US FORUM CONNECTION #76, APRIL 2010

This free newsletter is sponsored by the United States Forum of The Delta Kappa Gamma Society International. The Delta Kappa Gamma Society International is an organization of leading women educators with over 105,000 members. Delta Kappa Gamma members wishing to subscribe to this FREE newsletter should send a request to Angela.Bedenbaugh@usm.edu. We urge you to share this newsletter with other interested individuals who are not members of Delta Kappa Gamma or members who do not subscribe to this publication.

PAYCHECK FAIRNESS ACT
PROTECTING YOUR EMAIL IDENTITY
HEALTH WARNING FOR DIABETICS

PAYCHECK FAIRNESS ACT

The Paycheck Fairness Act (H.R.12;S.182) passed the house on January 9, 2009. A strong move by several women's organizations is currently under way to get the bill passed in the Senate. At the National Legislative Seminar in March, Lisa Maatz from the American Association of University Women provided us with information about the status of this act. A state specific message has been sent to DKG U. S. Forum Connection subscribers in states whose U. S. Senator/s can help with passage of the bill by either signing on as a cosponsor or pledging to vote for cloture on debate on the bill. Of interest only four Republican senators voted for the Lilly Ledbetter Fair Pay Act of 2009 – Susan Collins, Kay Bailey Hutchinson, Lisa Murkowski, and Olympia Snowe. The only one of these women who signed on as a cosponsor of that bill was Olympia Snowe. We women have to stick together. It is to be hoped that these women would vote for cloture. Without a cloture vote by at least one or two of these women the Paycheck Fairness Act will not come up for a vote.

PROTECTING YOUR EMAIL IDENTITY

Email phishing is an e-mail sent to you and hundreds of thousands of others with a message that tries to trick you into revealing sensitive personal information, such as passwords, banking information, your Social Security number, your mother's maiden name, your date of birth and more. The attack is waged against you in an attempt to hijack your assets, steal your identity or even open credit card accounts in your name.
Five ways to spot phishing

1. Check the spelling

Scammers are notorious for their lack of basic spelling and grammar skills. Look for misspelled words and incomplete or awkwardly written sentences. It's not uncommon for a scam e-mail that is purportedly from a reputable and well known organization to misspell the name of that organization! For example, one e-mail scam aimed at Facebook users spelled the name of the site in lowercase ("facebook").

2. Who signed it?

If it's a legitimate e-mail from a business, it will be signed with a person's name and contact information, but if it signs off with something vague, such as "Customer Support," be suspicious.

3. DOES THE E-MAIL SCREAM AT YOU IN ALL CAPS?

Be especially aware of e-mails that try to get your attention by using all capital letters, especially in the subject line. Using all caps has long been viewed as online shouting. It just isn't done. The authors of scam e-mails tend to write prose that is over-the-top and very emotional. In addition to a lot of capital letters, look for an excess of exclamation points and dire warnings, such as "Urgent!" or "Danger!"

4. The e-mail has an executable attachment

Phishers can only scam you if you let them. You do just that if you download e-mail attachments, which may contain computer viruses. Since a favorite way to send a scam e-mail is by making it look as if it were sent to you by someone in your e-mail address book, don't be fooled by the sender's name. Never download an attachment unless you are sure it's legitimate.

5. The e-mail has a link to a Web site

As more people have learned they shouldn't download attachments from strangers, scammers have caught on. Instead of attaching a file, they include a clickable link to a Web site. Click on that link, and you might be asked to provide personal information. Do it, and you've been scammed. For example, you might receive an e-mail

that appears to be from your bank, offering you a very low interest rate on a mortgage or home equity loan. If you click on the link, it could ask your name, bank account number and online banking password to get onto the site. Don't ever provide this information if you got on the site by clicking a link in an e-mail.
6. Even if the email looks as though it came from a reputable source and asks for personal information it is a phishing attempt. For example from a recent email

******* WARNING*******

If you receive the email below, do NOT respond to it.
It is a phishing attempt to jeopardize your email account.

Kevin Sellers
College of Science and Technology
University of Southern Mississippi
kevin.sellers@usm.edu
601-266-6671

Dear usm Webmail User,
This mail is to inform all our webmail users that we are upgrading our server.We are deleting all unused webmail and old mail accounts which are no longer active to create more space for Quota Increase.Please you are required to click the Link Below to re-confirm your account so that we will know that it's a present used account and is still active by providing the information.

usmemailaccountupgrade:
Validate your email to increase your quota by filling out your Information correctly on the link form above or your account will be suspended within 72 hours for security reasons.
Thanks
NOTE THE IMPLIED THREAT OF SUSPENDING YOUR ACCOUNT. THE EXTENDER @USM.EDU IS CORRECT, THE 601-266 IS THE UNIVERSITY TELEPHONE EXCHANGE AND KEVIN SELLERS IS A UNIVERSITY EMPLOYEE IN THE TECHNOLOGY OFFICE.

One final word of advice: Never, ever respond to a spam e-mail. By doing so you confirm your e-mail account is active, and you'll likely be inundated with more spam.

HEALTH WARNING FOR DIABETICS
If you are taking the drug Avandia, I strongly urge you to consult with your physician. Since 2003 the Nader Public Citizen/Health Research Group has warned of serious side effects affecting the heart from taking this drug. In 2008 the American and European Diabetes Associations warned doctors not to use the drug. Physicians at the Food and Drug Administration concluded that the drug is "too dangerous to be sold," but the pharmaceutical company was able to override this recommendation. In a February 2010 issue of the New York Times a warning was published about the side effects of the drug. (http://www.nytimes.com/2010/02/20/health/policy/20avandia.html) Information about a class action law suit against the maker of Avandia can be found at http://avandia.legalview.com/avandia-lawsuit.aspx

For on-line information on specific bills go to http://thomas.loc.gov/

CONTACT ADDRESSES FOR GOVERNMENT INFORMATION

U.S. GOVERNMENT CONTACT INFORMATION can be obtained through Congressional Switchboard 1-866-327-8670 (this is a toll free number). You can contact your Congressman and Senator through this number without paying long distance charges.
http://www.house.gov/ for members of the House of Representatives http://www.senate.gov/ for members of the U.S. Senate

STATE GOVERNMENT CONTACT INFORMATION can be obtained through

http://www.emailyourgovernor.com/ Information available at this site allows contact with governors, members of the state legislature, state supreme court, congressional delegation and state agencies such as the Education Department, Attorney General, Motor Vehicles Department and Voter Registration.

INFORMATION ON HOW YOUR CONGRESSMAN VOTED ON KEY BILLS
http://projects.washingtonpost.com/congress/111/bills/
FIVE CONSTITUENT CONTACTS WILL CAUSE A LEGISLATOR TO PAY SERIOUS ATTENTION TO A GIVEN ISSUE.

Archival copies of the U.S. Forum Connection can be found at
http://ocean.otr.usm.edu/~w305514/HomePage.htm

Dr. Angela O. Bedenbaugh
The University of Southern Mississippi
118 College Drive #8466
Hattiesburg, MS 39406-0001
Office: (601) 266-5718, (800) 814-4673
Fax: (601) 266-5718
Answering machine (601) 266-4712