

Learn to Recognize Fraudulent Emails

Fraudulent emails (phishing) and websites can be very sophisticated, and may look identical to NACHA emails and websites. Fraudsters can even tamper with the sender information in an email to make it appear even more legitimate. Although fraudsters use various tactics in their phishing attacks, there are common elements with which you should familiarize yourself.

SAMPLE PHISHING EMAIL

From: ach.01@nacha.org [REDACTED]

Subject: ACH Security Notification [REDACTED]



Dear Valued Client(s), [REDACTED]

We strongly believe that your account may have been compromised. Due to this, we cancelled the last ACH transactions [REDACTED]

-ID: 38350555 [REDACTED]

-ID: 38914735 [REDACTED]

Initiated from your bank account by you or another person who might have access to your account. Detailed report on initiated transactions are reason for cancellation can be found in attachment [REDACTED]

[Click here to download report](#) [REDACTED]

NACHA-The Electronic Payments Association
13450 Sunrise Valley Drive, Suite 100 Herndon, VA 20171
www.nacha.org
(703) 561-1100 [REDACTED]

1. **Authenticate Email Address:** Email addresses can be spoofed. Inherent in the email communications channel is a reliance on the recipient of an email to authenticate that the email is from the party that indicates it is from, i.e. an email sent by nacha.org from our association's publicly registered and authorized IP address and server. Some Internet Service Providers (ISPs) and spam filters have stronger authentication than others to validate that the email originated is from the authentic IP address and domain name server.
2. **Typos:** This isn't because fraudsters don't know how to spell, it's so phishing emails won't be blocked by email filters.
3. **Awkward Greeting:** A phishing email may not refer to the email recipient by name or in a nonsensical manner "Client(s)".

4. **Sense of Urgency:** An urgent need to communicate with you for your own security, or a request to verify payment information immediately; compelling language that urges the recipient to take action.

5. **Random Generation of Numbers:** A phishing email may contain a random sequence of numbers, such as ACH Payment #38350555 canceled, that can also be inserted into the subject line or text of the email to make it appear as though it is a specific transaction ID or payment amount. That random number can also be inserted into the file name of the pdf.exe file or pdf.zip file, creating a sense of uniqueness and legitimacy.

6. **Incorrect Grammar:** Another tactic used to bypass email filters. In this phishing example refer to, "Detailed report on initiated transactions are reason.."

7. **Strange or Unfamiliar Links:** The links may look official, but when the mouse cursor rolls over the link the link source code points to a completely different website which may contain malware as a pdf executable file or pdf zip. Never open attachments, click on links, or respond to emails from suspicious or unknown senders.

8. **Fraudulent Use of Legitimate Business Logo, Website, Address, Phone:** Fraudsters often insert actual identification references to a business into their phishing emails to make them appear legitimate.