

Understand & Report Phishing / Email Scams

NACHA does not send communications of any type to persons or organizations about individual ACH transactions that they originate or receive. If you or your customer has received a communication of this nature that purports to come from NACHA regarding a payment transaction, it is fraudulent.

What to Do?

Do not open suspicious emails or emails from unknown parties. Never respond to or click on any links, attachments, photos, graphics, etc., in an email that you receive from an unknown sender or that is suspicious. If you receive a suspicious email that claims to be from NACHA regarding a payment transaction, forward the email to abuse@nacha.org and delete it from your system.

If malicious code is detected or suspected on a computer, consult with a computer security or anti-virus specialist to remove malicious code or re-install a clean image of the computer system. Always use anti-virus, anti-malware, anti-spamming security software on your system and ensure that all available security patches are installed and remain current.

What is phishing?

Phishing or fraudulent emails may contain links to phony websites or request you to share personal or financial information by using clever or compelling language, such as an urgent need to update your information, decline a payment or communicate with you to ensure the security of your accounts.

Where can I learn more about phishing and other types of fraud and scam, and steps I can take to protect myself?

- [American Bankers Association](#)
- [Federal Deposit Insurance Corporation \(FDIC\)](#)
- [Internet Crime Complaint Center](#)
- [OnGuardOnline.gov](#)
- [USA.gov](#)