

## Warning of Recent Phishing Attacks

Recently there has been an increase in phishing e-mails being sent from various sources which are scams. You could receive an official-looking e-mail from a financial institution or other legitimate institution you do business with which states that your ACH transaction or wire transfer was held in which you need to confirm some details or are warning you that your account requires some kind of immediate action.

The following are examples of e-mail messages that you could receive:

Subject line: Money transfer was not accepted by 'name of institution'

Dear Account Holder,

Money Transfer sent by you or on your behalf was hold by our bank.

Transaction ID: 17019302204565051

Current status of transaction: on hold

Please review transaction details as soon as possible.

*or*

Subject line: Wire transfer was hold by 'name of institution'

Dear Bank Account Operator,

I regret to inform you that Wire transfer initiated by you or on your behalf was hold by us.

Transaction: 238006864683285

Current transaction status: pending

Please review transaction details as soon as possible.

### What is Phishing?

Phishing is the practice of electronically obtaining personal information such as passwords, debit or credit card numbers, and other sensitive personal information by posing as a trusted institution, such as a financial institution or other legitimate institution you do business with. The purpose of phishing is to trick recipients into giving away account information, which can be used to steal money directly from linked accounts.

### How does phishing work?

Phishing usually involves an e-mail message that purports to be from a legitimate institution. Sometimes the recipient is instructed to click on a link within the message to “verify” their account information, with a threat of account deactivation or suspension.

Users who click on this link will be taken to a fake website that may look very similar to their own financial institution's. The user may be asked to provide his or her account number, PIN,

Social Security number, mother's maiden name and other information, which can be used to commit identity theft and fraud.

Occasionally, the message will contain instructions to call a phone number, at which time they will be prompted to enter this information.

### **How to protect yourself:**

The first thing to remember when it comes to phishing is this: **your financial institution and other legitimate institutions you do business with already have your personal information.** They have no need to contact you to verify this information. If there is a legitimate problem with an account, your financial institution will contact you with instructions to rectify the situation, which will never involve revealing personal information to an unsolicited e-mail or caller.

When you receive an e-mail message that claims to be from a trusted institution and asks you to verify account information, the easiest way to deal with it is to simply delete the message.

You may also forward the message (including all headers) to [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org), [spam@uce.gov](mailto:spam@uce.gov) and to the institution whose name is used in the message.

If a message seems like it might be legitimate, contact the institution directly, using the number in the phone book or by typing their web address directly into your web browser. Do not use the phone number contained in the e-mail message, and do not click on any links contained in the message. It is easy to make a link say one thing, but lead elsewhere.

### **Warning Signs:**

1. The message uses a generic greeting ("Dear valued customer") instead of your name
2. The tone of the message is urgent and demands that you respond immediately
3. The message asks you to verify account information or provide other personal information
4. The message is from an institution you don't even do business with
5. There are grammar errors in the message
6. The e-mail address that the e-mail is sent from contains the institution name, but it is not immediately after the @ in the e-mail address
7. If your web browser or other software are trying to alert you of a problem with a website or message, pay attention to these warnings

### **Links for additional information:**

- Anti-Phishing Working Group: <http://www.antiphishing.org/>
- Federal Trade Commission: <http://www.ftc.gov/>
- Internet Crime Complaint Center (IC3): <http://www.ic3.gov/>