البنك
السعودي
الفرنسي
Banque
Saudi
Fransi

# الأمن السيبراني لا يكون مكتملًا إلا بك!

# Security is not complete without you !

# Index

# الفهرس

# نصائح أمنية عامة
# General Security Tips

# خطوات أمنية
## النصيحة 01

1 

**حدّث رقم هاتفك الجوال** من خلال التواصل مع فريق الدعم للفرسي جلوبال.

**Update your mobile phone** number only through Fransi Global support team.

2 

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

**Do not disclose your personal** or banking information through phone calls or online.

3 

**لن يطلب منك موظفو البنك السعودي الفرنسي** أبداً أن تزودهم بمعلوماتك الشخصية أو المصرفية عبر الهاتف أو الرسائل النصية أو البريد الإلكتروني (مثل بطاقة الصراف الآلي أو البطاقة الائتمانية، كلمة المرور، اسم المستخدم أو رمز التوثيق).

**BSF staff will never ask** you to provide personal or banking information such as credit/ debit card information, password, username, or one-time PIN over the phone or via text messages.

4 

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

**Use strong/complex passwords** for your Fransi Global account.

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.

**Maintain the security** of all your devices by keeping the operating system, browsers, and banking application up to date with the latest official/legitimate updates.

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.

**Avoid using un official/customized** mobile phones through Jailbreak or rooting to access your banking services.

7 

**فعّل التوثيق الثنائي** المعتمد عبر استخدام جهاز المشفر أو تطبيق المشفر.

**Add an extra layer of security** by enabling two-factor authentication via a security Token device or soft Token app.

# Security Steps
## Section 01

# How to create a strong password?

## Section 02

# كيف تنشئ كلمة مرور قوية!

## النصيحة 02

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

**Password length!** Make your password at least 8 to 10 characters long.

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

**Complex combination means strong passwords!** Add at least one capital letter, numeral (0-9), and special character (@, #, $, etc.)

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

**Make it harder to guess!** Avoid using personal information (ID number, birthday, phone number, spouse or family member names.)

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

**Create it as unique but memorable!** Avoid writing your passwords on papers or saving them as plaintext on your phone or computer.

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

**Sharing is not caring!** Never share your passwords with others even friends and family members.

**عدم تكرار كلمات المرور!** في جميع التطبيقات كي لا يسهل على المحتال اختراق جميع التطبيقات

**Avoid using un official/customized** mobile phones through Jailbreak or rooting to access your banking services.


التعرف على عمليات الاحتيال
والهندسة الاجتماعية
Identify Scams and
Social Engineering

# What is a scam!

## Section 01

Scam is an attempt to manipulate or trick someone into sharing their personal or confidential information with the intention of stealing their money or impersonating their identity for further scamming campaigns.

Scammers might attempt to contact you in order to steal your sensitive information such as username, passwords, or credit/debit cards information through many different techniques such as: fake text messages, WhatsApp messages, instant messaging, through social media, via phone calls or even reach you in person.

# ما هي عمليات الاحتيال (scam)؟

## النصيحة 01

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؟

## النصيحة 02

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.

# What is a Phishing!

## Section 02

Phishing is one of the most common type of scams which is a form of deceptive and fake messages that appear to be coming from a legitimate source such as governmental institutions, popular companies, or services that victims subscribe to.

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

Phishing messages might come to you via emails with links to click on or attachments that contain malwares to download.

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

Phishing messages might come to you via SMS text messages with links to click on or instructions to follow.

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.

Phishing messages might also come to you via social media such as Twitter, WhatsApp, LinkedIn, Instagram or Facebook asking for your credit/debit card information or a copy of your card.

# علامات تحذيرية تساعدك للتعرف على حملات التصيد!

## النصيحة 03

**مرسل مشبوه:**

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

**Suspicious sender:**

A message coming from a phone number, account name, or email address that you do not know.

**لغة غير مألوفة مشتملة على أخطاء نحوية:**

رسالة تحتوي على أخطاء هجائية أو نحوية ولها تنسيق غير معتاد.

**Unusual language with grammar mistakes:**

A message coming from a phone number, account name, or email address that you do not know.

**طلب يحثك على التصرف بطريقة عاجلة:**

رسالة تحذرك بأن خدمة معينة على وشك أن تتعطل إذا لم تدفع غرامة أو تضغط على رابط على الفور!

