Awareness
On
Cyber Security
For
Online Banking

ফার্স্ট সিকিউরিটি ইসলামী ব্যাংক লিঃ
فارست سيكيوريتى اسلامى بنك ليميتد FIRST SECURITY ISLAMI BANK LTD.

সবার জন্যে সবসময়

ONLINE BANKING

The banking industry is one of the industries that have adopted internet technologies for their business operations. The aim was to provide online banking customers the facilities to access and manage their bank accounts easily and globally. Online banking, also known as internet banking, e-banking or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking which was the traditional way customers accessed banking services.

Online banking has been deployed more frequently to support and improve the operational and managerial performance within the banking industry.

THREATS TO ONLINE BANKING -

There are some information security threats and risks associated with the use of online banking systems. The confidentiality, privacy and security of internet banking transactions and personal information are the major concerns for both the banking industry and internet banking. Attacks on online banking today are based on deceiving the user to steal login data. Phishing, pharming, Cross-site scripting, adware, key loggers, malware, spyware, Trojans and viruses are currently the most common online banking security threats and risks.

THE FOLLOWING ARE THE MAJOR ATTACK SCENARIOS:

1. A credential stealing attack (CSA), is where fraudsters try to gather user's credentials, either with the use of a malicious software or through phishing.

2. A channel breaking attack (CBA), involves intercepting the communication between the client side and the banking server, by masquerading as the server to the client and vice versa.

3. A content manipulation also called man-in-the browser (MiTB) attack, it takes place in the application layer between the user and the browser. The adversary is granted with privileges to read, write, change and delete browser's data whilst the user is unaware about it.

SECURITY AWARENESS -

First Security Islami Bank Ltd. is committed to keeping your personal online information secure and confidential. We understand the importance of securing your financial records both in the branch and through our online banking system. To help preserve your personal information you must also take an active role. Here is some information about security tips and guidelines:

- Protecting Your Computer & Data
- Phishing Awareness

- Password and PIN Guidance
- Important Information

PROTECTING YOUR COMPUTER & DATA :

The Internet is a great place to browse and do business, however it can also be a dangerous place for identity theft if you don't know what to watch for or how to protect yourself. There are several types of malware – which means malicious software – that can infect your computer as you surf the web including:

- Viruses
- Spyware/Adware
- Trojan Horses
- Keystroke Loggers
- Ransom ware

These programs are becoming more sophisticated and ingenious in their ability to infect your computer. Many are designed to steal your personal and/or business information. While "surfing" the Internet, follow these steps to protect your computer from the majority of Internet crime:

INSTALL AND UPDATE ANTI-VIRUS SOFTWARE - Virus protection software is critical to keeping your personal computer and your internet banking safe. Install and regularly update anti-spyware, anti-virus, and firewall protection on your computer. Scan your computer at least weekly for all types of virus including those that could be used to capture keystrokes.

REGULARLY INSTALL UPDATES AND PATCHES - Make sure your computer operating system and web browser software are always updated with the latest updates and security patches. Checking for and downloading new versions/security enhancements from the vendor's authentic web site. This ensures that you close the gaps in the system that viruses or other malware could exploit.

BE CAUTIOUS WITH DOWNLOADS - Do not download software from unknown or un-trusted websites unless you are sure it is safe. Downloads can be infected with spyware/adware attached to the file.

WATCH FOR SIGNS OF SPYWARE - frequent pop-up ads, unexpected icons on your desktop, random error messages or sluggish computer performance are all signs of infection. The pop-up ads (adware) sometimes appear to offer free credit reports or credit scores as part of the scam. First Security Islami Bank does not offer credit scores or credit reports. Run a full system anti - virus and anti-spyware scan to identify and safely remove spyware.

BE CAREFUL when using public computers to perform any type of personal transactions. Just logging into a Website may give away passwords and other private information if spyware has been installed on that computer.

Be cautious of email attachments and URL links - Do not open email attachments received from unknown sources. Never login to your bank website through a URL link in an email, even if the email appears to have come from your bank. Type the web address into your browser yourself.

Lookout for the secure padlock - The login pages of our website are secured through an encryption process, so a locked padlock or unbroken key symbol should appear in your browser window when accessing our login pages.

Regularly clear your cache, cookies and browsing history - Consider erasing/deleting your browser's cache and your browsing history after each session, or on a periodic basis, so that any account information and browsing history are removed.

