البنك السعودي الفرنسي
Banque Saudi Fransi

الأمن السيبراني لا يكون مكتملًا إلا بك!

الفهرس

نصائح أمنية عامة 01
- خطوات أمنية 02
- كيف تنشئ كلمة مرور قوية؟ 03

تعرف على عمليات الاحتيال والهندسة الاجتماعية 04
- ما هي عمليات الاحتيال (scam)؟ 05
- ما هو التصيّد الإلكتروني؟ 06
- علامات تحذيرية تساعدك في التعرف على حملات التصيد! 07
- ماذا تفعل إذا وقعت في عمليات احتيال؟ 08
- كيف تبلغ عن الأنشطة المشبوهة! 09

فرنسي بلس - الخدمات المصرفية الآمنة عبر الإنترنت 10

فرنسي موبايل - الخدمات المصرفية الآمنة عبر الجوال 11

استخدام بطاقات الصراف الآلي والبطاقات الائتمانية بأمان 12


نصائح أمنية
عامة

النصيحة 01

خطوات أمنية

1

حدّث رقم هاتفك الجوال من خلال أجهزة صراف البنك السعودي الفرنسي أو زيارة فروعه فقط.

2

لا تكشف عن معلوماتك الشخصية أو المصرفية من خلال المكالمات الهاتفية أو عبر الإنترنت.

3

لن يطلب منك موظفو البنك السعودي الفرنسي أبدًا أن تزودهم بمعلوماتك الشخصية أو المصرفية عبر الهاتف أو الرسائل النصية أو البريد الإلكتروني (مثل رقم الهوية الوطنية، معلومات بطاقة الصراف الآلي أو البطاقة الائتمانية، كلمة المرور، اسم المستخدم أو رمز التفعيل المستخدم لمرة واحدة)

4

استخدم كلمات مرور قوية وفريدة لإدارة حساباتك في البنك السعودي الفرنسي عبر الإنترنت.

5

حدّث جميع أنظمة التشغيل لأجهزتك الإلكترونية بما في ذلك البرامج المثبتة عليها كالمتصفحات والتطبيقات ذات الأهمية كتطبيقات الخدمات المصرفية والحكومية وفق آخر تحديث رسمي من المصادر الموثوقة.

6

تجنّب استخدام أجهزة الجوال التي تم التعديل على أنظمة التشغيل فيها بطرق غير مشروعة لإزالة قيود الأمان المثبتة عليها أو ما يسمى بال Jailbreak أو Rooting.

7

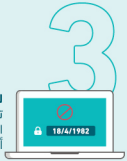
فعّل التوثيق الثنائي المعتمد على المصادر الحيوية كبصمة الإصبع أو التعرف على الوجه في أجهزتك الإلكترونية والتطبيقات التي تتسم بياناتها بالخصوصية العالية كتطبيقات الخدمات المصرفية أو الحكومية.

النصيحة 02

كيف تنشئ كلمة مرور قوية!

طول كلمة المرور!
لتكن كلمة المرور مكونة من 8 إلى 10 أحرف على الأقل.

استخدام مجموعة من الرموز المتنوعة يعني كلمة مرور قوية!
أضف على الأقل حرفًا كبيرًا واحدًا مع استخدام الأعداد (9-0)، وحرفًا خاصًا واحداً @ أو # أو $ أو غير ذلك).



ليكن من الصعب تخمينها!
تجنّب استخدام المعلومات الشخصية (رقم الهوية أو يوم الميلاد أو رقم الهاتف أو أسماء الزوج/الزوجة وأفراد الأسرة).

أنشئ كلمة مرور فريدة يسهل عليك تذكرها!
تجنب كتابة كلمات المرور على الورق، أو حفظها كنص عادي بدون تشفير على هاتفك أو حاسوبك.

الكلمات السرية ليست للمشاركة!
لا تشارك أبدًا كلمات المرور مع الآخرين ولو كانوا أصدقاء أو من أفراد العائلة.


التعرف على عمليات
الاحتيال
والهندسة الاجتماعية

01

ما هي عمليات الاحتيال (scam)؟

هي محاولة للتلاعب بشخص ما وخداعة حتى يقوم بمشاركة معلوماته الشخصية أو الإفصاح عن معلوماته السرية وذلك بقصد سرقة أمواله أو انتحال شخصيته في عمليات احتيال أخرى.

