing sensitive information • Be aware of social engineering tactics and avoid revealing sensitive data. **Educate Yourself:** • Stay informed about the latest cyber fraud trends and best practices for online security.	**قم بحماية الأجهزة والشبكة** : • ابق أجهزتك (الكمبيوتر ، الهواتف الذكية ، الأجهزة اللوحية) محدثة باستمرار مع أحدث برامج الحماية • استخدم برامج حماية من الفيروسات ذو نوعية موثوقة وكذلك برنامج حماية من البرمجيات الخبية. • تجنب استخدام الاتصال بشبكة واي فاي عامة لانجاز معاملاتك المصرفية عبر الانترنت. • كن حذراً من تنزيل أية تطبيقات من مصاجر غير موثوقة. **راقب الحسابات باستمرار :** • قم بمراجعة كشوفات حساباتك دورياً وكافة العمليات للتأكد من عدم وجود اية عمليات غير مصرح بهاز • ضع تنبيهاً لمراقبة نشاطات حسابك ، كالعمليات الكبيرة أو الدخول غير الإعتيادي. • قم بإبلاغ البنك فوراً عن أي نشاط مشتبه أو مشكوك فيه. **حماية بياناتك الشخصية :** • كن حذراً من مشاركة بياناتك الشخصة خلال الانترنت أو عبر الهاتف. • قم بتمزيق أو التخلص بشكل آمن من أية مستندات تتضمن معلومات حساسة. • كن على حذر من عمليات الاحتيال المعتمدة على أساليب الهندسة الاجتماعية وتجنب كشف أية بيانات خاصة وحساسة. **درِب نفسك :** • اطلع باستمرار على أحدث أساليب الاحتيال الرقمي ، وعلى أفضل أساليب الحماية للتعاملات عبر الإنترنت.

• Take advantage of the educational resources provided by your bank. **BANQUE BANORIENT FRANCE**	• قم بالاستفادة من المصادر التعليمية التي يقدمها مصرفك **بنك بانورينت فرنسا**