JS Bank Security Advisory

As a responsible financial institution, it is our responsibility to keep customers updated regarding financial scams, to help keep your banking relationships secure.

We live in a digital world where more members than ever before are banking online or on their mobile phones.

Internet and Mobile banking make daily banking fast and convenient, and with the tools we've put in place to make your online banking experience secure and safe, the risk to you and your money is low. However, online and mobile banking is never 100 per cent safe. There are many fraudsters out there who've made it their business to get you into sharing your financial information by using sophisticated tools that look real to most users.

Through this advisory, we aim to educate you on the most common types of Internet and Mobile banking fraud, share what we're doing to protect you, and give you some quick and easy tips for protecting yourself.

- Phishing/Scamming and fraudulent e-mails
- Malware and viruses
- Mobile fraud
- Text message fraud (Smishing)

Scamming incidents are based on customers sharing their information (such as CNIC, internet banking password, ATM/Financial PINs, mother's maiden name, credit/debit card numbers etc.). Perpetrators of "phishing" will go to any lengths to look convincing, including developing fake websites, offering participation rewards, sending masked SMS messages, or other means to access your emails.

Con artists and fraudsters are becoming more sophisticated in finding ways to access your personal and financial information online without your knowledge. One of the most insidious methods is through the use of unwanted, malicious software – generally referred to as malware – that's installed without your knowledge on your computer. This can happen when you visit to certain websites, download videos or files, etc.

The risks to members of mobile fraud are similar to other types of online fraud. Fraudsters try to obtain information through various means on your mobile device (tablets, smartphones and more) to access your personal and account information. For instance, phishing on phones via phone calls made through massed phone numbers, Such calls can be identified as before the caller number there will be a + sign or 00 appearing.

Another type of mobile fraud and a variant of the email phishing scam is smishing (SMS phishing or smishing), which uses text messages to get you into sharing your financial and personal information and access non-secure weblinks.

JS Bank is committed to protecting your personal information. Our Mobile and Internet Banking services use several different methods to protect unauthorized access to your account. Accessing Internet or Mobile Banking requires multiple levels of security, which are designed to ensure fool-proof security for your financial relationship.

JS Bank will NEVER request personal information by email, phone or SMS, specifically account numbers, passwords, personal identification numbers or any other confidential information. Fraudulent emails and SMS may be designed to appear as though they have originated at JS Bank. Do not respond to any email or SMS message which requests any type of confidential information, and do not click on any links listed on such emails and SMS messages.

In addition to the security features put in place by JS Bank, here are some tips on keeping your information secure.

- Never give out any personal information including user names, passwords, CNIC, mother's maiden name, credit or debit card numbers, ATM or Financial PINs.
- Never write down or record your PIN, passwords or other security information on cards or at a place easily accessible by others.
- Create difficult passwords which include letters, numbers and special characters.
- Avoid using public computers to access Internet Banking.
- Timely inform the mobile phone service provider to block the SIM card or terminate the mobile phone number in case of loss or theft of the mobile phone to avoid any misuse of Mobile Banking Service by any unauthorized person.
- Lock the mobile phone prior to leaving it unattended, to avoid any unauthorized access of mobile app or any breach of confidential data/information sent to the mobile phone.
- Do not give any of your personal, financial or payment cards related information to any web sites that do not use encryption or other secure methods to protect it.
- Avoid clicking suspicious or non-secure web links in e-mails and sms, especially any requesting private information.
- Do not reply to the emails from unauthenticated source nor download attachments.

We advise you to be alert and vigilant in dealing with such messages or emails. Please report many suspicious emails, websites and SMS messages to JS Bank by calling at 0800-011-22. We assure you of our commitment to keeping your financial relationship absolutely secure, and are constantly working towards upgrading our security parameters.