يسعى المحتالون للتواصل معك بقصد جمع معلومات عنك والحصول على معلومات سرية كاسم المستخدم أو كلمات المرور أو معلومات بطاقة الائتمان أو الصراف الآلي. ويقوم المحتالون بذلك مستخدمين أساليب مخادعة ومختلفة عبر رسائل نصية أو رسائل واتساب أو رسائل فورية زائفة، أو عبر وسائل التواصل الاجتماعي أو مكالمات الهاتف، أو حتى محاولة التواصل معك وجهاً لوجه.

ما هو التصيّد الإلكتروني؟

التصيّد الإلكتروني هو النوع الأشهر من عمليات الاحتيال الإلكترونية، وهو شكل من أشكال الرسائل الزائفة التي تدعي أنها تنتمي لجهات رسمية مثل المؤسسات الحكومية والشركات المشهورة أو الخدمات التي يشترك فيها عامة المستخدمين كخدمات البريد وخدمات التسوق الإلكتروني.

قد تصلك رسائل التصيّد عبر البريد الإلكتروني مع روابط للنقر عليها أو مرفقات تتضمن برمجيات خبيثة لتقوم بتحميلها.

قد تصلك رسائل التصيّد عبر الرسائل النصية القصيرة وتتضمن روابط للنقر عليها أو تعليمات لتتبعها

قد تصلك رسائل التصيّد عبر وسائل التواصل الاجتماعي، مثل تويتر وواتساب ولينكدإن وإنستغرام أو فيسبوك، بطرق احتيال مختلفة تطلب منك إرسال صورة أو معلومات بطاقة الصراف الآلي/الائتمانية أو مشاركة رمز التفعيل المؤقت المرسل إليك برسالة نصية.

علامات تحذيرية تساعدك للتعرف على حملات التصيد!

مرسل مشبوه:
رسالة آتية من رقم هاتف أو اسم حساب أو عنوان بريد إلكتروني لا تعرفه.

لغة غير مألوفة مشتملة على أخطاء نحوية:
رسالة تحتوي على أخطاء هجائية أو نحوية ولها تنسيق غير معتاد.

طلب يحثك على التصرف بطريقة عاجلة:
- رسالة تحذرك بأن خدمة معينة علي وشك أن تتعطل إذا لم تدفع غرامة أو تضغط على رابط على الفور!
- رسالة تطلب منك مشاركة رمز التفعيل المستخدم لمرة واحدة الذي استلمته عبر الرسائل النصية أو البريد الإلكتروني على الفور لمساعدتك بخدمة أو تطبيق.

طلب غير متوقع:
- رسالة تحاول إقناعك بتقديم معلومات شخصية لتصلك عروض خصم أو جوائز.
- رسالة تطلب معلوماتك الشخصية لتأكيد شحنة أو طلب خدمة لم تقم بتقديم طلب عليها، ودون أي أرقام تأكيد حتى تتحقق منها!
- رسالة تطلب منك قبول تحويل أموال إلي حسابك المصرفي ومنه إلى طرف آخر، مع الوعد بمنحك مبلغ مالي نظير هذه الخدمة.
- رسالة تأتي من صديق أو فرد من العائلة أو شخص تعرفه تشتمل على طلب غير معتاد، مثل تحويل مال إلى شخص آخر غير معروف.
- رسالة تستغل مواسم سنوية أو أحداث عالمية، مثل كوفيد19-، لتخدع الناس بمعلومات أو خدمات زائفة.

ماذا تفعل إذا تلقيت عمليات احتيال؟

04

1

لا تقم بالرد مطلقًا على أي رسائل إلكترونية مشبوهة أو مكالمات من مصادر غير معروفة.

2

لا تقم بمشاركة أي معلومات سرية عبر الهاتف أو الرسائل النصية أو الرسائل الإلكترونية.

3

لا تثق بالمتصل أو المرسل حتى لو زعم أنه موظف في مؤسسة موثوقة ما لم يتواصل معك من خلال أرقام الهواتف أو عناوين البريد الإلكترونية الرسمية الموثقة في موقع المؤسسة الرسمي.

4

ابحث لتتحقق من هوية المرسل، واسأل عن طريق الاتصال بالرقم الرسمي للمؤسسة أو زيارتها شخصيًا.

5

إذا كنت تعتقد أنك وقعت ضحية لعملية احتيال، أبلغ عن ذلك فوراً

كيف تبلغ عن الأنشطة المشبوهة!

