AI-Powered Scams: How Fraudsters Are Getting Smarter and How You Can Stay Safe

Scammers are always evolving, but recent advances in artificial intelligence (AI) have taken fraud to a new level. Today's cybercriminals are using AI tools to create more convincing scams that are harder than ever to detect, putting consumers and their finances at greater risk.

One of the biggest changes is how realistic scams have become. In the past, fraudulent emails or messages often contained spelling errors or awkward phrasing. Now, AI can generate polished, professional messages that closely mimic legitimate communications from credit unions, banks, and businesses. These messages may include accurate logos, formatting, and language designed to build trust and create urgency.

Even more concerning is the rise of voice cloning and deep-fake technology. Fraudsters can use AI to imitate the voice of a family member, coworker, or financial institution representative. Imagine receiving a phone call that sounds exactly like someone you trust, asking you to transfer money or share sensitive information. These scams are designed to bypass your instincts and make you act quickly without verifying the request.

AI is also helping criminals scale their efforts. Instead of targeting a few individuals, scammers can now generate thousands of personalized messages in seconds. They may use publicly available information, such as social media details to tailor attacks specifically to you, increasing the likelihood that you'll respond.

Despite these growing risks, there are simple steps you can take to protect yourself:

Pause and Think Before You Act
Scammers often create a sense of urgency, such as claiming your account is compromised or a payment is overdue. Take a moment to slow down and avoid making quick decisions based on fear.

Verify Before You Trust
If you receive a suspicious call, text, or email, contact the organization directly using a phone number or website you know is legitimate. Never rely on contact information provided in the message itself.

Be Cautious with Links and Attachments
Avoid clicking on links in unexpected messages, even if they appear to come from a trusted source. These may lead to fake websites designed to capture your login credentials.

Protect Your Personal Information
Never share passwords, PINs, or one-time verification codes. All One Credit Union will not ask for this information through unsolicited messages or phone calls.

Use Available Security Tools
Enable multi-factor authentication (MFA) on your accounts whenever possible. This adds an extra layer of protection, even if your password is compromised. AI may be making scams more sophisticated, but awareness remains your strongest defense. By staying alert, verifying requests, and practicing safe online habits, you can significantly reduce your risk and help keep your financial information secure.

Getting Help

If you have identified suspicious activity involving All One Credit Union, contact us immediately at 800-649-4646.