إرشادات التوعية الأمنية للعملاء

متعاملنا الكريم،

في إطار حرصنا في بنك صفوة الإسلامي على تقديم خدماتنا الإلكترونية ضمن أعلى معايير ومستويات أمن المعلومات وحماية سرية معلومات متعامليه، يقوم البنك باتخاذ كافة التدابير والاحتياطات الأمنية الفعالة، وتطبيق أفضل معايير أمن المعلومات العالمية لحمايتكم من أي مخاطر يمكن حدوثها من خلال استخدامكم خدماتنا الإلكترونية.

ونُذكر متعاملنا الكريم بأن بنك صفوة الإسلامي لن يقوم على الإطلاق بإرسال رسالة بريد إلكتروني تتضمن روابط أو مرفقات أو إرسال رسالة نصية أو رسائل من خلال وسائل التواصل الاجتماعي أو الاتصال معكم لطلب معلوماتكم السرية (مثل رقم بطاقة الائتمان أو رقم بطاقة الصراف الآلي أو كلمة السر الخاصة بالبطاقة أو طلب معلوماتكم المتعلقة باسم المستخدم أو كلمات السر للدخول إلى حسابكم المصرفي عبر خدماتنا الإلكترونية مثل الإنترنت البنكي أو الموبايل البنكي). راجين منكم عدم إفشاء هذه المعلومات تحت أي ظرف من الظروف.

بالإضافة إلى الإجراءات الأمنية المتوفرة في خدماتنا البنكية وخدماتنا المصرفية الإلكترونية، نؤكد على أهمية دورك الأساسي في حماية معلوماتك البنكية ولهذا ننصحك باتباع الإرشادات التالية:

١- عدم إفشاء المعلومات البنكية الخاصة بكم:

- رقم بطاقة الصراف الآلي أو رقم البطاقة الائتمانية.
- رقم بطاقة الأحوال والرقم الوطني.
- رقم حسابك في البنك.
- الرقم السري أو اسم مستخدم لخدمات البنك الإلكترونية مثل (الصراف الآلي، خدمة الإنترنت البنكية والموبايل البنكي).

٢- اتباع إرشادات الحماية للبيانات الخاصة بالبطاقات الائتمانية

- لا تقم بإفشاء أو تخزين أي معلومات حساسة ترتبط ببيانات بطاقات البنك الإلكترونية (بطاقات الصراف الآلي أو البطاقات الائتمانية) وغيرها من البطاقات مثل الرقم السري الخاص بالبطاقة ورقم البطاقة.
- يجب عدم إعطاء رقم البطاقة لأي شخص إلا عند الشراء من مواقع تسوق موثوقة وآمنة، علماً بأن البنك يلتزم بالمعيار العالمي الخاص بحماية البطاقات PCI - DSS والذي يتم تجديده سنوياً.
- عدم الاحتفاظ بكلمة السر مع بطاقة الائتمان.

٣- اتباع النصائح الأمنية للحفاظ على الرقم السري الخاص بالخدمات الإلكترونية

- حافظ دائماً على سرية كلمة السر الخاصة بك وعدم تدوينها أو حفظها مع بطاقة الائتمان أو مع اسم المستخدم.
- استخدم كلمة سر معقدة يصعب على الآخرين تخمينها تحتوي على أحرف وأرقام أو رموز خاصة. ينصح بعدم ربط كلمة السر بأي شيء شخصي مثل أعياد الميلاد، أسماء وأرقام متسلسلة.
- قم بتغير كلمة السر بشكل دوري.
- حاول استخدام كلمة سر مختلفة في كل نظام، ولا تستخدم نفس كلمة السر لحساباتك في المواقع على شبكة الإنترنت.

٤- ضرورة معرفة أنواع التهديدات المتعلقة بالإحتيال الإلكتروني:

٤,١ الاحتيال عبر الاستدراج الإلكتروني التصيد (Phishing E-mail)

يقوم المتصيدون بإرسال رسائل الكترونية/ نصية زائفة تطلب من مستخدمي الشبكة زيارة إحدى المواقع الإلكترونية المشابهة لموقع البنك والطلب من المستخدم إجراء تحديث على بياناته، مثل: اسم المستخدم، كلمة المرور، بطاقة الائتمان، أرقام الحساب في البنك.

