



INTELLIGENCE BROADCAST

DATE: November 29, 2005

SUBJECT: New E-Scams & Warnings

IMPORTANCE: **Priority**

DETAILS: The Los Angeles Field Intelligence Group has received numerous reports of various internet based email scams. In an effort to warn the public of these on-going scams and prevent the possibility of falling victim to them, below are several of the email scams that the FBI has been made aware of. Included with the description of each scam is a portion of the text which may be included within the email.

FRAUDULENT FBI EMAIL ALERT

This scheme informs recipients that their Internet use has been monitored by the FBI and that they have accessed illegal websites. The emails then direct recipients to open an attachment and answer questions.

The email appears to be sent from the email addresses of mail@fbi.gov, post@fbi.gov and admin@fbi.gov. There may be other similarly styled addresses. The recipient is enticed to open the zip attachment which contains a variant of the w32/sober virus. If the program within the zip attachment is executed then the virus is launched and may affect the user's computer.

The text of the email is as follows:

Dear Sir/Madam,

We have logged your IP-address on more than 30 illegal Websites.

Important: Please answer our questions! The list of questions are attached.

*Yours faithfully,
Steven Allison
Federal Bureau of Investigation-FBI*

These emails did not come from the FBI. Recipients of this or similar solicitations should know that the FBI does not engage in the practice of sending unsolicited emails to the public in this manner.

Opening email attachments from an unknown sender is a risky and dangerous endeavor as such attachments frequently contain viruses that can infect the recipient's computer. The FBI strongly encourages computer users not to open such attachments. For detailed information on the effects of running this virus please log onto www.cert.org.

The FBI takes this matter seriously and is investigating. Users are instructed to delete the email without opening it.

Link: [Related Story](#)

NEW LEVEL OF SOPHISTICATION IN PHISHING SCAMS

A typical phishing scam involves three steps:

- The phisher deploys a website that mimics portions of a legitimate financial institution or other e-commerce website.
- The phisher crafts an email message that appears to be from the organization represented on the phishing website. The email message notifies the potential victim of a problem with their account and instructs them to login to the phishing site where the account information will be "verified."
- Utilizing spam, the phisher sends this email to hundreds of thousands of potential victims. If the victim falls for the scam, they end up divulging their account, credit card, and other identity theft related information. This information is then collected by the phisher and used to commit credit card fraud and other identity theft related offenses.

A new phishing technique adds another step to the process. It utilizes the login credentials entered by the victim to connect to the authentic website and downloads unique identifying victim information such as first and last name. This data is then used to populate portions of the phishing website. By doing so, the phishing site appears more legitimate; therefore, the victim is more likely to divulge sensitive information.

If you have received a fraud, or similar email, please file a complaint at www.ic3.gov.

FRAUDULENT FBI EMAIL ALERT

The FBI continues to see reports of email hoaxes similar to the [7/7/04 warning](#) posted on the [Internet Crime Complaint Center \(IC3\) website](#). The individual closing the internet transaction changes on the email; otherwise, the text of the email is identical to the email circulated in July 2004. The following is the message brought to our attention:

-----Original Message-----

From: IFCC [internetfraudcenter@usa.com]

Sent: Friday, September 16, 2006 6:10 PM

To:

Subject: Internet Fraud Complaint Center

Please note that this E-mail was generated by FBI and IFCC(Internet Fraud Complaint Center) E-mail services and any attempt to reply to this E-mail cannot and will not be answered or received by FBI or IFCC.

The Internet Fraud Complaint Center (IFCC) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). IFCC's mission is to address fraud committed over the Internet.

Our records show that you have closed an internet transaction with David Harrys. We are now able to inform you that this person is an internet scam artist. For almost 2 years he had ripped off over 100 internet buyers using Western Union for payment. We were not able to catch him until now because we don't have enough proves and details about him. Here is what we suggest:

Please pretend that you are interested in buying a product from him and accept any offer that he will make you. Follow all the instructions you receive from him regarding the payment procedure via Western Union wire transfer. We will watch this particular transaction and arrest him when he will try to pick up the funds at the Western Union office.

This way we will be able to stop his illegal activity and you will receive this amount you will have to send now and a \$10,000 bonus from FBI for your cooperation.

