

Fraudulent Emails, Websites & Phishing Variations

Protect Yourself

1. Do not share any confidential information through suspicious emails, websites, social media networks, text messages or phone calls.
2. Protect your personal and account information, including your online banking username, password, and answers to security questions. Do not write this information down or share it with anyone.
3. Install, run, and keep anti-virus and anti-malware software updated.

Fraudulent Emails (Phishing)

Phishing is usually a two-part scam involving emails and spoof websites. Fraudsters, also known as phishers, send an email to a wide audience that appears to come from a reputable company. This is known as a phish email.

In the phishing email, there are links to spoof websites that imitate a reputable company's website. Fraudsters hope to convince victims to share their personal information by using clever and compelling language, such as an urgent need for you to update your information immediately or a need to communicate with you for your own safety or security. Once obtained, your personal information can be used to steal money or transfer stolen money into another account.

Use caution if you receive an email expressing an urgent need for you to update your information, activate your online banking account, or verify your identity by clicking on a link. These emails may be part of a phishing scam conducted by fraudsters to capture your confidential account information and commit fraud.

How Fraudsters Obtain Email Addresses

Fraudsters obtain email addresses from many places on the Internet. They also purchase email lists and sometimes guess email addresses. Fraudsters generally have no idea if people to whom they send banking-related phish emails are actual bank customers. Their hope is that a percentage of those phish emails will be received by actual bank customers.

If you receive a fraudulent email that appears to come from NACHA, this does not mean that NACHA has your email address, name, or any other information.

Fraudulent Websites (Phishing or Spoofing Websites)

Fraudsters may attempt to direct you to spoof websites via emails, pop-up windows or text messages. These websites are used to try to obtain your personal information. One way to detect a phony website is to consider how you got to the site. Use caution if you may have followed a link in a suspicious email, text message, online chat or other pop-up window requesting your personal or account information.

Pop-up Windows

Fraudsters may use pop-up windows – small windows or ads – to obtain personal information. These windows may be generated by programs hidden in free downloads such as screen savers or music-sharing software. To protect yourself from harmful pop-up windows, avoid downloading programs from unknown sources on the Internet and always run anti-virus software on your computer.

Telephone or Voice Phishing

Known as **vishing**, or voice phishing, this tactic is a phishing attempt made through a telephone call, fax or voice message. If you are uncomfortable continuing a phone call that was not initiated by you with someone who claims to be from NACHA, ask for a reference number and call NACHA, using legitimate sources of contact information.

Text-Message Phishing

A phishing attempt sent via SMS (Short Message Service) or text message to a mobile phone or device. This tactic is also referred to as **smishing**, which is a combination of SMS and phishing. The purpose of text message phishing is the same as traditional email phishing: convince recipients to share their sensitive or personal information.

Never disclose via text message any personal information, including account numbers, passwords, or any combination of sensitive information that could be used fraudulently. Use caution if you receive a text message expressing an urgent need for you to update your information, activate an account, or verify your identity by calling a phone number or submitting information on a web site. These messages may be part of a phishing scam conducted by fraudsters to capture your confidential account information and commit fraud.