Online Banking Safety, Awareness and Protection

NRB Bank Limited, IT & ADC Operations.

Today Online Banking important ingredient of business process all over the world and especially in Bangladesh. All are commercial, Government, specialization bank are involving to transaction through online banking and E-commerce's other services & recently banks are introducing new and flexibility transaction service through online to more attachment with service and interact with banks. Intruder or hacker has taken advantage of the growing scope, they using sophisticate method like malware, Phishing, key-logger and other application and network layer exploitation to gaining unauthorized access and processing the unauthorized transactions.

NRB Bank took several security measure to secure transaction and it will be more effective when customer aware and follow the below instruction.

1. Never ever share user ID, Password or other online banking credential on an unsolicited basis & avoid to provide transaction information, credentials to other trusted or untrusted sources.

2. Online banking transaction, System upgrades, security awareness material or the availability Periodic or system change message will be notified customer through email, messaging or other sources.

3. To accessing online banking sties from public computer must be prohibited. Sometime key logger as install on public computer it can be stolen credential.

4. Use a complex password, of at least eight character composed of a combination of upper/lowercase letters, numbers, and special characters and do not include the username to avoid easily guessed passwords. You are encouraged to periodically change your password.

5. Do not open any suspicious e-mail and attachment.

Workstation Controls:

1. Enable Operating system firewall and protect your computer with well-known anti-virus/spyware software. Update the virus definitions and scan your workstation regularly.

2. Install prominent anti-malware, anti-phishing solution

3. On the regularly basis, workstations security Patch should be Up-To-Date. Many viruses rely on systems without current patches or security to spread. Configure your workstation to update the operating system automatically if possible with current service packs etc.

4. Consideration of using a stand-alone, dedicated computer for only financial transactions with no web browsing, e- mail, or social media allowed.

At NRB, We are committed to protecting your information, however it is critical that you also be aware of the risks present, implement various controls to minimize the risks, and actively monitor your accounts for any potential fraud. If you ever feel your online profile, accounts or identify has been compromised or you receive an unsolicited request for any information, please contact us immediately at 09666456000.

We appreciate your business and want to work closely with you to protect what is yours!