

New Spam Poses as Failed Wire Transfer Message from the Federal Reserve

A new spam campaign is delivering hundreds of thousands of messages a day to consumers, warning recipients of allegedly failed wire transfers. When the recipient follows the links provided in the message to “learn more information,” the password-stealing Zeus Trojan is delivered instead.

Zeus targets users of online banking services to obtain banking credentials of small businesses and government agencies with higher account balances.

This spam uses actual graphics hosted by the Federal Reserve, including the notice of a failed wire transfer that appears to be legitimate. The messages also contain poorly-constructed sentences (as seen below).



If the recipient clicks the link that promises additional information, they are presented with a choice to run a double extension of .pdf.exe. This is not a PDF file; it is the Zeus Trojan. If it is installed, it will run quietly in the background, intercept browser traffic, and send any banking credentials it finds to its command and control server.

It is important to remember the following tips to minimize your chances of becoming a victim of spam:

- Do not trust unsolicited e-mails and never provide your password or any other confidential information in response to an e-mail;
- Treat e-mail attachments with caution, especially if they are coming from an unknown source;
- Do not click on links in e-mail messages if you do not know the source;
- Do not be intimidated by threats of negative consequences for not immediately providing requested information; and
- If you receive an unsolicited message regarding an issue with your bank or debit/credit card account, do not provide any sensitive account information (e.g., account numbers, Social Security numbers, PINs, etc.). Your bank will already have the information necessary to assist you.

If you have disclosed sensitive information in this or any other spam attempt, contact First Horizon/First Tennessee Online Financial Services at (888)382-6654 or PhishingAlerts@firsthorizon.com immediately.

You should also file a complaint or report suspicious activity to The Federal Trade Commission at www.consumer.gov/idtheft, or by calling 1-877-IDTHEFT.