BSF Security Center
FransiPlus

البنك السعودي الفرنسي
Banque Saudi Fransi

Banque Saudi Fransi is committed to the security and privacy of your information.We ensure security by ensuring Confidentiality of your information, Integrity of your transactions and Availability of BSF systems for your online banking transactions.

While Banque Saudi Fransi has cutting edge technology and state-of-the art processes and professionals deployed to extend secure internet banking to its customers, it is important for customers to know that "SecUrity is incomplete without U". Customers need to be alert and exercise caution when using FransiPlus to avert any frauds or security breaches to their accounts.

How we protect YOU

General Security Controls

Banque Saudi Fransi has implemented a robust Risk Management Framework and cutting edge security technologies and solutions such as Firewalls, Intrusion Detection Systems, Multi Factor Authentication etc. in order to protect our systems against threats from the Internet.

Registration Security

To facilitate both a secure and convenient online registration to FransiPlus, you need to have an account with Banque Saudi Fransi (BSF) and provide your ATM card and PIN number information for verification purposes.Entering your correct ATM card number and PIN represents the first stage in identification and authentication.The second stage requires you to provide your corresponding BSF bank account number and National ID / Iqama number.If all of this information is valid, then you can proceed with choosing a Subscriber ID and password, at which point access is granted.

Why do I have to enter the characters shown in the image on the first page of FransiPlus Online Registration and Forgot password?

The image's characters are to tighten the security measures of online registration and forgot password processes within FransiPlus.

I have forgotten my FransiPlus password - what should I do?

You can use the Forgot Password link on the FransiPlus homepage and follow the instructions. Contact our customer service on 800-124-2121 for any problem or inquiry

Secure Login

To restrict unauthorized access to your FransiPlus account and to ensure only you have access to your FransiPlus account, 2 Factor Authentication has been implemented for FransiPlus.

Stage 1:

To begin a session with FransiPlus, you must enter your correct Subscriber ID and password. On successful authentication at the first stage, a unique One Time Password will be sent to the subscriber's mobile number registered with the bank.

Stage 2:

The subscriber will be able to access his/her FransiPlus account only after successfully authenticating on the second stage by entering the unique One Time Password.

Secure Data Transmission

All information that flows between your web browser and FransiPlus is protected by 2048-bit strength Secure Sockets Layer (SSL) encryption, which is a strong safeguard to maintain the privacy and confidentiality of data in transit.

Account Lockout

FransiPlus uses a lockout mechanism to deter unauthorized users from repeated Subscriber ID and password guessing attempts.After five unsuccessful attempts, the system locks the Subscriber ID being attempted, requiring a phone call to BSF to re-authenticate you before reactivation.

Automatic Logout

To provide additional protection, a timeout feature is in effect whilst using FransiPlus, in case you walk away from your computer and forget to log-out. This feature automatically logs you out of your session after a period of inactivity. Re-establishing and authenticating your credentials for your online session helps to reduce unauthorized access to your accounts.

Saudi Arabia's Leading Security Team

Banque Saudi Fransi has a dedicated security department which ensures FransiPlus maintains the highest possible level of security.

Sending E-mail to Banque Saudi Fransi

E-mails sent within the Fransiplus.com.sa website are secure. However, e-mails sent to Banque Saudi Fransi via other means may not be secure. Therefore, we advise you not to send confidential information via an unsecured e-mail.

How Attackers target YOU

Email scams

If you receive an email asking for your personal details such as Subscriber ID, Password, card details etc., please do not reply as it might be fraudulent. Kindly note that Banque Saudi Fransi will never contact you to ask you for personal information such as Subscriber ID, Password, Credit Card Number etc. via email, phone or any other means, so do not be tricked by these emails.

Be wary of emails especially if they prompt you to visit FransiPlus by clicking on a link in the email. These emails may say they are security alerts from Banque Saudi Fransi, or mails about the status of your account.

You can check the authenticity of the site by reviewing the certificate as detailed above. If you're in any doubt about the source of an email, it's best to delete it without opening it.

Banque Saudi Fransi will never contact you by email to ask you questions related to your account so don't be tricked by these emails.

Fake Websites

Fraudsters may try to trick you to visit bogus websites which may look similar to FransiPlus. The only purpose of these sites is to fool you to entering your FransiPlus ID and password. Don't be fooled by these sites and only ever visit the real FransiPlus site by checking the websites certificate as detailed in reviewing the certificate.

Malware

Fraudsters may trick you to install malicious software on your computer. The malicious software may steal your personal information to steal your login credentials, perform unauthorized transactions on your behalf etc.

