AI and Your Financial Accounts

Protect yourself and your accounts

What is AI?

AI, or artificial intelligence, involves the simulation of human intelligence by machines, such as computer systems. AI systems perform tasks that usually require human intelligence, such as understanding languages, identifying patterns, solving problems, and making decisions.

AI is transforming industries by allowing machines to learn from data, adapt to new information, and perform complex tasks without human interaction.

Key areas in AI programming focus on cognitive skills, such as:

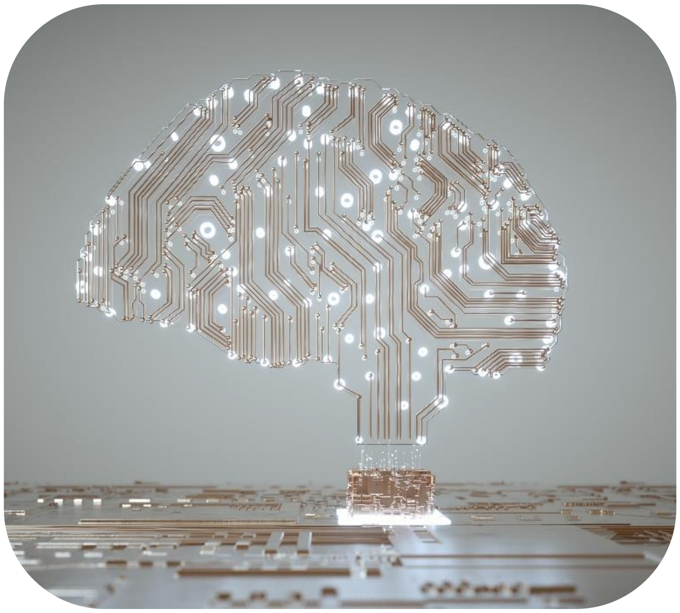
- **Learning:** This aspect of AI programming involves acquiring data and creating algorithms to convert into actionable information. Step-by-step instructions for specific tasks can be provided from the algorithms.
- **Reasoning:** This aspect focuses on selecting the best algorithm to achieve a desired result.
- **Self-correction:** This aspect allows algorithms to refine themselves continuously for best results.
- **Creativity:** This aspect uses neural networks, statistical methods and other AI techniques to generate new images, text, music, and ideas.

Everyday Examples of AI

AI is already integrated into your everyday life. Below are a few examples of how AI enhances user experience and provides seamless, personalized interactions.

Unlocking your phone with face ID: Machine learning algorithms compare your facial scan to stored data, confirming your identity to unlock your device.

Social media: AI uses your activity history to curate your personal feed and make friend suggestions.



Search engines (Google, Bing, etc.): AI powers search engines by scanning the internet and delivering relevant information. Targeted ads that follow your search history are driven by AI.

Digital voice assistants: Siri, Alexa, Google Home and Cortana rely on AI-driven natural language processing to understand and answer questions.

Chatbots: Businesses use automated assistants for calls or chats to answer frequently asked questions, guide you through their website, or place you in a queue to speak with a representative.

Financial Benefits With AI

AI can help you create a budget.

Start by tracking your income and expenses, then set your savings goal and get an idea of what you would like to save for. You can input the numbers you calculated into an AI-powered budgeting tool and ask how to achieve your savings goals based on your income and expenses. AI will analyze your spending habits and provide feedback on how to meet your financial goals.

It is important to remember that AI accuracy depends on the quality of the data it is fed, whether that data is from the user or an external source. There is a chance that the information you are presented is inaccurate. Only use AI as a tool to get your budgeting started.

AI can help you save money.

AI-driven tools can analyze your spending habits and suggest cost-saving strategies. Examples include:

- Suggesting subscriptions to cancel.
- Providing tips to reduce utility bills.
- Finding better deals on recurring charges.
- Comparison shopping to locate the best prices or sales.

AI can help with tax preparation.

AI-powered tax preparation tools go beyond data entry. These apps help taxpayers to organize their documents, calculate deductions, and create accurate tax returns.

Many AI-powered tax apps also offer AI-powered virtual assistants to help with any questions that may arise.

