# HOW TO CONDUCT SAFE TRANSACTIONS
## ON EMI DIGIBANK AND EMI DIGBIZ

## 07 SEVEN PRINCIPLES TO ENSURE SAFETY

To ensure safety when conducting online transactions through digital banking, please adhere to the following principles:

01 **Never disclose your personal identification information** (Username, Password, and One-Time Password – OTP) to anyone else. Do not write your password on paper or record/store it in any form.

02 **Never download or use applications from unknown sources** (only use applications that have been clearly verified on the App Store and Google Play Store).

03 When using services on websites, **only access services through th official website of** EMIMFI (Absolutely do not log into services throug links embedded in SMS messages, emails, Zalo, Viber, etc.).

04 **Only log in through trustworthy devices.** Do not use mob devices that have been jailbroken or had their operating syster tampered with (rooted, jailbreak, etc.) to access services.

05 **Avoid using basic personal information** (birthdate, phon number, name, etc.) **as your password**. It is advisable to change yo password at least once every three months or whenever it has be disclosed or suspected of being disclosed.

06 If you receive notifications from the Bank about an OTP, unusu balance changes, activation of an application on a differe device, linking to an electronic wallet, etc., without havi performed any transactions on digital banking, **never provide th OTP** and immediately notify the Bank.

07 Always remain calm and alert when receiving requests f information or money transfers. **Verify and authentica information through official channels** (e.g., the official helpline the requesting party) and check the credibility of website links on the Network Trust Portal of the Ministry of Informati and Communications (tinnhiemmang.vn).

## WARNING ABOUT ONLINE FRAUD SCHEMES

Fraudsters use sophisticated tactics to persuade customers to follow instructions designed to steal bank service information, thereby gaining access to the services and appropriating money from accounts or requesting customers to transfer money themselves.

Some common tactics include:

- **Impersonating authorities** *(police, courts, tax agencies, etc.)* **by sending links/websites of fake public services for customers to install counterfeit apps** *((like VNeID, apps from the General Department of Taxation, etc.)*, which then take control of the device and covertly steal banking service security information to conduct unauthorized money transfers from the customer's account.

- **Impersonating authorities** *(courts, police, etc.)* **and threatening customers with alleged illegal activities** *(traffic accidents, money laundering involvement, smuggling, international telecom dues, etc.)* and instructing them to follow certain steps (open a new account, provide information, install applications, transfer money to specified accounts, etc.).

- **Faking a bank's website/Fanpage/SMS messages** and sending counterfeit links for customers to enter their information.

- **Impersonating bank staff to contact customers offering support** *(fixing transaction errors, handling trace requests, etc.)* then requesting customers to provide secure information to facilitate the appropriation of assets.

- **Sending mail with content designed to earn the customer's trust** *(notification of winning a prize, offering promotional codes, etc.) along with instructions that guide customers to provide their banking service's secure information.*

- **Stealing login information on social media platforms** (Facebook, Zalo, etc.) of friends and relatives of the customer, then contacting the customer to request money transfers for support or loans.

**Please be advised**

EMIMFI does not send any digital banking service login links to customers in any form, **and all login links sent to customers are fraudulent.**

EMIMFI does not contact customers requesting secure in-formation in any form, **and any requests for secure service information are fraudulent.**

Customers are advised to be vigilant about requests received through online channels and social media platforms. Additionally, please report to the nearest police or relevant authorities if you suspect any fraudulent activities.

## IN CASE OF AN EMERGENCY

If you suspect or detect signs of being scammed or hacked, please prioritize the following actions:

1. **LOCK THE SERVICE OR CHANGE THE SERVICE PASSWORD IMMEDIATELY:**
   - **For** EMIMFI **Digibank:** Send a message with the format EMIMFI **KHOA DIGIBANK** to **6167**
   - **For** EMIMFI **DigiBiz:** Change the login password by going to the **Utilities section and selecting Change Password.**
2. **IMMEDIATELY CALL THE BANK**
   Immediately call the bank on the 24/7 hotline at 1900545413, or visit a bank branch for assistance (during business hours).
3. **PERFORM A FACTORY RESET**
   If a fake application installation is detected or suspected
4. **REPORT THE INCIDENT TO THE NEAREST POLICE STATION.**