Log out - When your online banking is complete, log out before closing the browser or going to the next website. Always log out and close the browser every time you leave your computer. Never leave your PC unattended when logged into Online Banking.

PHISHING AWARENESS -

What is Phishing?

"Phishing" is a scam used by cyber criminals who imitate legitimate banking/financial organizations through emails. Cyber criminals use this technique to obtain personal information including login information such as usernames, passwords and PINs. Victims are persuaded to provide these details either by logging on to fraudulent websites or – less frequently – by phone or fax.

How Do You Recognize a Phishing Email?

Awkward greeting - A phishing email may address the customer with a generic greeting ("Dear valued customer" or something similar) rather than by name.

Spelling and bad grammar - Cybercriminals are not renowned for correct grammar and spelling. If you notice spelling and grammatical mistakes in an email, it is most likely a phishing email.

"Click on this link" - If you see a link in a suspicious email message, don't click on it. The link looks official, but when your mouse cursor rolls over it the link's source code points to a completely different website. Remember that you can always type a URL into your web browser instead of clicking on a link. Similarly, never use a phone or fax number contained within an email without first checking its authenticity using our website.

URGENT CALL TO ACT - Different approaches include things such as "We're updating our records", "We've identified fraudulent activity on your account", or "Valuable account and personal information was lost due to a computer glitch". To encourage people to act immediately, the email usually threatens that the account could be closed or cancelled.

PASSWORD AND PIN GUIDANCE -

You are responsible for maintaining two of your most important security measures: your password and PIN.

CREATE A UNIQUE PASSWORD AND PIN EVERY TIME - Stay away from anything easy to guess and anything connected to your life. Avoid using birthdates, birth years, family members' or pets' names, information related to your school or college or favorite team, account numbers, or other easily obtained information.

FOLLOW THE "8 4 RULE"- Stick with passwords that are at least eight characters in length. The more character in the passwords the better. At least one character in your passwords should be each of the following.

- Lower case letters
- Upper case letters
- Numbers
- Special characters

USE DIFFERENT PASSWORDS AND PINS - That way, if someone does get access to one of your web or bank accounts, he or she cannot access the rest of them.

CHANGE YOUR PASSWORDS AND PINS ON A REGULAR BASIS - Schedule a recurring appointment on your calendar to change your passwords once every six months.

DON'T TYPE YOUR PASSWORD OR PIN ON A COMPUTER THAT DOES NOT BELONG TO YOU - If possible, don't use someone else's computer that you don't trust to login to any website, especially for very sensitive purposes such as banking.

KEEP YOUR PASSWORDS AND PINS A SECRET - Do not carry your passwords in your purse or wallet and if you write them down, keep them somewhere safe, and not near your computer. Make sure no one watches you enter your password.

DON'T SHARE WITH ANYONE - Anyone includes your friends and family.

PROMPT REPORTING OF SUSPICIOUS ACTIVITY –Contact your bank immediately, if you think someone knows your security access code or in case of theft of your code/money or in case you have forgotten your credentials. Your prompt action is crucial to prevent any (further) damage.

IMPORTANT INFORMATION -

Be wary of anyone asking you to disclose personal details, passwords or PINs. Remember:

- First Security Islami Bank staff will never ask for your password, PIN, other personal access credentials or any other personal or financial information except to verify your identity when you have asked us to do something.

- The First Security Islami Bank website will not ask you to enter any of your security details except on web pages that can be accessed directly from the home page of our website.

STAY ALERT :

- Sign-on to Online Banking regularly and review your account transactions, checking for any fraudulent activity on your account (e.g. transactions you do not recognize).

- Keep track of your last log-on date and time, displayed.

- Once logged into Online Banking, you can also monitor the actions performed online

TELEPHONE RISK -

The telephone is one of the most often used sources for criminal activity. Here's how it works. Your phone rings. The caller claims to be from your financial institution, or any other source. They begin asking questions about you and your bank account information. Other telephone scams claim that you've won a sweepstake and ask for personal information in order to claim the "prize". These are attempts to obtain account information and/or steal your identity, and it happens to millions of peoples every year. Protect yourself from telephone scams by following these steps:

- Never offer personal or business related information over the phone without verifying the caller's identity.

- If you are uncertain of the identity of a caller, hang up and initiate the call yourself using a known phone number.

- Do not call any phone number received in a voice message or e-mail asking for personal information. It could lead you to a phony answering system.

As a general guideline, be highly suspicious anytime you are requested to provide personal information over the phone.

BE AWARE, BE SAFE