

Spotting Spam/Scam E-mail



Always check that

- ✓ **The e-mail address has the correct company domain**
 - (ex: UCF e-mail will come be a “ucf.edu” address)
- ✓ **Spelling, grammar and capitalization are correct**
- ✓ **No sensitive information is asked for in a reply back to the e-mail**
- ✓ **The e-mail is personalized with your name/information**
 - Spammers are getting smarter about this, but it is still a good way to spot some spam
- ✓ **There is a specific sender or department (that exists!)**
 - Most UCF e-mail will have a person or department listed. You can look them up on the UCF Phonebook: <http://phonebook.ucf.edu>

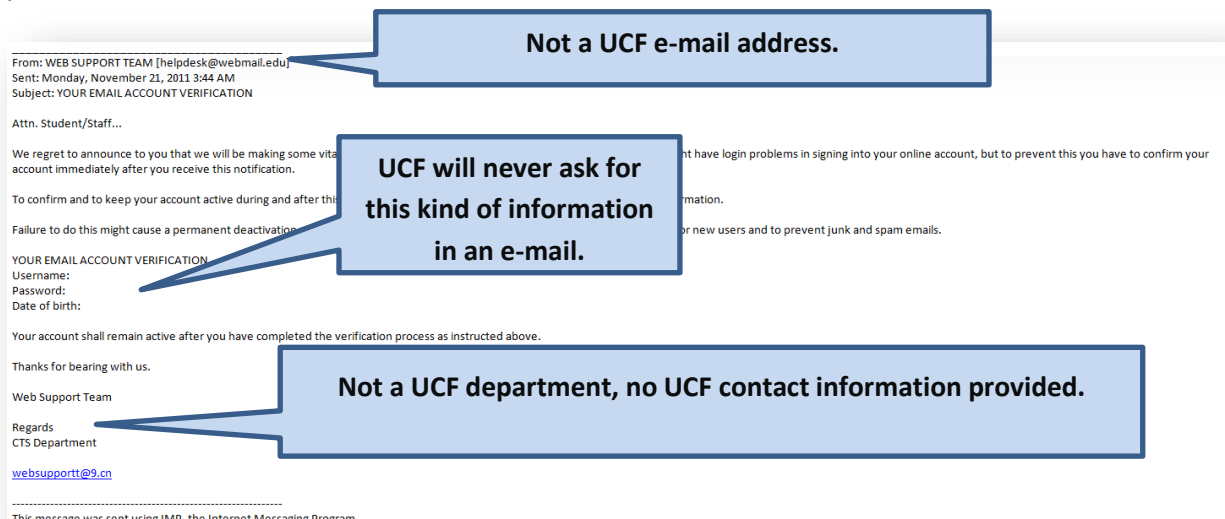
Scam 1: Your Account is in Trouble!

Scammers want to scare you into clicking a link or replying with sensitive information. Often they write that your account will be deleted or your access blocked.

1. **Is it asking for personal or account information? SPAM.** UCF will never ask for you to reply with personal or account information. No legitimate company will ask you to send that kind information in an e-mail.
2. **Is e-mail address different than the company domain? SPAM.** Often the sender’s address won’t even match the company they are claiming to represent. UCF messages will come from UCF e-mail addresses ending in the ucf.edu domain. (ex: ucfstaff@listserv.cc.ucf.edu or servicedesk@ucf.edu)

Important: Never click a link or call a number provided in an unsolicited e-mail. Always open a web browser and go to the official site to get a phone number or find an e-mail address.

Example 1: This e-mail threatens “permanent deactivation” of your e-mail account if you don’t reply with your account information.