Phishing

'Phishing' is an act of sending a fraudulent e-mail or creating a forged screen or pop-up, in an attempt to capture a customer's sensitive personal details like User ID, Password or PIN, Date of Birth, CVV number etc.

Verify FransiPlus's Security Certificate before entering any sensitive information.

Always remember that Banque Saudi Fransi never send any emails to customers asking for sensitive information.

Vishing

Vishing is the concept of phishing over a voice channel.Fraudsters claiming to represent real companies such as banks attempt to trick customers into providing their personal and financial details over the phone.

Do not reveal any personal or sensitive information on a telephone call, even if the caller claims to be from your bank.

Do not call and or disclose any personal or sensitive information on any telephone system that you are directed to by a telephone message or

from a telephone number provided in a phone message, an e-mail or an SMS.

When dialing Banque Saudi Fransi customer center, always use the contact number provided behind your debit card or credit card to ensure that you are dialing to the BSF genuine customer care.

Improve your Security

Take these steps when you're using Online Banking to keep your account information safe.

Always enter the FransiPlus website URL "https://fransiplus.com.sa", directly into your browser address bar before you login to ensure that you are on the legitimate FransiPlus website. Never click a link that offers to take you to our website. This will reduce the chances of you becoming a victim of phishing attacks.

Before Logging in to FransiPlus, double-click the padlock symbol on your browser to ensure the site certificate belongs to FransiPlus. This will ensure you're not being duped into entering your details on a 'fake' site. How to check the site certificate.

Password Security

Choose a password that is hard to guess or identify as relating to you.

When you create your password, make it at least 8 characters long. Include at least one capital letter, one numeral (0-9) and one special character (like @, #, $, etc.). This makes the password comparatively difficult to crack.

Don’t use the same password you use for other purposes.

Ensure that no one is watching you while you key in your password / PIN or any other sensitive information.

Don’t disclose your password, PIN, CVV to anyone. Banque Saudi Fransi will never ask you to divulge your password, PIN, CVV or other personal information

Change your FransiPlus password at periodical intervals (at least once in every 90 days).

Do not select the option auto-save on browsers for storing or retaining user name and password when logging into FransiPlus.

Keep your personal details secret. Never write down or reveal your Subscriber ID or Password.

Change your FransiPlus password from a secure computer immediately if you suspect your account has been compromised or if you had to use a public/shared computer for logging in to your FransiPlus account for any reason.

Keep your operating system (eg. Windows XP, Macintosh etc.) and web browser (eg. Internet Explorer, Safari etc.) up to date. Flaws are sometimes found in these products and the publishers will issues 'patches' to correct the problem.

Update your system and web browser

Download the latest manufacturers' security patches:

Windows and Internet Explorer | Apple Macs

Use a personal firewall and anti-virus software to prevent unauthorized access and viruses being downloaded onto your PC when you're on the Internet. Ensure that your anti-virus software is updated with the latest signatures.

Be wary of emails especially if they prompt you to visit FransiPlus by clicking on a link in the email. You can check the authenticity of the site by reviewing the certificate as detailed above. If you're in any doubt about the source of an email, it's best to delete it without opening it.

Avoid using cyber cafes or shared computers to access your FransiPlus account. PCs at cyber cafes may be infested with viruses and Trojans that can capture and transmit your personal data to fraudsters. Your personal information may be grabbed easily using key logging software, which records all the keystrokes you typed, to be retrieved later for fraudulent usage. Beware of typing passwords on unknown PCs. If you access your FransiPlus account from a cyber cafe or on a shared computer for any reason, change the password as soon as you can access your secured computer.

Beware of websites offering free software or applications - don't download software unless you are sure the site is genuine and the application is not harmful.

Avoid using cracks, key generators and other pirated software as they may contain virus, trojans or other malware that may affect the security of your online banking accounts.

Adequately protect your home WiFi (wireless) network if you are using one. Do not use public/unsecured WiFi (wireless) networks. These public/unsecured WiFi (wireless networks)

Update Banque Saudi Fransi with your new contact details when you change your contact details. This will enable us to contact you in a timely manner if we detect unusual transactions.

Never leave your PC unattended while you're logged in to the service. Do not directly close the browser without logging off from your FransiPlus account.

Always log-out after using FransiPlus by selecting the log-out button, close the browser window to clear the web page history stored in memory. logging off from your FransiPlus account.

After logging-out of FransiPlus by selecting the log-out button, always close the browser window to clear the web page history stored in memory.

