

## IT SERVICE ADVISORY

### **Issue: Spoofing**

On occasion you may receive an email in either your Microsoft Outlook Inbox or Postini Message Center (CTC's outside spam filtering service) with your CTC email address as the sender. These emails are usually trying to sell you something or get you to click on a provided link. Although you never sent this email your email address is listed as the sender. How can this be? Simply put, your email address has been spoofed.

There are three forms of spoofing:

1. Using your email address to send spam or fake email messages.
2. Attempting to gain access to a system by posing as an authorized user.
3. The unauthorized use of a third-party domain name as the sender's name in an e-mail message e.g. PayPal or eBay notices.

Email addresses are generally harvested from various Web sites and newsgroups where users enter registration information. This information is then stored in a database for easy retrieval for future logons or to confirm access to specific areas of the Web site. Those databases can sometimes be compromised by crackers, the information harvested, and later sold to spammers. Spammers will pay up to \$10 per megabyte for email addresses. If a spammer gets one or two unsuspecting users to give them money for a false advertisement then they have made their money back. Based on some reports, over 75% of all email traversing the Internet is spam and most is sent using a spoofed address.

Spammers use legitimate spoofed email addresses because junk filters can filter out fake email addresses that may appear to be gibberish. A legitimate email address is more likely to make it past spam and junk filters and past an enterprise's firewall ending up in email inboxes throughout the organization and even the sender's inbox. Think of it as putting the wrong return address on a letter. The sender does not want the recipient to know who really sent the letter but still wants the letter to be opened so a false return address is used.

Spoofed email addresses are one of the dangers associated with Internet usage. The more you register your email address on Web sites, newsgroups, or even routine email messages, the more likely your email address will be spoofed. Attempts to track down who is actually sending spam with spoofed email addresses is costly and time consuming and requires a large scale attempt that most IT departments cannot perform. To hide their tracks, spammers use Internet Protocol Anonymizers to hide their true IP address making it even more difficult to track spam's origin. Recently the Federal Trade Commission had to shut down an Internet Service Provider because it refused to stop spammers from sending spam.<sup>1</sup>

If you receive spam in your Outlook Inbox perform the steps outlined on the IT Web site (<http://www.ctcd.edu/infotech/ctcisd/Education/Tech%20Tips/email/postini.html>). If you receive spam in your Postini Message Center simply delete it.

**Number: ITSAD-060909-01**

Carla Littlefield  
Director, IT Customer Service  
Central Texas College  
800-223-4760 ext: 3102  
Fax: 254-526-1950  
[Central Texas College Information Technology Division Home Page](#)