

The Electronic Payments Association has received reports that individuals and/or companies continue to receive fraudulent emails that have the appearance of having been sent from NACHA. These emails vary in content and appear to be transmitted from email addresses associated with the NACHA domain (@nacha.org). Some bear the name of fictitious NACHA employees and/or departments. In the recent fraudulent e-mails, the subject lines have read as follow "ACH transaction cancelled," "ACH Transfer rejected," "Your ACH transaction," and other such variations.

NACHA itself does not process nor touch the ACH transactions that flow to and from organizations and financial institutions. NACHA does not send communications to persons or organizations about individual ACH transactions that they originate or receive.

Be aware that phishing emails frequently have attachments and/or links to Web pages that host malicious code and software (e.g. Zues Trojan). Do not open attachments or follow Web links in unsolicited emails from unknown parties or from parties with whom you do not normally communicate, or that appear to be known but are suspicious or otherwise unusual.

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 software and ensure that the virus signatures are automatically updated.

Ensure that the computer operating systems and common software application security patches are installed and current.