٤,٢ االإحتيال عبر تقنيات الخداع الإجتماعية (Social Engineering)

هي عملية الحصول - أو محاولة الحصول - على معلومات سرية من خلال قيام المنتحل بالكشف عن المعلومات الخاصة بالمتعامل وتكون عادة بإقناع المستخدمين بأن المتحدث هو شخص مسموح له الحصول على هذه البيانات ومثال لذلك يقوم هذا الشخص بالاتصال التليفوني أو إحدى وسائل التواصل الإجتماعي ومحاولة تعريف نفسه وإقناعك بأنه ممثل للبنك ويناقش معك بعض التفاصيل الخاصة والمعلومات السرية لحساباتك البنكية.

٤,٣ الإيميل المخادع

إرسال رسالة مزيفة عبر البريد الإلكتروني تطلب منك معلومات سرية أو تفصيلية حول حسابك، أو بعض البيانات الشخصية، كأن تستلم بريد إلكتروني مزيف باسم البنك يطلب معلوماتك السرية، ويكون المرسل شخص آخر ويسعى للحصول على المعلومات المصرفية السرية الخاصة بالعميل.

٤,٤ الاحتيال عبر الرسائل النصية القصيرة

من أشكال الاحتيال التي تستخدم الرسائل النصية للهاتف المحمول حيث يتم خداع المستخدم لتحميل فيروسات أو غيرها من البرامج الضارة أو طلب معلومات على الهاتف النقال أو غيرها من الأجهزة المحمولة الأخرى.

٤,٥ الاحتيال عبر البرمجيات الخبيثة والفيروسات

هي نوع من أنواع البرمجيات الضارة والمخادعة التي يتم تثبيتها على الأجهزة الخاصة بالمتعاملين من دون استئذان.

٤,٦ بعض الأساليب الأحتيالية المتعلقة باستخدام الموبايل البنكي

- **البرمجيات الخبيثة المتنقلة "Mobile Malware"** - وهي الفيروسات والجذور الخفية الموضوعة داخل التطبيقات المصرفية التقليدية عبر الإنترنت والمصممة خصيصا لسوق الهاتف المحمول.
- **تطبيقات الطرف الثالث "Third-Party Apps"** تأتي هذه التطبيقات من جهات خارجية بممارسات أمان مشكوك فيها. أو يتم إنشاء التطبيقات من قبل المحتالين وتحميلها مع البرامج الضارة للتمكن من الوصول إلى المعلومات البنكية على جهاز الهاتف المحمول للمتعامل.
- **شبكة Wi-Fi غير المؤمَّنة** - تعد الشبكة اللاسلكية غير الآمنة وسيلة سريعة تتيح للمحتالين الوصول إلى الأجهزة المحمولة، إما للتحكم في معلومات الحساب أو الوصول إليها.

٥- الارشادات المتعلقة بالخدمات المصرفية الآمنة عبر الإنترنت/الموبايل البنكي والحماية من عمليات الاحتيال

- لزيارة موقع بنك صفوة الإسلامي الإلكتروني، دوماً الجأ إلى إدخال العنوان التالي مباشرة في شريط عنوان المتصفح الخاص بـك/ https://www.safwabank.com/ar، وتأكد من وجود رمز https واشارة القفل في منطة العنوان، وكذلك عند الانتقال الى رابط الانترنت البنكي "صفوة أون لاين" https://ibs.safwabank.com/IBS/index.jsp.
- لا تستخدم أي رابط إلكتروني مذكور في رسالة بريد إلكتروني أو الرسائل النصية القصيرة للدخول إلى الخدمة المصرفية عبر الإنترنت ولا تقم بالرد على رسائل البريد الإلكتروني أو الرسائل النصية التي تطلب منك إفشاء معلومات سرية.
- استخدام متصفح انترنت لديه ضوابط أمنية جيدة مثل مانع النوافذ المنبثقة، والتحقق من المواقع الخبيثة والمشبوهة.
- التطبيق الرسمي لخدمة SAFWA Mobile Banking يكون فقط من خلال Google Play Store، Apple App store
- في كل مرة تكمل فيها معاملتك البنكية عبر الإنترنت/ الموبايل، قم بالتأكد من تسجيل الخروج من الموقع Sign Out، و عند كل عملية دخول للخدمة، تأكد من تاريخ اخر دخول سابق للنظام.