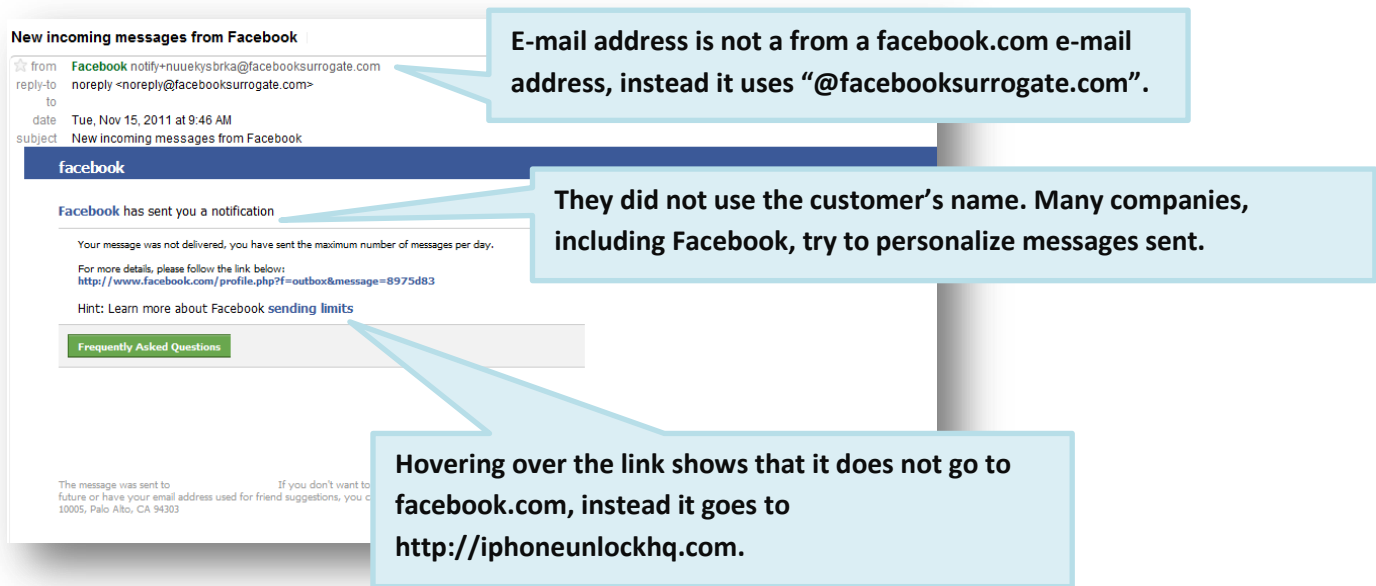
The screenshot shows an email from 'WEB SUPPORT TEAM [helpdesk@webmail.edu]' with the subject 'YOUR EMAIL ACCOUNT VERIFICATION'. The email body contains a warning about account deactivation and asks for 'Username', 'Password', and 'Date of birth'. Three callout boxes highlight red flags: 'Not a UCF e-mail address.' points to the sender's email address; 'UCF will never ask for this kind of information in an e-mail.' points to the request for personal information; and 'Not a UCF department, no UCF contact information provided.' points to the 'Web Support Team' and 'CTS Department' information.

Scam 2: Faking It

Many scammers will try to make the e-mail look as legitimate as possible. They may copy the style and graphics. If you are in doubt, open a new browser, go to the actual company website. From there you can check your account or use the contact information and then verify what is going on.

- Never call a number provided in a spam e-mail
- Never click the links provided in a spam e-mail

Example 1: This e-mail is trying to look like it came from Facebook.



New incoming messages from Facebook

from: Facebook notify+nueekysbrka@facebookssurrogate.com
 reply-to: noreply <noreply@facebookssurrogate.com>
 to:
 date: Tue, Nov 15, 2011 at 9:46 AM
 subject: New incoming messages from Facebook

facebook

Facebook has sent you a notification

Your message was not delivered, you have sent the maximum number of messages per day.

For more details, please follow the link below:
<http://www.facebook.com/profile.php?f=outbox&message=8975d83>

Hint: Learn more about Facebook sending limits

Frequently Asked Questions

The message was sent to [redacted] If you don't want to be added to our mailing list in the future or have your email address used for friend suggestions, you can unsubscribe here: <http://iphoneunlockhq.com>

E-mail address is not a from a facebook.com e-mail address, instead it uses "@facebookssurrogate.com".

They did not use the customer's name. Many companies, including Facebook, try to personalize messages sent.

Hovering over the link shows that it does not go to facebook.com, instead it goes to http://iphoneunlockhq.com.

Example 2: This e-mail is pretending to be from a bank.



Re-Confirm Your Online Account

JPMorgan Chase Bank <online-banking@chase.com>

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Sent: Thu 11/3/2011 4:52 PM
 To:

Dear Customer,

We Are Currently Upgrading Our Online Banking Security. To ensure Secured Access To Your Bank Account Online. Please Re-Confirm Your Online Banking Account To Avoid Losing Access To Your Account Online.

To View Your Account Information, please click the "Re-Confirm" link below to access your account information at <http://www.arhantcards.com> or chaseonline/online.htm

[Click to follow link](#)

Re-Confirm

JP Morgan Chase & Co. Customer Service

Copyright © 2011 JPMorgan Chase & Co. Bank of America. All rights reserved.

The spammers did manage to fake the e-mail address so it looks like it could be from the bank.

Capitalizing every word is poor business writing. A legitimate company uses proper spelling, grammar and capitalization. The e-mail threatens "losing access" to the site if the link isn't clicked. This is clearly spam.

They use a link and not a web address in plain text (like www.chase.com). Hovering over the link shows that it goes to www.arhantcards.com. This is clearly a spam site.