



Information Technology Services  
Security Bulletin

## Phishing Emails

From time to time members of the Baylor University community receive false and misleading phishing emails regarding “Baylor Webmail” or other accounts. Phishing is an attempt to acquire sensitive information electronically by pretending to be a trustworthy entity. Phishing attempts may ask for usernames, passwords, credit card information and other personally identifiable information. Any email you receive regarding your Baylor email or “Webmail” account asking you to reply with your username and password is a scam. Higher education institutions have increasingly been targeted with these types of emails in an effort to gain access to university resources.

Phishing messages may look as though they are coming from Baylor ITS or the Baylor Help Desk. At no time will ITS or the Help Desk ask for your username/password with an email, phone call or during an in-person visit.

If you are in any way suspicious of an email you receive, please contact the Help Desk (x4357) about the message. Some examples of the emails are located at:

<http://www.baylor.edu/its/news.php?action=story&story=60314>

Tips to avoid being Phished:

- Never send your username/password or personal account information in an email.
- Be suspicious of links within email messages, particularly from unknown or dubious sources. (It is preferable to type the URL into your web browser.)
- Contact the Help Desk (x4357/HELP) in the event you receive an email about which you are unsure.

*Protect Your Past, Secure Your Future*



One Bear Place #97268, Waco, Texas 76798-7268 • [www.baylor.edu/its/](http://www.baylor.edu/its/) • (254) 710-4357