إذا لاحظت أي أنشطة مشبوهة على حساباتك، أو شعرت بأنك وقعت ضحية لعملية احتيال وأرسلت أي معلومات سرية أو مصرفية للمحتالين، أبلغ عن هذا فورًا بالاتصال بفرنسي كير على:

من جوال أو من خارج المملكة:
92 00 00 576

الخط الأرضي داخل المملكة:
800 124 2121


فرنسي بلس
الخدمات المصرفية
الآمنة عبر الإنترنت
Login
Open New Account
FransiCare
FransiMobile

01

استخدم إحدى المتصفحات المعتمدة من البنك السعودي الفرنسي للوصول إلى حسابك على "فرنسي بلس".

تأكد من تحديث متصفح الإنترنت الخاص بك من المصادر الرسمية والموثوقة.

اكتب عنوان URL الآتي: www. fransiplus.com للوصول إلى حسابك على "فرنسي بلس".

تحقق من عنوان URL الخاص بالموقع. فيجب أن يبدأ بـ [https وليس http]. ملحوظة! الـ "S" تمثل التصفّح الآمن.

02

تأكّد من عدم تسجيل الدخول إلى حسابك في فرنسي بلس مستخدماً شبكات الواي فاي العامة/غير الموثوقة، أو من خلال هواتف ذكية وأجهزة لوحية أو حواسيب مشتركة مع الآخرين أو غير محمية.

تجنّب قبول خاصية الحفظ التلقائي لكلمات المرور التي تقدمها لك المتصفحات عند تسجيل الدخول إلى "فرنسي بلس".

استخدم كلمات مرور قوية وفريدة لإدارة حسابك في البنك السعودي الفرنسي عبر الإنترنت.

إذا لاحظت أي أنشطة مشبوهة على حسابك في "فرنسي بلس"، أبلغ البنك السعودي الفرنسي على الفور.

فرنسي موبايل

الخدمات المصرفية
الآمنة عبر الجوال

01

يتيح لك البنك السعودي الفرنسي الوصول السريع والآمن إلى حسابك المصرفي عبر الإنترنت باستخدام تطبيق فرنسي موبايل.

حمّل تطبيق فرنسي موبايل المصرح به فقط من متاجر تطبيقات الجوال الرسمية.

حدّث تطبيق فرنسي موبايل الخاص بك دائمًا من خلال التحديثات الرسمية المتاحة في متاجر التطبيقات الرسمية.

كن حذرًا جدًا مع التطبيقات التي تطلب إذن الدخول والتحكم بمعلوماتك شخصية، مثل قائمة جهات الاتصال وموقعك الجغرافي والرسائل القصيرة والصور.

5

اسمح للتطبيقات الموثوقة بالوصول المحدود الى المعلومات المخزنة في جهازك بالاستناد إلى الخدمة المقصودة من كل تطبيق.

6

راجع كل الأذونات الممنوحة بشكل منتظم وامنع الوصول من التطبيقات المشبوهة أو التي لم تعد تستخدمها.

7

قم بتفعيل التوثيق الثنائي المعتمد على المصادر الحيوية كبصمة الإصبع أو التعرف على الوجه على هاتفك الجوال، وتأكد من ضبط وقت قصير لخاصية القفل التلقائي.

8

استخدم كلمات مرور قوية وفريدة لإدارة حسابك في البنك السعودي الفرنسي عبر الإنترنت.


استخدام
بطاقات الائتمان
مدى بأمان

01

لا تنشر أو تشارك معلومات بطاقة الصراف الآلي أو البطاقة الائتمانية، مثل رقم البطاقة الكامل أو تاريخ الانتهاء أو الرمز السري أو رمز CVV مع أي شخص عبر الإنترنت أو الهاتف أو الرسائل النصية/الفورية.

لن يتواصل معك فريق عمل البنك السعودي الفرنسي عبر الهاتف أو الرسائل النصية أو البريد الإلكتروني ليطلب منك تقديم معلومات شخصية أو معلومات بطاقة الصراف الآلي أو البطاقة الائتمانية.

لا تكتب أبدًا رقم العميل أو الرقم السري الخاص ببطاقة الصراف الآلي أو البطاقة الائتمانية على ظهر البطاقة.

كن حذرًا عند التسوق عبر الإنترنت، وتسوق فقط من مواقع تجارية موثوقة ممن يتمتعون بسمعة طيبة في التعامل مع معلومات العملاء.

5

تجنّب تخزين معلومات بطاقة الائتمان/ مدى على مواقع التسوق.

6

ينبغي التخلص من بطاقة الصراف الآلي أو البطاقة الائتمانية المنتهية الصلاحية بشكل مناسب من خلال قطع البطاقة من الرقاقة والشريط الممغنط.

7

إذا تعرضت لسرقة أو فقدت بطاقة الصراف الآلي أو البطاقة الائتمانية، أبلغ "فرنسي كير" على الفور.