

# Spotting Phishing Attempts

The email below is a phishing attempt that was sent to University email accounts in the Fall of 2008. The timing of this email was well thought out because an account notification is something you are likely to receive at the start of a semester. But a careful reader should be able to spot at least four major errors in this email that make it obvious that this is a phishing attempt. Can you spot at least four errors?

---

----- Original message -----

Date: Sun, 24 Aug 2008 21:17:14 +0300

(From): Helpdesk <helpdesk@inrets.fr> >(Subject): Dear MAIL.Uiuc User >(To): undisclosed-recipients;;

Dear MAIL.Uiuc User,

This message was sent automatically by a program on MAIL.Uiuc which periodically checks the size of inboxes, where new messages are received. The program is run weekly to ensure no one's inbox grows too large. If your inbox becomes too large, you will be unable to receive new email.

Just before this message was sent, you had 18 Megabytes (MB) or more of messages stored in your inbox on MAIL.Uiuc. To help us re-set your SPACE on our database prior to maintain our INBOX, you must reply to this e-mail and enter your Current User name ( ) and Password( ).

You will continue to receive this warning message periodically if your inbox size continues to be between 18 and 20 MB. If your inbox size grows to 20 MB, then a program on MAIL.Uiuc will move your oldest email to a folder in your home directory to ensure that you will continue to be able to receive incoming email. You will be notified by email that this has taken place. If your inbox grows to 25 MB, you will be unable to receive new email as it will be returned to the sender.

After you read a message, it is best to REPLY and SAVE it to another folder.

Thank you for your cooperation.

MAIL.Uiuc Help Desk  
Basement South 23  
David Rittenhouse Labs  
Philadelphia, PA 19104  
E-mail: webmail.uiuc.edu

---

Need some help knowing what to look for? Turn this sheet over for information about some of the most common tell-tale signs of phishing attempts.

# Common Signs of a Phishing Attempt

Not every phishing attempt will contain these tell-tale signs, but bad phishing attempts will contain some or all of the following:

## **MISSPELLINGS AND GRAMMATICAL ERRORS**

Many phishing attempts are hastily thrown together and contain numerous misspellings and grammatical errors. More carefully crafted phishing attempts might not have any errors at all.

## **THE EMAIL IS NOT ADDRESSED TO A SPECIFIC PERSON**

Most major companies that correspond through email (eBay, PayPal, Amazon, etc) have learned to start legitimate emails addressing you by your name or some kind of identifying information. While not every email addressed to something generic, such as “user,” is a phishing attempt, it is a great first sign that the email may be fraudulent.

## **THE SENDER’S EMAIL ADDRESS DOES NOT SEEM LEGITIMATE**

Every email will display the address that the email is sent from. Many phishing attempts rely on the fact that most people don’t take the time to check the actual address an email came from. But it can be the easiest way to spot a phishing scam. Your bank will never send you email correspondence from a Hotmail account, for example. So an email that was sent from buseybank@hotmail.com very likely could be a phishing attempt. Always check what email address you are replying to before sending a reply.

## **THE EMAIL IS ASKING YOU TO SEND SENSITIVE DATA OR ACCOUNT INFORMATION BY EMAIL**

Nearly all major stores, banks, universities, and other institutions and companies will **not** ask you to send your password, account details or other sensitive data by email. If you are unsure whether or not you should send sensitive information, you should simply call the company or institution that the email is supposedly from. If you do really need to update account information, it can usually be done over the phone.

## **THE EMAIL CONTAINS FACTUALLY INCORRECT INFORMATION**

Everyone makes mistakes, but if an email that you receive contains information that is noticeably incorrect, it could be a sign that it is a phishing email.

## **THE EMAIL CONTAINS LINKS TO UNRELATED WEB SITES OR COMMERCIAL OFFERS**

An email from your bank will not include an advertisement for pharmaceuticals, nor should the links in the email take you to any place but the company’s actual web site. Emails that contain potentially real information alongside information you’d see in junk emails, usually are just phishing attempts.

## **THE EMAIL APPEARS TO COME FROM AN ORGANIZATION OR COMPANY THAT YOU ARE NOT AFFILIATED WITH**

If you do not have an account with Wells Fargo, but you receive an email from Wells Fargo asking you to update your account details, it is a safe bet to characterize this email as a phishing attempt. These are usually the easiest phishing attempts for people to spot.