ePAPER

APCI FEDERAL CREDIT UNION

APCI eBanking Security

Digital Banking Security

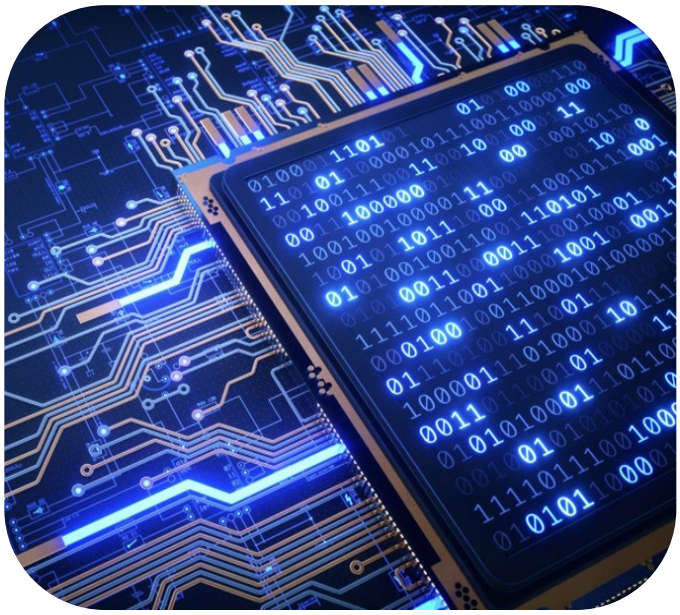
We Work to Keep Your Accounts Safe

ThreatMetrix Digital DNA is the force behind APCI eBanking that uses enhanced precision to identify and block Fraudsters. It also provides genuine APCI eBanking users with a more straightforward, faster, and secure login experience.

ThreatMetrix Malware Protection helps in minimizing risk and safeguarding our systems against a variety of hacking attempts which include:

- **Man-In-The-Browser:** A cybersecurity attack where a Trojan horse is installed that is capable of modifying a user's web transactions.
- **Remote Access Trojan:** A malware program that includes a back door for administrative control over the target computer.
- **High velocity/frequency bot attacks:** A bot attack is the use of automated web requests to manipulate, defraud, or disrupt a website, application, or end-user.
- **Low-and-slow attacks:** The mimicking of legitimate customer behavior to gain access to systems.
- **Ransomware:** Malicious software is designed to block access to a computer system until a sum of money is paid.
- **Key logging attempts:** The action of recording the keys struck on a keyboard, typically covertly. Data can then be retrieved by the person operating the logging program. A keystroke recorder or keylogger can be either software or hardware.

Intelligence from ThreatMetrix's Digital Identity Network is utilized to transform the way members use online banking. This is done by ensuring information stays confidential and secure, but with added simplicity when logging in to accounts.



Extra Steps Towards Safety

ThreatMetrix uses a combination of Device Fingerprinting, True Location Detection and Device Tampering Detection to ensure a trusted device is accessing the system. If ThreatMetrix cannot verify the device's worthiness, additional authentication will be requested.

Both authentication and authorization are supported by technology that deters unauthorized events.

Authentication provides verification of credentials, such as username, password, biometrics and other multi-factor authentication methods. **Authorization** supports access to specific resources within the APCI eBanking platform.

Member registration, login, and access are securely managed by the up-to-date and latest security that is integrated within the system.

Technology Today

Multi-Factor Authentication

Step-up authentication, also known as Two-Factor or Multi-Factor authentication, is in the form of a six-digit PIN.

Our system gives the user the opportunity to choose a method of two-factor authentication that meets their needs. The options are:

- SMS (text)
- Email
- Voice calls
- Push Notifications

Some reasons multi-factor authentication may be required are:

- Logging in from an unknown device
- Logging in via a VPN or from a different IP address
- Clearing cookies/cache on your device

Biometrics

APCI eBanking login supports the use of biometrics. This includes fingerprints, facial recognition, and saved devices. The use of biometrics eliminates the need to enter passwords repeatedly.

During every login, before members are provided access to APCI eBanking, the device being used, and the credentials are verified. Devices used to log into APCI eBanking are stored in the system, which is then utilized at future logins to access risk.

The risk score of a member is assessed at the login. If actions associated with higher risk are completed during the session, their risk score will increase.

Added Security in Registration

When registering to use APCI eBanking, members will be asked for specific information that matches their data on record. This includes:

- Providing their account details
- Confirming their identity
- Performing stepped up authentication
- Selecting their username and password

Password Safety

Members are provided with a fully self-service password reset. If a password reset has been activated too many times the system will lock the account.

When members are having a hard time remembering their password, a lockout help prompt will be presented. This prompt is designed to deter members from locking themselves out of APCI eBanking by asking if the member would like to reset their password.