



Prevention TIPS

To: Members
From: Steve Wildes, Member Support & Service Manager
Date: January 13, 2012

Phishing Alert: Email Claims to be from Southeast Corporate

Southeast Corporate has received reports that individuals and/or companies have received a fraudulent e-mail that has the appearance of being sent from an e-mail address on our domain, Support@secorp.org. The e-mail claims that a requested wire transfer has been cancelled and includes a link to a website. The website is host to a malware application designed to exploit vulnerabilities in some versions of Java.

This is a FRAUDULENT e-mail. If you receive this e-mail, do not click on the link or the attachment. See sample below.

From: support@secorp.org [mailto:support@secorp.org]
Sent: Wednesday, January 11, 2012 11:52 PM
To: [e-mail address removed]
Subject: Re: Wire Transfer Confirmation (FED_04693P68712)

Dear Operator,
WIRE TRANSACTION: FED526524835449649
CURRENT STATUS: CANCELED

Please [Review your transaction](#) as soon as possible.

Be aware that phishing e-mails frequently have links to Web pages that host malicious code and software. Do not open attachments or follow Web links in unsolicited e-mails 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 specialist to remove the malicious code. Always use anti-virus software and ensure that the virus signatures are automatically updated. Ensure that the computer operating system receives security updates automatically and that security patches are installed and current on your software applications.

If you have questions please contact Steve Wildes, Member Support & Service Manager at 800-342-0203, ext. 6885.