WE SUGGEST THAT YOU KEEP THIS E-MAIL SECRET FOR NOW. PLEASE DON'T ATTEMPT TO CONTACT FBI OR IFCC FOR THE MOMENT. WE WILL CONTACT YOU AS SOON AS YOU COPMLETE THE TRANSACTION WITH HIM. HE WILL TRY PICK UP THE MONEY AND WE WILL ARREST HIM AND CONTACT YOU AFTER THAT.

Regards, FBI team.

WARNING: DO NOT COOPERATE WITH SOMEBODY ELSE BESIDE FBI. OTHER COMMUNICATIONS MAY BE NEGATIVE TO OUR INVESTIGATION. EVEN THE COMMUNICATION WITH WESTERN UNION MAY BE DEADLY FOR OUR PLAN.

If you have received this, or a similar hoax, please file a complaint at www.ic3.gov

KATRINA DISASTER RELIEF FRAUD ALERTS

Email Disguised As American Red Cross Message Phishing For Credit Card Information

The FBI has become aware of a spam email soliciting \$5 donations that purports to be coming from support2@redcross.org, with the subject line of “American Redcross Help Needed! Katrina relief.” The email provides a link to click and enter credit/debit card information for the \$5 contribution. The link appears to go to the RedCross.org website. However, the link actually sends one to a non-affiliated collection site of <http://pro-solutions2.com/cgi-bin/register.pl>. **THIS EMAIL IS A HOAX. DO NOT FOLLOW THE PROVIDED LINK.** Be cautious when responding to requests or special offers delivered through unsolicited email:

- Guard your account information carefully.
- Keep a list of all you credit cards and account information along with the card issuer’s contact information. If your monthly statement looks suspicious or you lose your card(s) contact the issuer immediately.
- To ensure contributions to U.S. based non-profit organizations are received and used for intended purposes, go directly to recognized charities and aid organizations’ websites, as opposed to following links provided in emails.

If you have received this, or a similar hoax, please file a complaint at www.ic3.gov.

NIGERIAN 419 SCHEME

The FBI has become aware of spam emails crafted in the style of a Nigerian 419 schemes, exploiting the loss of lives attributable to Hurricane Katrina disaster. The email continues with instructions on how the recipient can claim money left behind, in an overseas bank account, by the next of kin. In some instances, in exchange for helping to move the funds, a portion of the inheritance is purported to be donated to Hurricane Katrina relief efforts. One version of the scam actually states family members have died in both the Thailand Tsunami and Hurricane Katrina. **THESE EMAILS ARE A HOAX. DO NOT RESPOND.** Other disasters Nigerian 419 schemes have attempted to capitalize on include: London Bombings; September 11, 2001; and various airplane crashes. When opening emails from unknown authors, please consider the following:

- Be skeptical of individuals representing themselves as Nigerian or foreign government officials asking for your help in placing large sums of money.
- Do not believe the promise of large sums of money for your cooperation.
- Guard your account information carefully.
- To ensure contributions to U.S. based non-profit organizations are received and used for intended purposes, go directly to recognized charities and aid organizations’ websites, as opposed to relying on others to make the donation on your behalf.

If you have received this, or a similar hoax, please file a complaint at www.ic3.gov.

CHARITABLE PHISHING, SPOOFING ALERT

The FBI is seeing an influx of websites soliciting for charitable donations to aid the victims of the latest natural disaster, Hurricane Katrina. Consistent with previous guidance on incidents of phishing/spoofing and identity theft, when considering online options for providing funding to this relief effort, consumers should consider the following:

- Do not respond to any unsolicited (SPAM) incoming emails.
- To ensure contributions to U.S. based non-profit organizations are used for intended purposes, go directly to recognized charities and aid organization's websites, as opposed to following a link to another site.
- Attempt to verify the legitimacy of non-profit organizations by utilizing various Internet-based resources which may assist in confirming the existence of the organization, as well as its non-profit status.
- Be leery of emails claiming to show pictures of the disaster areas in attached files, as the files may contain viruses. Only open attachments from known senders.

Several variations of this scam are currently in circulation. Be aware, scammers will attempt to capitalize on the popularity of the relief efforts along the Gulf coast. If you have received this, or a similar hoax, please file a complaint at www.ic3.gov.