البنك السعودي الفرنسي
Banque Saudi Fransi

Security is not complete without U!

Index


General
Security
Tips

Section 01

Security Steps

1

Update your mobile phone number only through Fransi ATM or branches.

2

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

3

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

4

Use strong/complex passwords for your Fransi online accounts.

5

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

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

7

Add an extra layer of security by enabling biometric authentication on your devices such as using fingerprint or facial recognition.

Section 02

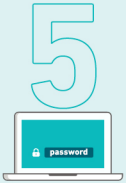
How to create a strong password?

Password length!
Make your password at least 8 to 10 characterslong.

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

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

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



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


Identify
Scams
and social Engineering

01

What is a scam!

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.

02

What is a Phishing!

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.

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

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

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.

03

Warning signs of phishing campaigns!

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

Unusual language with grammar mistakes:
A message coming from a phone number, account name, or email address that you do not know.

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

Unexpected request:
- A message trying to convince you to give your personal information in order to receive a discount offer or a prize.
- 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!
- A message asking you to accept transferring funds in and out of your own bank account to a third party and promise granting you easy money in return of this service.
- A message that comes from a friend, family, or someone you know with unusual request such as transferring money to unknown third person.
- A message that takes advantage of holydays or latest trends such as COVID 19, to deceive people with fake information or services.

04

What to do in case you received scams?

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

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

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

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

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

How to Report suspicious activities!

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

Land line inside KSA:
800 124 2121

From a Mobile Phone or outside KSA:
92 00 00 576

FransiPlus

Secure Online Banking

01

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

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

Type the following URL address: www.fransiplus.com to access your FransiPlus account.

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

02

Be careful not to log into FransiPlus through public/untrusted Wi-Fi networks or from shared or unprotected smartphones, tablets, and computers.

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

Use strong and complex passwords for your Fransi online accounts.

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


FransiMobile
Secure Mobile Banking

01

Quick and secure access to your online bank account is available through FransiMobile application.

Download the authorized FransiMobile application ONLY from official mobile application stores

Keep your FransiMobile application up to date with the official updates available on the legitimate mobile application stores.

Be extra cautious with downloaded applications that request access permissions to personal information such as your contact list, location, SMS and photos.

02

Carefully give access permissions only based on each application's intended service.

Regularly review all granted permissions and deny access to suspicious applications.

Activate password protection/biometric authentication on your mobile phone and make sure to set a short time for the auto-lock feature.

Use strong and complex passwords for your Fransi online accounts.

Credit/Debit Cards

Using your Cards Securely

01

Never post or share your credit/debit card information such as the complete card number, expiration date, PIN number, or CVV code with anyone online, over the phone, or via text/ instant messaging.

BSF staff will never contact you over the phone, text messing, or by email to ask you to provide personal or credit/debit card information.

Never write the PIN number of your credit/debit card information on the back of the card.

Be extra careful when shopping online and only shop from trusted ecommerce sties who have a great reputation in handling customer information.

02

Avoid storing your credit/debit card information into shopping websites.

Expired/old credit or debit cards should be disposed properly by cutting the card through the chip and the magnetic strip.

If your credit/debit card is lost or stolen, report it to FransiCare immediately.