- إنشاء واستخدام كلمة سر الموبايل مع ضبط إعدادات الهاتف بحيث يقفل تلقائيا إذا لم تستخدمه لمدة دقيقة أو دقيقتان.
- تأكد من وجود برامج حديثة للحماية من الفيروسات على جهاز الحاسوب الشخصي لديك أو جهاز الموبايل الذي تعتمده لاستخدام الخدمة المصرفية عبر الانترنت/ الموبايل.
- لا تختر الحفظ التلقائي في اختيارات المتصفحات لتخزين أو الاحتفاظ باسم المستخدم وكلمة السر على اجهزتك بطريقة يمكن فهمها من قبل أشخاص آخرين.
- تجنب استخدام الخدمة المصرفية عبر الانترنت/ الموبايل من خلال مقاهي الإنترنت أو الأماكن العامة أو Free Wireless Connection
- في حال تغيير رقم هاتف الموبايل قم بإعلام البنك حتى تتمكن من استقبال الرسائل النصية SMS الخاصة بك ورقم كلمة السر لمرة واحدة OTP للخدمات الإلكترونية.

٦. الحماية من الاحتيال باستخدام أجهزة الصراف الآلي (ATM)

- تأكد من أن لوحة المفاتيح وقارئ البطاقة هي جزء من الجهاز وليست مركبة بشكل خارجي فوق اللوحة الاصلية.
- تأكد من عدم وجود كاميرا مراقبة حول لوحة المفاتيح أو فوقها.
- عند إدخال البطاقة في القارئ، تأكد من وجود الضوء فإن أجهزة سرقة بيانات البطاقات تغطي هذا الضوء.
- التأكد من أن الأفراد الآخرين في طابور الصراف الآلي يقفون على مسافة مقبولة منك.
- تأكد من عدم وجود أي شخص يقوم بمراقبتك أثناء إدخال الرقم السري.
- الوقوف على مقربة من أجهزة الصراف الآلي وتغطية لوحة المفاتيح بيدك عند إدخال الرقم السري.
- إذا شعرت بأن جهاز الصراف الآلي لا يعمل بشكل طبيعي، اضغط على مفتاح إلغاء واسحب البطاقة وقم بإبلاغ البنك بذلك.
- في حال (علقت) البطاقة في جهاز الصراف أو احتفظ بها الجهاز، أو فقدت، يجب إبلاغ البنك على الفور.
- لا تكن على عجلة خلال استخدام جهاز الصراف الألي. وقم بحفظ البطاقة والنقد بعناية في محفظتك، أو حقيبة اليد قبل مغادرة الصراف.

٧- التسوق الآمن باستخدام البطاقات الالكترونية

- يجب عدم النقر على روابط رسائل البريد الإلكتروني التي تدعي بأنها من الموردين أو مواقع التسوّق. وبدلاً من ذلك، يجب كتابة عنوان URL الرئيس للمورد يدوياً أو مواقع التسوّق في المتصفح الإلكتروني.

- أن يتم استخدام النسخة الأحدث من متصفح الإنترنت لما يحتويه من خصائص حماية أفضل.

- لا تحفّظ معلوماتك:
بعض المواقع أحياناً تقدم ميزة "تذكر"، وهي تعني تذكّر معلومات الدفع الخاصّة بك لراحتك خلال مشترياتك المقبلة. ألغِ التحديد لتجنّب ترك أرقام البطاقات في قواعد بيانات التجّار.

٨- التبليغ عن الشبهات الأمنية أو أي عمليات احتيال إلكتروني؟

إذا سأورتك شكوك حول حدوث إختراق أمني غير مصرح به لحساباتك عبر شبكة الإنترنت، أو إذا تم إجراء عملية إلكترونية على حسابك من قبل آخرين، ينبغي عليك إبلاغ بنك صفوة الإسلامي فوراً بالاتصال على هاتف بنك صفوة الإسلامي – مركز خدمات المتعاملين ٠٦ ٤٦٠٢١٠٠ أو زيارة أحد فروع البنك.

ملاحظة: هذه الارشادات تمثل الحد الأدنى من الاجراءات الواجب اتباعها عند استخدامكم لأي من الخدمات الإلكترونية وقد تم اصدارها لزيادة الوعي المصرفي حول استخدام الخدمات المصرفية الإلكترونية دون تحمل البنك أي مسؤولية.