We automatically instruct most browsers not to store your personal information in the cache (memory). As this may be affected by the type of browser you use, always clear the cache yourself.

Checking FransiPlus's security certificate

How to check a site certificate

1. Double-click on the padlock in your browser window.
2. A dialogue box opens. Click on the 'Details' tab at the top.
3. Select the entry marked 'Subject'.
4. The entry marked 'CN' should be secure.fransiplus.com.

How to check the security certificate is valid:

After double-clicking the padlock (as above):

1. Click on the tab that says 'certification path' in the dialogue box.
2. Select secure.fransiplus.com in the certification path dialogue box.
3. Verify that it says 'This certificate is OK' in the certificate status dialogue box.

Detecting Fraud

Possible Unauthorized Logons

The best way to stay informed about your activities within FransiPlus is to view the last logon date and time.The last logon date and time is displayed in the top left-hand corner of the screen and indicates when we recorded you last accessing FransiPlus.If you do not remember accessing FransiPlus at this time, then please report the matter immediately to us.

You can also review the activities performed during your last logon session by selecting the 'Session History' option.If you notice any activities that you believe you have not performed then please contact us immediately.

Possible Unauthorized Transactions

Regularly check your online balance and transaction history and report any irregularities.In addition to the 'Last Ten FransiPlus Transactions' , the best way to stay informed about your account is to ensure that your online records match your hardcopy BSF account statement.

FransiPlus provides email notifications, SMS messages, and online statement capabilities to assist you in monitoring your account activity.Be aware of the activities in your account and contact us immediately to report any discrepancies.

Reporting Fraud

If you suspect a fraud or if you have revealed your security details in any way, it is important that you notify us immediately by calling FransiCare at 800 124 2121 (National) or +966 1 4089089 (international).

البنك السعودي الفرنسي
Banque Saudi Fransi

Browser Upgrade Notice

In compliance with industry standards and best practices, starting August 8, 2017 we are disabling access to Online Banking from browsers that do not support TLS version 1.2. We strongly recommend you to use the latest version of the web browser when conducting transactions through our online banking FransiPlus. For your convenience, below is the list of supported browsers.

Browser	TLS 1.2 Compatibility Notes
Microsoft Edge	
Desktop and mobile versions	Supported and Compatible by default
Microsoft Internet Explorer (IE)	
Desktop and mobile IE version 11	Supported and Compatible by default
Desktop IE versions 9 and 10	Supported when run in Windows 7 or newer, but require actions. (see below)
Desktop IE versions 8 and below	Not Supported.
Mozilla Firefox	
Firefox 27 and higher	Supported and Compatible by default.
Firefox 23 to 26	Supported but require actions. (see below)
Firefox 22 and below	Not Supported.
Google Chrome	
Google Chrome 38 and higher	Supported and Compatible by default.
Google Chrome 37 and lower	Not Supported.
Google Android OS Browser	
Android 6.0 (Marshmellow) and higher	Supported and Compatible by default
Android 5.0 (Lollipop) and higher	Supported and Compatible by default
Android 4.4 (KitKat) to 4.4.4	Not Supported.
Android 4.3 (Jelly Bean) and below	Not Supported.
Apple Safari	
Desktop Safari versions 7 and higher for OS X 10.9 (Mavericks) and higher	Supported and Compatible by default
Desktop Safari versions 6 and below for OS X 10.8 (Mountain Lion) and below	Not Supported.
Mobile Safari versions 5 and higher for iOS 5 and higher	Supported and Compatible by default
Mobile Safari for iOS 4 and below	Not Supported.
Opera	
Opera version 17and higher	Supported but require actions. (see below)

How to Enable TLS 1.2

Internet Explorer

- Open Internet Explorer
- Click Alt+T and select Internet Options
- Select the Advanced tab
- Scroll down to the Security section
- Locate and check Use TLS 1.2
- Then, press the OK button

Google Chrome

- Open Google Chrome
- Click Alt+F and select Settings
- Scroll down and select Show advanced settings.
- Scroll down to the Network section and click on Change proxy settings...
- Select the Advanced tab
- Scroll down to the Security section
- Locate and check Use TLS 1.2
- Then, press the OK button

FireFox

- Open FireFox
- Type in "about:config" in the URL bar and press Enter
- Scroll down to "security.tls.version.max" and press Enter
- Set the value to 3
- Then, press the OK button

Opera

- Open Opera
- Click Ctrl+F12
- Click on Security
- Click on Security Protocols...
- Check on Enable TLS 1.2 Press the OK button.