Payments and Artificial Intelligence

Protecting yourself against AI-based scams

Payments Innovation Alliance®

Artificial Intelligence (AI) has transitioned from science fiction to everyday reality. While AI offers many ways to make life easier, read on to understand how to protect yourself and your loved ones, plus find helpful tips for recognizing and responding to financial scams.

Generative AI is a new technology that simplifies everyday personal and business tasks. However, there is a dark side: scammers use generative AI to refine their financial crimes. They use AI tools to help them correct spelling and language that appear legitimate or to imitate companies and loved ones quite convincingly. AI tools are readily available, making scammers' work easier than ever, even across geographic borders.

FOUR STEPS TO PROTECT YOURSELF BEFORE AN AI-BASED SCAM ATTEMPT

1. Increase security.

Take measures to safeguard your banking and social media accounts, including passwords and multi-factor authentication. A strong password is at least 12 characters long and uses a combination of uppercase and lowercase letters, numbers and symbols.

Enroll in real-time notifications and alerts at your financial institution for transactions above a specified limit and regularly monitor your accounts for suspicious activity.

Use a password for your financial account data that is significantly different from passwords you use for other sites.

Change passwords periodically.

2. Limit data sharing.

Restrict the information you post on social media and only share information with people you trust.

Fraudsters use publicly available information like names, addresses, birthdays and photos. Voice impersonations can be created using only a few seconds from videos or an outgoing voicemail message. Pictures from social media can be easily altered.

3. Establish a code word.

Make up a private word or phrase that you share with your trusted contacts that only you and they know. Avoid using something that can be easily guessed, such as a pet name.

If you receive a call from a family member or friend in trouble pressuring you to send money, ask for the code word to verify who you are talking to. Practicing using the code word is a good idea so you don't forget it.

4. Do research whenever possible.

Refer to online resources from your financial institution, the Better Business Bureau, the FBI, the Federal Trade Commission and other organizations to learn how to recognize scams.

WHAT TO DO IF IT HAPPENS TO YOU

Be prepared to recognize fraudsters sending emails, making phone calls, sending text messages or using social media. Trust your instincts, take precautions and react wisely.

Email

Warning Signs

AI can make email phishing attempts look very real. Misspellings and poor grammar are giveaways, but AI is closing that gap.

Scammers may create a sense of urgency around fixing your security settings or changing or confirming account numbers.

Scammers may provide weblinks (aka URLs) that appear to be legitimate but are not. The imposter URL may have a subtle change (e.g., the letter "o" is changed to a zero, and the company domain may be changed from .com to .org).

What to Do

Use a separate email address or alias for only financial transactions.

Do not click on links within an email, even if you believe you recognize the sender.

Validate the company's official website link by looking it up yourself.

Delete the message and report it as junk.

Block the email address and/or the domain.

Don't opt out if you are asked to enter your email address.

Phone

Warning signs

Scammers can spoof phone numbers that appear to be legitimate. They may pose as your financial institution to discuss unusual activity or a company that wants you to fix your settings. They may also pose as law enforcement or a government agency.

Scammers may use synthetic images or voices – also known as deepfakes – purporting to be a loved one.

Scammers will generally pressure you to send money within a specific deadline.

What to Do

Avoid answering calls from unknown numbers. If you choose to answer, ask the caller for the number to call them back.

Validate the phone number by looking it up on the company website.

Ask the caller to provide the pre-arranged code word. It is likely a scam if the caller cannot offer the correct word.

Request the caller to turn on the video camera so you can see your loved one.

Contact your family member or friend directly to confirm they are safe. Do not provide any personal information.

Stay calm. Do not panic or feel pressed to react quickly.

Do not send money or provide any personal information.

Hang up and block the number.

Text Messages

Warning signs

Scammers may impersonate companies to collect overdue bills or start a personal conversation. Watch for messages such as:

- Your bill is overdue. Click on link to make a payment.
- Hey, I left something in your car!
- Are we still on for golf?
- I changed/lost my phone and want to add you to my contact list.

What to Do

Avoid responding to texts from unknown numbers.

Do not click on a link in a text message.

Do not click on a link from an unsolicited text message.

Delete the message, report it as junk and block the number.

Forward the scam text to 7726. The major carriers use your information to report and block similar messages.

Social Media

Warning signs

Scammers may comment on your social media post, reply to a comment you made on someone else's post or message you directly.

Scammers may:

- Send a message that your social media account has been flagged and needs to be re-verified by clicking on a link to download a form.
- Ask for a favor.
- Ask you to send money.
- Make a too-good-to-be-true job offer.

What to Do

Only connect and respond to people you know. Block unknown profiles. Hide the comment so others cannot see it.

Never give a stranger your login credentials or other personal information without verifying it is legitimate.

Do not send or receive money unless you have validated that the person contacting you is legitimate.

Do not click on a link purporting to be the company. Go directly to the company's social media site outside of the message.

Research firms before responding to job offers. Your resume should include your email address but not your address or phone number.

ADDITIONAL RESOURCES

Better Business Bureau Scam Tips
Did You Know: There are Two General Categories for Defining Artificial Intelligence
Someone Sending You Money? You Could Be a Money Mule
Highway to Easy Money? Think Again! [video]

REPORT YOUR EXPERIENCE

If you believe you are a victim of a scam, reporting what you see and experience helps law enforcement take action and protect others from becoming victims.

BBB Scam Tracker
Federal Trade Commission (FTC)
FBI
Internet Crime Complaint Center (IC3)
Report scam text messages by forwarding to 7726

If you paid or sent money, contact your financial institution, credit card provider, money transmitter or other organizations involved in the transaction and file a police report.

This document was developed by the Cybersecurity & Payments AI Project Team of Nacha's Payments Innovation Alliance. The Payments Innovation Alliance is a membership program that shapes the future of the payments industry and develops thought leadership relevant to financial service institutions. The Alliance established the Cybersecurity & Payments AI Project Team to help organizations understand and respond to evolving threats related to potential cyberattacks. Visit the Cybersecurity & Payments AI Project Team page to see more resources developed by the team.

Payments Innovation Alliance®

Nacha®