Account Security Guide

ATME provides its clients with an online platform (**Platform**) to enable trading and self custody of digital tokens. As part of our security commitment to our clients, we incorporate access control and verification measures such as login credentials, multi-factor authentication, and wallet keys (**Security Measures**) when accessing your ATME Client Account or availing the relevant ATME service. These Security Measures are enabled by us for you and as part of our security commitment we do not maintain access to your Security Measures.

You play an active role in the security of your Client Account. It is important that you maintain your Security Measures against loss or compromise by third parties. In particular, please be aware:

- that internet use might expose you to risks such as viruses, third-party scams, and communication failures.
- that private keys are required to access the digital tokens you hold in your wallets and your diligent management of private keys is central to the security of your digital tokens.

This guide is designed to provide an overview of the top practices to enhance the safety of your Client Account. Please read and implement this guide carefully.

Your ATME Client Account

When setting up your Security Measures or accessing ATME's Platform or services you should do the following:

- Employ unique Security Measures not replicated on other services.
- Restrict access to your Security Measures and ensure no third party can surveil your screen or record your Security Measures.
- Avoid accessing ATME services from public internet points.
- Store your Security Measures confidentially and refrain from documenting them on any software or using browser "save password" functions.
- Maintain the security of devices used to access the Services/Platform such as the use of trusted anti-virus and malware prevention software.
- Exercise caution with communications claiming to originate from banks or ATME, particularly those requesting personal security details—ATME will never solicit your Security Measures.
- Adhere to any instructions from ATME concerning Platform operations, Security Measures, and associated security protocols.
- In the event of an investigation into the misuse of security details or Security Measures, provide full cooperation and assist with information on request from us or law enforcement.
- In the event you suspect your Client Account is compromised, please notify ATME immediately at support@atme.com.

Your Wallets

- **Secure Backups:**
    - Create and store multiple backups of your private keys in separate, secure locations to mitigate the consequences of losing access to your primary copy.
    - Safeguard your mnemonic phrase, which serves as a backup to restore your wallet, in a protected environment.
- **Theft Prevention:**
    - Utilize a hardware wallet for storing private keys offline, significantly reducing the risk of online theft.
    - Manage private keys in a secure setting to avoid physical theft or surveillance.
    - Defend your devices with state-of-the-art anti-malware software to negate digital threats.
- **Unauthorized Access Control:**
    - Establish complex and distinct passwords for different services to hinder unauthorized access.
    - Activate Multi-Factor Authentication (MFA) as an added security layer.
- **Phishing Scam Vigilance:**
    - Stay alert against phishing schemes. Never reveal your private keys and exercise caution with dubious links or communications.
- **Inheritance and Succession Planning:**
    - Arrange a digital token inheritance strategy to assure your assets and private keys are bequeathed as per your preferences.
- **Device Security:**
    - Engage in transactions only on trusted and malware-free devices.
- **Backup Strategies:**
    - Diversify your backup solutions, encompassing both digital backups on encrypted mediums and physical backups in fortified locations.
    - Test your backups systematically to confirm their reliability.
- **Environmental Safeguards for Backups:**
    - Store physical backups, such as paper or steel wallets, in conditions resistant to fire and water.
    - Consider safe deposit boxes or other secure settings for off-site backup storage.
- **Adaptability to Technological Shifts:**
    - Be prepared to transition your assets onto novel technologies to secure against evolving threats.
- **Password Strength Regulations:**

    - Employ a password manager to create and retain robust, unique passwords.
- **Regulatory Compliance Awareness:**
    - Stay informed about legal standards for the protection of private keys, particularly in business asset management.
- **Seed Phrase Secrecy:**
    - Treat your seed phrase with the same confidentiality as your private key. Never disclose it.
- **Transaction Coercion Mitigation:**
    - Familiarize yourself with mechanisms, such as duress passwords, to safeguard against forced transactions.

Recovery Protocols for Lost Private Keys: If you lose your private key, follow these steps to attempt recovery

- **Check Your Backups**: Immediately refer to your various backup systems, reviewing any physical documents, such as paper printed copies of your private keys, recovery phrases, or other critical information , as well as any digital formats on secured drives or cloud storage.
- **Use Your Recovery Phrase**: If you've prepared a mnemonic recovery phrase, apply it to restore access to your wallet and assets.
- **Consult with Your Account Manager**: Contact your account manager for guidance in the recovery process. They can help explore every potential method to regenerate your keys.

By adhering to these practices, you can substantially diminish the risks and enhance the safety and security of your digital tokens. In case of uncertainties or if you require additional support, don't hesitate to get in touch with your account manager or our customer support team at support@atme.com. We are here to assist you in managing your digital tokens securely and confidently.