البنك السعودي للاستثمار
The Saudi Investment Bank

BE SECURE...BE AWARE

Counter-Fraud Awareness Program

Dear Customer,

As we work hard to protect the Banking sector from fraud, we take the security of our customer's information very seriously. We believe that a collaborative effort between us can go a long way in combatting the problem of fraud.

The purpose of this document is to share some updates related to fraud covering the latest trends and tactics used by fraudsters and sharing best practices to protect yourself from any exposure.

We would also like to request that you keep us informed of any suspected activity or actual fraud as early detection is key to preventing further losses and ensuring that our mutual information is protected.

We believe that by working together, we can significantly reduce the exposure to fraud and thereby protect our interests.

Thank you for your attention to this matter and look forward to your continued support on our fraud awareness initiatives.

Sincerely,

The Saudi Investment Bank

Our Counter-Fraud Philosophy

We are committed to maintaining the highest standards of ethics and integrity in all aspects of our business, including preventing and detecting fraudulent activity. We believe that fraud prevention is a critical component of our responsibility to protect the interest of customers and all parties we are associated with.

The Counter-Fraud philosophy is rooted in the following principles:

Zero Tolerance	A zero-tolerance policy towards any fraudulent behavior and is committed to taking swift and appropriate action against the perpetrator.
Proactive Prevention	Promote a proactive approach towards fraud prevention which includes implementing robust controls, providing regular training and awareness, and a culture of integrity.
Early Detection	Emphasize on implementation of a mechanism for early detection of fraud such as regular monitoring and review, timely review of financial transactions and statements, etc.
Swift Response	Initiate a quick response to the detection of fraud including investigating of incidents, recovery of losses, and disciplinary actions required.

"Protecting our customer's interests is our top priority. We request you to join us in our commitment to preventing and detecting fraud and ensuring a safe and secure operating environment for everyone."
- The Saudi Investment Bank

What is Social Engineering?

Social Engineering is a technique used to gain information known about a user to elicit additional information from the target user. So basically, Social Engineering leads to Identity Theft.

Types of schemes used by fraudsters for Identity Theft:

What is Phishing?	Phishing is a technique used to gain personal information for the purpose of identity theft by using fraudulent e-mail messages that appear to come from legitimate sources.
What is Smishing?	Smishing is another form of Phishing where a fraudster will send a Scam SMS to trick the victim into sharing confidential financial details or personal information.
What is Vishing?	Vishing is a technique that uses phone calls or voice-based messages to trick people into sharing sensitive information such as financial details or personal information.
What is Spoofing?	Spoofing is a technique that uses an email address, display name, phone number, text message, or website URL to convince a victim to part with the financial details or personal information.

How to protect yourself:

- Do not open any suspicious emails from unknown sources.
- Do not click on links or attachments sent by unknown people.
- Do not reply to emails or calls that look suspicious or ask to share personal information such as National ID/ Iqama Number, account number or PIN or password.

What is Breach in Cybersecurity?

A cybersecurity breach is any incident that results in unauthorized access to computer data, applications, networks, or devices. It results in information being accessed without authorization.

Types of schemes used by fraudsters for inducing Cybersecurity breach:

What is Malware?	Malware attacks are usually orchestrated through malicious websites, emails, software, etc. Malware can be hidden in other files, such as image or document files, or seemingly innocuous files such as .exe file.
What is Scareware?	Scareware is a tactic that scares people into visiting spoofed or infected websites or downloading malicious software. Scareware can be sent in the form of pop-ups ads or spread through spam email.
What is Ransomware?	Ransomware is a technique in which the victim's system is held hostage until they agree to pay a ransom. After the payment is sent, the fraudster provides instructions to regain control of the computer.
What is Denial of Service(DOS)?	DOS is a technique in which a fraudster sends a massive amount of traffic to the victim's computer and shut them down. This makes the victim's website unavailable for its users.

How to protect yourself:

- Implement strong passwords, access controls, and data encryption to protect your accounts and systems from unauthorized access
- Implement Two-factor authentication as an added layer of security
- Conduct system and process audits to identify risks

What is Your Responsibility?

As a Service Provider of SAIB, we request you to partner with us in our endeavor to combat fraud. We expect you to stay vigilant and report any suspected or fraudulent activity directly to us.

The steps to be followed in case of a fraudulent activity identified:

Stop the Fraudulent Activity	Take immediate steps in your capability and capacity to stop any fraudulent activity that comes to your notice to prevent any further financial loss or reputational damage to the bank or yourself.
Ensure you Notify us	Notify us immediately if you suspect or identify fraud to allow us to take appropriate and timely action to mitigate the risk. You can use any of the reporting channels to notify us.
Collect and Preserve Evidence	Collect and preserve any evidence regarding the suspected or fraudulent activity such as emails, invoices, or any other evidence that will support the investigation.
Cooperate in the Investigation	Cooperate fully with our investigation team as and when required including providing the available information on the incident or any interviews as a part of the investigation.