Professional Development

**Introduction to Information Security**
Facilitators: Ms. Lori McElroy and Mr. Corbett Consolvo
Thursday, January 24 and Friday, January 25, 2008
Summary of Evaluations

| Registered | 62 |
| Completed Workshop | 58 |
| Completed Evaluations | 53 |

(Percentages taken on completed evaluations)

Excellent: 4  Good: 3  Fair: 2  Poor: 1

A. To what extent did this workshop meet its objectives?  

<table>
<thead>
<tr>
<th>Rating</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excellent</td>
<td>35</td>
<td>66.0%</td>
</tr>
<tr>
<td>Good</td>
<td>17</td>
<td>32.1%</td>
</tr>
<tr>
<td>Fair</td>
<td>1</td>
<td>1.9%</td>
</tr>
<tr>
<td>Poor</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>No Response</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Avg. 3.64

B. What is your overall impression of the workshop?  

<table>
<thead>
<tr>
<th>Rating</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excellent</td>
<td>34</td>
<td>64.2%</td>
</tr>
<tr>
<td>Good</td>
<td>17</td>
<td>32.1%</td>
</tr>
<tr>
<td>Fair</td>
<td>2</td>
<td>3.8%</td>
</tr>
<tr>
<td>Poor</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>No Response</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Avg. 3.60

C. How would you rate presenter(s) as to knowledge of subject and presentation?  

<table>
<thead>
<tr>
<th>Rating</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excellent</td>
<td>46</td>
<td>86.8%</td>
</tr>
<tr>
<td>Good</td>
<td>7</td>
<td>13.2%</td>
</tr>
<tr>
<td>Fair</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Poor</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>No Response</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Avg. 3.87

D. Has this workshop provided you with information/motivation to do something differently in your job?  

<table>
<thead>
<tr>
<th>Response</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>41</td>
<td>77.4%</td>
</tr>
<tr>
<td>No</td>
<td>8</td>
<td>15.1%</td>
</tr>
<tr>
<td>No Response</td>
<td>4</td>
<td>7.5%</td>
</tr>
</tbody>
</table>

If “yes,” identify one or more things:
1. Call IT immediately to secure a computer IT administrator for department
2. Get personal e-mail account for work
3. Make sure sensitive information is adequately secured or removed from department computers
4. How spam and viruses can be transmitted through e-mail
5. Back up computer regularly
6. Ensure home computer is secured and ensure work updates are current
7. Be more aware of my desktop and securing the information
8. Lock keyboard when away from computer
9. Do not forward e-mails.
10. Spam
11. Password
12. Back-up home computer
13. Talk to kids and stress security issues
14. Change passwords to strong passwords
15. Limit use of computer for personal information
16. Campus resources I can use
17. Will check my equipment to make sure it is secure
18. Monitor security procedures better
19. Help with passwords
20. Learned more about IT security services
21. Range of protection needs
22. Threats to information
23. Annual report
24. Be aware of what I am actually forwarding or viewing in e-mail
25. Change all passwords
26. Encrypt router at home
27. Back-up home computer
28. Take additional security measures at home
29. Data backup
30. Put forth greater effort to protect my information
31. Use stronger passwords
32. Back-up my computer
33. Use better passwords
34. Change passwords frequently
35. Encrypt wireless at home
36. Check systems at home and at work
37. Back-up valuable files
38. Address issues related to confidential and restricted data/information
39. Lock all paper based records and shred them after their use is over
40. Check to see if we have a firewall on server hosted by the college for annual faculty evaluation. I will ask for a security scan.
41. I have made lists of action items for my IT person.
42. Be a little more cautious with my personal information on-line
43. Be very careful about data and activities using university and personal network
44. Updating programs when you get the first notice
45. Better passwords
46. Better updates
47. Put a password on my PDA
48. Levels of protection
49. Make a list of things to do to make my computer more secure. Examples: clear cache, delete temporary files. Some of this was covered. Please teach us more.

If "no," identify one or more things:
1. It's my job.

E. Topics of interest to you for future Professional Development workshops:
1. Host technical firewalling
2. How to encrypt
3. Identifying viruses
4. Travel security workshops through IT
5. What to do when you get a virus
6. What a virus can do to your computer
7. Wireless networking
8. Setting and securing personal wireless networks
9. More IT related topics
10. How to fix Spyware on the computer
11. What operating systems are more at risk
12. Specific "how to" information on the general topics covered
13. Hands-on workshop for the novice user to keep systems clean
14. How to encrypt your own network
15. Best practices for fixing Spyware
17. Offer a workshop on network security
18. Cleaning hard drive
19. Microsoft XP and Vista-comparison
20. Hands on configuration.
21. Training on cleaning out computers' confidential information, how to manage passwords, how to secure PDA's, more on identity theft. One page information sheets for administrators would be helpful. MySpace and Facebook information sheets for advising centers and student organizations.
22. What to look for when purchasing computers. University discounts?
23. Cleaning up your computer
24. After identity theft
25. More hands-on training on how to have a more security conscious work style. Example--how to clear cache, etc.
26. Home router security set up

Suggestions for future speakers/facilitators:

<table>
<thead>
<tr>
<th>Name</th>
<th>Subject Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phil Zimmerman</td>
<td>Security</td>
</tr>
</tbody>
</table>

F. Comments for improvement of this workshop:
1. Handouts are very hard to read because the print too small.
2. Log retention policy?
3. Have regular semester information workshops on this subject.
4. Having some technical people in the room was good to help answer some of the questions.
5. Technical people in the room need to let the presenters actually present.
6. Great job
7. Lots of good important information that didn't get covered. Introduction was too heavy. Spent too much time convincing us why security is important. We know this. That's why we're here.
8. Well done.
9. The print was too small to read a lot of the web site addresses. TR website was mentioned and didn't see the link to TR in the presentation.
10. Perhaps the last page could be a print out of all the links presented throughout the presentation, but not in slide format so they are legible.
11. Make it three hours long.
12. May not need to create the name badges.
13. Incorporate (be sensitive to) audience questions. May assist for less participative groups than today.
14. Excellent job at anticipating my questions!
15. The presentation was slowed down due to too much feedback from audience, and we had to hurry through rest of the material.
16. Expected more specific information
17. I enjoyed the apple; offering fresh fruit and vegetables as snacks. Also, other healthy choices in beverages. Reduce the sugar-heavy items!
18. This was a very well thought-out presentation. Thank you.
19. I would like to provide the handouts with overheads to chairs/directors, etc., but some are not readable (especially those slides with shaded backgrounds). Web site addresses were also unreadable on the handout.
20. Brochures about downloading music should be sent to deans with suggestions that they be posted in advising centers for students to read.
21. On the video powerpoint slide, put the main point for the reader who isn't present at the training.
22. Good job. Thank you. I learned a lot of practical things.
23. Perhaps provide pamphlets on things to do for your computer--encrypting your computer at home.
24. Well presented
25. Good job of covering information.
26. I think the student worker was great. He should talk more.
27. Can you send slides? We cannot read links. Send the information security slides to everyone.
28. Training such as this is very important to administrative assistants. It should be mandatory.