# Don't Get Hooked by "Phishers"

- Do not share your password
- Do not reply to phishing e-mails or click on links in a phishing e-mail
- Warn your friends about phishing e-mails
- For information about phishing-emails, visit security.sc.edu
- Contact the UTS Help Desk at 803.777.1800 if you replied to a phishing e-mail or if you need assistance

**phish** (fĭsh) n. -ers, -ing. 1. Any communication intended to trick the recipient into disclosing secret or sensitive information, such as passwords, Social Security Numbers, user names, or bank account numbers. Most often this communication is done by e-mail. 2. A phishing attempt targeted at a small group of people, rather than broadly distributed is called "spear-phishing".


**From:** USC ITS HELP DESK
**Date:** Sunday, February 15, 2009 04:23
**To:** itshelpdesksc@mail2webmaster.com
**Subject:** Confirm Your USC Account Details.

Attn. USC Webmail User,

We regret to announce to you that we will be making some vital maintainance in The University Of South Carolina webmail database. During this process you might have login problems in signing into your USC Online account, but to prevent this you have to confirm your USC account immediately after you receive this notification.

To confirm and to keep your USC account active during and after this process, please reply to this message with the below account informations. Failure to do this might cause a permanent deactivation of your user USC account from our database to enable us create more spaces for new users.

CONFIRM YOUR USC ACCOUNT DETAILS BELOW:
==========
Name:
USC E-mail ID:
USC E-mail Password:
Date of birth:
==========
Your USC account shall remain active after you have successfully confirmed your account details.

Thanks for bearing with us.

USC ITS HELP DESK.

# Can you spot a phishing attempt?

## Learn the warning signs.

**Unfamiliar sender?**
Who is the webmaster? Remember, "from" addresses are very simple to forge.

**WARNING!**
System generated warning in subject line.

Out of date, or misplaced logos.

**WARNING!**
System generated warning message at the bottom of the e-mail.

**From:** webmaster@sc.edu
**Date:** Saturday, March 07, 2009 09:44
**To:** name@mailbox.sc.edu
**Subject:** *POTENTIAL PHISHING ATTEMPT* Account Update

Dear University of South Carolina webmail Users;
This message is from University of South Carolina webmail messaging center to all University of South Carolina webmail users. We are currently upgrading our data base and e-mail center. We are deleting all unused University of South Carolina webmail Account. You are required to verify and update your email by confirming your email identity immediately. This will prevent your email from been closed during this exercise. In order to confirm your email identity, you are to provide the following data;
CONFIRM YOUR EMAIL IDENTITY BELOW
First Name:_____
Last Name_____
Email Address:_____
Email Password:_____
Warning!!!University of South Carolina webmail user that refuses to verify and subsequent update his or her email within Seven days of receiving this warning will lose his or her email
permanently.

University of South Carolina webmail Management
Copyright © University of South Carolina webmail all rights reserved.

WARNING: The above message makes use of language that suggests it may be an attempt to obtain your password. The University of South Carolina employees or students should never request password information from you for any reason. In accordance with USC IT Security Policy, IT 1.06, you must not reveal your password information to anyone. If you believe that this message is an attempt to steal your password, forward this message to phishing@sc.edu and do not respond to this message.

Generic salutation!
Trusted organizations likely already know your name and information. Why wouldn't they use it?

**Attempt to collect!**
The university already knows your name and e-mail address. Why would they ask for your password?
**They won't.**

**Poor Grammar!**
It is a common warning sign of a phishing attempt.

**High Pressure Tactics!**
Phishers often threaten users with action, or provide a "limited time offer". They're trying to rush you into making a mistake.

**Remember:** Always "hover" over unfamiliar links to find out their true destination. Also, you should never open an attachment from e-mail unless you know the sender, and you're expecting a file.

Secure
**Carolina**
UNIVERSITY OF SOUTH CAROLINA