AI Generated Scams

While AI offers many benefits and is used for a multitude of purposes, it has expanded the methods available for fraudsters. AI can make it easier for malicious actors to carry out complex fraud schemes and deceive individuals.

The best way to keep yourself protected against fraudsters is to be one step ahead. Stay informed and always be cautious when sharing personal information. Below are a few common AI-driven scams.

Synthetic Identity Fraud

Fraudsters use AI to create synthetic identities by blending real and fabricated information. This often involves using legitimate information from stolen sources, such as Social Security numbers.
The legitimate information is combined with invented information such as made-up names, addresses, or birth dates.

The AI algorithms can create highly convincing synthetic identities that often pass traditional verification checks.

These identities are then used to open bank accounts, apply for credit, or make fraudulent transactions and purchases. This can lead to account takeovers and significant financial losses.

Deepfakes

Deepfakes use AI and machine learning techniques to manipulate or fabricate realistic visual and audio content. This technology can create lifelike videos or audio of individuals doing or saying things they never did. This can lead to potential identity theft and deception.

In the financial sector, fraudsters may use deepfakes to impersonate executives or other key personnel to attempt to authorize fraudulent or unauthorized transactions in online accounts.

Similar to synthetic identities, a fraudster can create a deepfake of a member and use it to open an account. This can lead to an account being taken over without the real owner even realizing that it is happening.

Automated Hacking

AI can automate the process of discovering and exploiting vulnerabilities in software and hardware systems. This includes techniques that identify weak passwords, execute brute force attacks, or scan for unpatched software vulnerabilities that can be exploited.

AI can also facilitate the creation and distribution of malware, making infections more efficient and harder to detect. For instance, AI-driven polymorphic malware can alter its code to evade signature-based detection systems.

Social Engineering

AI enables sophisticated social engineering by analyzing data from social media, the dark web, online activities, data science, and even personal communications. This information is used to craft highly personalized phishing emails that are tailored to an individual’s interests, activities, and writing style. These factors increase the likelihood that the individual will engage with the email.

How To Protect Yourself

Be mindful of personal information: Only share sensitive details with trusted platforms that clearly explain how they handle personal data.

Understand privacy settings: Review and adjust privacy settings on AI platforms that match your comfort level and control what information is shared.

Don't overshare: Limit the amount of personal information that is publicly accessible.

Think critically: AI systems are not flawless and can make mistakes. Verify facts, cross-reference information, and consider different viewpoints before making decisions based solely on AI-generated output.

Report inappropriate content: If you encounter offensive or harmful content or inappropriate interactions, report it to the platform or service provider.

Be cautious with AI-generated messages: Avoid sharing personal information in unexpected or suspicious messages from AI-powered accounts or chatbots. Stop or leave the conversation if it is uncomfortable.

Stay informed: Keep up with AI advancements to better understand its capabilities, limitations and potential risks. This knowledge can help you to make well-informed choices and use AI responsibly.

Tools That Protect Your APCI FCU Accounts

ThreatMetrix® Digital DNA

When you log in to APCI eBanking, ThreatMetrix® Digital DNA is working behind the scenes to help identify and block fraudsters with high accuracy.

ThreatMetrix combines real-time data sources with industry-leading, AI-driven models to analyze complex fraud patterns and correlations, delivering precise risk decisions instantly.

Step-Up Multi-Factor Authentication (MFA)

If your login cannot be verified as coming from a trusted device, you will be prompted for additional authentication.

This authentication will be in the form of a PIN number sent via text (SMS), email, voice call, or push notification based on the preferences you selected.

You also have the option to require MFA at every login.

APCI eAlert Security Alert

You will receive alerts if any suspicious activity occurs on your account.

Security Alerts cannot be completely disabled, but you can choose how to receive them through your customizable APCI eAlerts settings.

Automated Fraud Alerts for Visa® Debit and Mastercard® Plus

If suspicious activity has been detected on your account, our automated system will contact you by text, phone, or email.

Member Identification Program

If you are calling our offices, identifying questions are asked prior to giving any personal account information, completing financial transactions, or making any modifications to an account.

For added security, you can request that a password be put on your account which is then required prior to releasing information, completing transactions, or making account modifications over the phone.