**Urgent call for action:**

A message warning you that a certain service is about to be disabled or revoked if you do not pay a fine or click a link immediately!

رسالة تطلب منك مشاركة رمز التفعيل المستخدم لمرة واحدة الذي استلمته عبر الرسائل النصية أو البريد الإلكتروني على الفور لمساعدتك بخدمة أو تطبيق.

A message asking you to provide the One-time password received via text message immediately to help you with a service or application.

# Warning signs of phishing campaigns!

## Section 03

**طلب غير متوقع:**

رسالة تحاول إقناعك بتقديم معلومات شخصية لتصلك عروض خصم أو جوائز.

**Unexpected request:**

A message trying to convince you to give your personal information in order to receive discount offer or a prize.

رسالة تطلب معلوماتك الشخصية لتأكيد شحنة أو طلب خدمة لم تقم بتقديم طلب عليها، ودون أي أرقام تأكيد حتى تتحقق منها!

A message asking for your personal information to confirm a shipment or a service request you do not know and without any confirmation numbers to check!

رسالة تطلب منك قبول تحويل أموال إلى حسابك المصرفي ومنه إلى طرف آخر، مع الوعد بمنحك مبلغ مالي نظير هذه الخدمة.

A message asking you to accept transferring funds in and out of your own bank account to a third party and promis granting you easy money in return of this service.

رسالة تأتي من صديق أو فرد من العائلة أو شخص تعرفه تشتمل على طلب غير معتاد، مثل تحويل مال إلى شخص آخر غير معروف.

A message that comes from a friend, family, or someone you know with unusual request such as transferring money to unknown third person.

رسالة تستغل مواسم سنوية أو أحداث عالمية، مثل كوفيد-19، لتخدع الناس بمعلومات أو خدمات زائفة.

A message that takes advantage of holydays or latest trends such as COVID 19, to deceive people with fake information or services.

## What to do in case you received scams?

## Section 04

## ماذا تفعل إذا تلقيت عمليات احتيال؟

## النصيحة 04

1

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

Do not respond at all if you receive emails, messages, or phone calls from unknown sources.

2

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

Do not ever give confidential information over the phone, via text message or emails.

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.

Do not trust the caller or sender even if they claim to be an employee from a legitimate organization you subscribe to.

4

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

Do your research to validate the sender identity and request by calling the official number of the organization or visit them in person.

5


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

If you think you may have been a victim of a scam, report it immediately!

## كيف تبلغ عن الأنشطة المشبوهة!

**النصيحة 05**

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:

البريد الإلكتروني :

Email

**FransiGlobal@alfransi.com.sa**

## How to Report suspicious activities!

**Section 05**

If you notice any suspicious activity on your accounts, or if you fallvictim to criminals and sent any confidential or banking information to scammers.


فرنسي جلوبال الخدمات
المصرفية الآمنة عبر الإنترنت
FransiGlobal Secure
Online Banking

## Secure Online Banking
## Section 01

## الخدمات المصرفية الآمنة عبر الإنترنت
## النصيحة 01

استخدم احدى المتصفحات المعتمدة من البنك السعودي الفرنسي للوصول إلى حسابك على "فرنسي جلوبال".

Use only the approved browsers list from BSF to access your FransiGlobal account.

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

Make sure your web browser is updated from the official sources.


اكتب عنوان URL الآتي:
**https://digital.fransiglobal.com/**
للوصول إلى حسابك على "فرنسي جلوبال".

Type the following URL address:
**https://digital.fransiglobal.com/**
to access your FransiGlobal account.


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

Double check the URL of the website, it has to start with [https not http]. Notice! The "s" represents secure browsing.

## الخدمات المصرفية الآمنة عبر الإنترنت
## النصيحة 01

## Secure Online Banking
## Section 01

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

Be careful not to log into Fransi Global through public /untrusted Wi-Fi networks or from shared or unprotected smart phones, tablets, and computers.

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

Avoid accepting passwords auto-save feature prompted to you by the browser upon logging into FransiGlobal.


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

Use strong and complex passwords for your FransiGlobal online accounts.


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

If you notice any suspicious activities on your FransiGlobal account, report it to BSF immediately.