

الإبداع  
القيمة  
الجودة  
المعرفة  
الخدمة

إستخدام خدمات  
البنك الإلكتروني بشكل آمن  
التوعية الأمنية



بنك صفوة الإسلامي  
Safwa Islamic Bank

مبادئ راسخة، حلول مبتكرة Solid Principles, Innovative Solutions

06 4602100 | f | t | in | @ | v | www.safwabank.com

## ارشادات التوعية الامنية للعملاء

متعاملنا الكريم ,,

في إطار حرصنا في بنك صفوة الإسلامي على تقديم خدمات إلكترونية 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 للخدمات الإلكترونية.

وتذكر متعاملنا الكريم بأن بنك صفوة الإسلامي لن يقوم على الإطلاق بإرسال رسالة بريد إلكتروني وأي روابط مرفقة أو إرسال رسالة نصية أو من خلال وسائل التواصل الاجتماعي أو الاتصال أو مطالبتك بالرد والكشف عن معلوماتك أو إدخال بياناتك أو رمز الدخول (User Name, Password) رقم بطاقة الائتمان، أو رقم حسابك المصرفي، كما لن يقوم البنك بطلب اسم المستخدم الخاصة بك والتي تخص خدمات البنك الإلكترونية على الإطلاق.



بنك صفوة الإسلامي  
Safwa Islamic Bank

Username

Password

Login

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

### 1- المعلومات البنكية الخاصة بالمتعاملين والتي يجب عليكم عدم الإفشاء بها للغير مهما كان

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



بنك صفوة الإسلامي  
Safwa Islamic Bank



## ٢- إرشادات لحماية البيانات 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 اعطاء رقم البطاقة لأي شخص إلا عند الشراء من مواقع تسوق موثوقة وامنة، علماً بأن البنك يلتزم بالمعيار العالمي الخاص بحماية البطاقات و معلوماتها PCI - DSS.
- يتم سنويا الحصول على المعيار العالمي PCI DSS لحماية البطاقات و معلومات العميل.
- عدم الاحتفاظ بكلمة السر مع بطاقة الائتمان.



بنك صفوة الإسلامي  
Safwa Islamic Bank



### ٣- نصائح أمنية للحفاظ على الرقم السري الخاص بالخدمات الالكترونية

- حافظ دائماً على سرية كلمة السر الخاصة بك وعدم تدوينها او حفظها مع بطاقة الائتمان او 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 و ارقام متسلسلة.
- قم بتغيير كلمة السر بشكل دوري.
- حاول استخدام كلمة سر مختلفة في كل نظام، ولا تستخدم نفس كلمة السر لحساباتك في المواقع على شبكة الإنترنت.



بنك صفوة الإسلامي  
Safwa Islamic Bank

## ٤- ضرورة معرفة أنواع التهديدات المتعلقة بالإحتيال الإلكتروني:

### ٤,١ الإحتيال 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 الإحتيال 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 بالمعلومات السرية لحساباتك البنكية.



بنك صفوة الإسلامي  
Safwa Islamic Bank

### ٤,٣ الإيميل المخادع

تكمّن هذه العملية عن طريق ارسال بريد إلكتروني مخادع، بحيث يبدو وكأنه من مصدر موثوق، كأن تستلم بريد إلكتروني يظهر بأنه من البنك يطلب منك الموظف معلومات سرية، يكون المرسل شخص آخر ويسعى للحصول على المعلومات.

### ٤,٤ الاحتيال عبر الرسائل النصية القصيرة

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



بنك صفوة الإسلامي  
Safwa Islamic Bank

## ٤,٥ الاحتيال عبر البرمجيات الخبيثة والفيروسات

هي نوع من أنواع البرمجيات الضارة و المخادعة التي يتم تثبيتها على الأجهزة الخاصة بالمعاملين من دون استئذان.

