

# DON'T LET PHISHERS PLAY YOU

“Phishing” is a trick that thieves play to get you to give them personal information — like your login ID and password, Social Security number, bank account or PIN numbers — by pretending to be someone they’re not. Phishers use the information to **spew spam, open accounts under your name or commit other fraud. This one tricked some Davis students last spring.**

## Learn to recognize phishing scams!

*Criminals phish at odd hours when they know IT help desks are closed*

From: UC Davis Support <ucdavis.sup@googlemail.com>  
Date: Sat, Apr 4, 2009 at 8:37 AM  
Subject: Verify Your UC Davis Account  
To:

*This info can be easily faked*

Dear UC Davis Webmail User,  
To complete your Account Verification process, you are required to reply to this mail and enter your username and password in the spaces provided below, you are to do this before the next 48 hours or your Account will be deactivated and erased from our database.

*Why do I need to verify?*

*Phishing messages usually contain threats*

Enter Username: (???????????? )  
Enter Password: (???????????? )

*UC Davis will NEVER ask for your password over email or phone*

Thank you for using UCDAVIS Internet Service

UCDAVIS INTERNET SUPPORT TEAM

*We don't know who this is, do you?*

**Not all phishing scams look like this one**, but if you get an email (or phone call or snail mail) that asks for your password, ignore or delete it. **When in doubt, call the IT Express Computing Services Help Desk at (530) 754-HELP (4357) before responding.**