## ٤,٦ بعض الأساليب الأحتيالية المتعلقة باستخدام الموبايل البنكي

- البرمجيات الخبيثة المتنقلة "Mobile Malware" - و هي التروجان والفيروسات 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 الى المعلومات البنكية على جهاز الهاتف المحمول للمتعامل.
- شبكة Wi-Fi غير المؤمنة -تعد الشبكة اللاسلكية غير الآمنة وسيلة سريعة مجانية تتيح للمحتالين الوصول إلى الأجهزة المحمولة، إما للتحكم في معلومات الحساب أو الوصول إليها.





## 0- 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 بك / <http://www.safwabank.com>، وتأكد من وجود رمز HTTPS وأشارة القفل في منطبة العنوان، عند الانتقال الى رابط الانترنت البنكي " صفوة اون لاين " <https://ibs.safwabank.com/IBS/index.jsp>.
- لا تستخدم أي رابط إلكتروني استقبلته عن طريق رسالة بريد إلكتروني او الرسائل النصية لقصيرة للدخول إلى الخدمة المصرفية عبر الانترنت ولا تقم بالرد على رسائل البريد الإلكتروني او 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 بتسجيل الخروج من الموقع، و عند كل عملية دخول للخدمة، تأكد من تاريخ اخر دخول سابق للنظام.
- إنشاء واستخدام كلمة سر الموبايل مع ضبط إعدادات الهاتف بحيث يقفل تلقائياً إذا لم تستخدمه لمدة دقيقة او اثنتان.
- 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 او Free Wireless Connection
- في حال تغيير رقم هاتف الموبايل قم بإعلام البنك حتى تتمكن من استقبال الرسائل النصية SMS الخاصة بك ورقم كلمة السر لمره واحدة OTP للخدمات الاللكترونية.



بنك صفوة الإسلامي  
Safwa Islamic Bank



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

- تأكد من أن لوحة المفاتيح وقرئ 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، فأجهزة الاحتيال 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.
- إذا حشرت البطاقة داخل الجهاز أو احتفظ بها الجهاز، أو فقدت ، يجب إبلاغ البنك على الفور.
- لا تكن على عجلة خلال استخدام جهاز الصراف الآلي. وقم بحفظ البطاقة والنقد بعناية في محفظتك، أو حقيبة اليد قبل مغادرة الصراف.



بنك صفوة الإسلامي  
Safwa Islamic Bank

## ٧- التسوق الآمن باستخدام البطاقات الإلكترونية

- يجب عدم النقر على روابط رسائل البريد الإلكتروني التي تدعي بأنها من الموردين أو مواقع التسوق. وبدلاً من ذلك، يجب كتابة عنوان URL الرئيس للمورد يدوياً أو مواقع التسوق في المتصفح الإلكتروني.
- أن يتم استخدام متصفح انترنت النسخة الاحدث، لما يحتويه من خصائص حماية أفضل.

• لا تحفظ معلوماتك:

بعض المواقع أحياناً تقدم ميزة "تذكر"، وهي تعني تذكر معلومات الدفع الخاصة بك لراحتك خلال مشترياتك المقبلة. ألع التحديد لتجنب ترك أرقام البطاقات في قواعد بيانات التجار.



بنك صفوة الإسلامي  
Safwa Islamic Bank





## ٨- التبليغ عن الشبهات الأمنية او أي عمليات احتيال الالكتروني ؟

إذا ساورتك شكوك حول حدوث اختراق أمني غير مصرح به لحساباتك عبر شبكة الإنترنت، أو إذا تم إجراء عملية إلكترونية على حسابك من قبل الغير، ينبغي عليك إبلاغ بنك صفوة الإسلامي فورًا 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 الالكترونية وقد تم اصدارها لزيادة الوعي المصرفي حول استخدام الخدمات المصرفية الالكترونية دون تحمل البنك اي مسؤولية.



بنك صفوة الإسلامي  
Safwa Islamic Bank