Session #:____________

CYBERGIRLS OUTREACH: A CYBER OUTREACH PROGRAM FOR MIDDLE AND HIGH SCHOOL YOUNG WOMEN

Khadija Stewart and Nadine Shillingford

DePauw University, Greencastle, IN; Email: khadijastewart@depauw.edu
Rose-Hulman Institute of Technology, Terre Haute, IN; shilling@rose-hulman.edu

ABSTRACT

We propose to use the increased interest of teens in the Internet and social networking to attract female middle and high school students to computing majors through outreach sessions focused on cyber security concepts and the ethics of social networking (Cybergirls Outreach). These sessions will also help make the teens aware of the security risks involved when using the Internet and social networking sites. The goal of this novel program is three-fold. First, we aim to introduce female students to the basics of Internet security including the areas of cryptography, social networking, and ethics in a fun and engaging manner. Secondly, we hope to culture an appreciation of computer science in the participants. Thirdly, we intend to extend this program's materials to middle and high school teachers so that they can implement them in their classroom. This paper gives a description of the outreach program including the outcomes and procedures of every module of the program and discusses the logistics of its implementation.

1. INTRODUCTION

Enrollment of college students in computing fields has suffered a significant decline since the Internet bubble burst in the early 2000s. According to ACT 2010, the number of job openings in computing is greater than the number of students interested in computing by a factor of five and a half. To remedy this, the National Science Foundation ushered several programs to help increase the enrollment of students in computing[1]. The Obama administration has been encouraging Americans to focus on STEM fields. In fact, in his January 2011 state address, President Obama stated that STEM education is necessary to 'win the future.'

In this work, we propose an Internet security outreach program for middle school and high school girls that we hope will spark their interest in STEM fields, teach them secure Internet practices, and increase their confidence in the sciences. We chose to focus on female students because the percentage of women in college majoring in STEM fields has been very low (a fraction of the percentage of male students in STEM fields) and declining for the past twenty

[1] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5488/

years. According to the 2008-2009 Taulbee survey[2], the percentage of women who received Bachelor's degrees in Computer Science and Computer Engineering was less than 12%. Female students tend to have less exposure to computer science and technology. In fact, (Milbourne, 1999) indicates that girls tend to lose interest in middle school. The authors of this paper are female computer scientists who realize the value of having female role models. Therefore, the outreach sessions will be conducted by the authors with the help of female computer science undergraduate students from their respective institutions.

We chose to focus on outreach sessions for Internet security and the ethics of social networking because of the widespread use of Internet and social networking applications, especially among teens. Sixty-five percent of teens in the US participate in online social networking sites such as Facebook[3]. These applications are available on cellphones so teens have constant access to them. We believe that because of the relevance of this topic to the teenager's social life, we can cultivate their interest in the program. We also believe that teenagers should be taught proper Internet security practices and be made aware of the ethical issues stemming from Internet security and social networking. According to Fisher et al. (2002), 43% of teens reported that they have experienced some form of cyberbullying. Furthermore, the MCPC report also states that female teenagers (15 and 16 year olds) are more likely to experience cyberbullying.

Despite the national push to increase the student's interest in computing, several states have not yet incorporated computing into their middle and high school curricular. Indiana is unfortunately one of those states[4]. Due to the recent nation-wide budget cuts in the education sector, the authors do not expect any additions to the curriculum in the near future. The authors believe that the creation of an outreach program to be a good intermediate solution to the problem.

An important component of the program is the participation of middle and high school teachers. The authors hope that by having the school teachers be part of the organization and implementation of the proposed program, they can increase the overall impact of the outreach sessions. The authors also plan to have modules made available to the teachers so that they could incorporate them in their regular curricular.

We believe that the novel focus of this outreach program will help attract female middle and high school students and allow them to embrace the program experience with an open mind. Several workshops and outreach sessions have been offered with the aim to attract girls to science and technology[5,6] (Groth et al., 2008) but unlike our proposed solution, none of these programs are focused on introducing female middle and high school students to cybersecurity and the ethics of social networking.

[2] http://www.cra.org/uploads/documents/resources/taulbee/0809.pdf

[3] http://www.pewinternet.org/Reports/2007/Teens-and-Social-Media.aspx

[4] http://dc.doe.in.gov/Standards/AcademicStandards/PrintLibrary/bme.shtml

[5] http://www.cs.cmu.edu/cs4hs/summer10/workshops.html

[6] http://outreach.cs.utexas.edu/firstbytes/

We are in the process of writing an NSF grant proposal to secure funding for the proposed program. We also intend to extend the outreach program to include summer camps. Initially, the program will take place in Central Indiana with plans to expand it to nearby states. We are also designing a cybersecurity workshop-in-a-box toolkit that can be shared with the community so that similar workshops can be implemented in other locations.

Students who successfully complete this program should be able to (1) explain the history of the Internet and Internet security by discussing major cybersecurity breaches and preliminary security concepts, (2) describe basic cryptography concepts including key exchanges and ciphers, (3) analyze the basic security risks of networks and databases, (4) identify phishing sites and other security attacks, (5) discuss the ethical issues associated with the Internet, and (6) develop proper social networking skills. The program material is divided into four main modules. We outline the different modules in the course curriculum in Section 2.

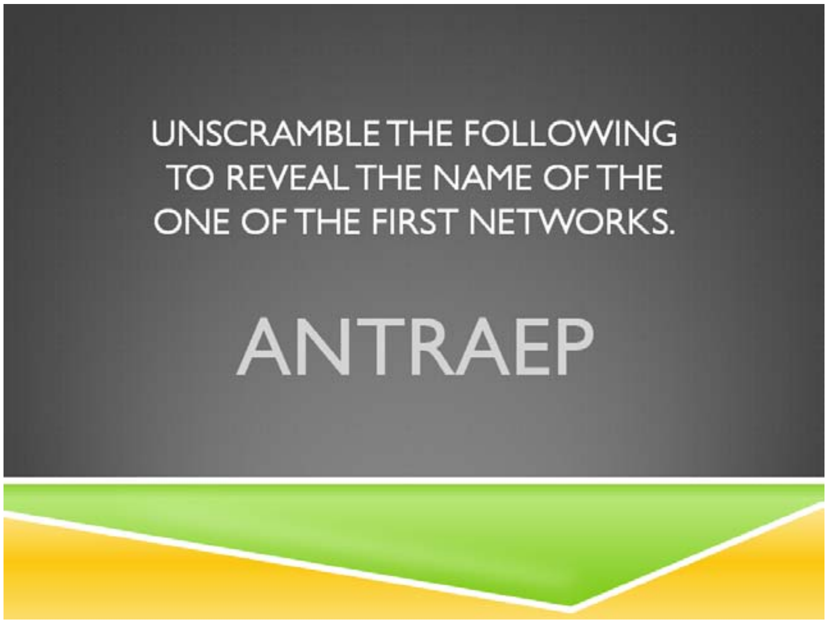
2. MODULES

The following are the modules we plan to cover during the outreach sessions. In addition, module objectives are outlines for each of the following subsections. We propose to have one outreach session every month during the academic year for a total of 7 outreach sessions per year in addition to one presentation day during the month of May. The presentation day will consist of a poster session where the students will present their group projects. The poster presentation will be attended by the student's teacher, family members and members of our institutions. The poster presentation will be followed by an award ceremony and a celebratory dinner.

2.1 Module 1 – Appreciation for the History of the Internet and Cybersecurity

In this module, students will learn about the history of the Internet and cyber security. This module lays the groundwork for the subsequent modules. It also aims to show the students the challenges in developing a secure Internet. On completion of this module, the students will be able to:

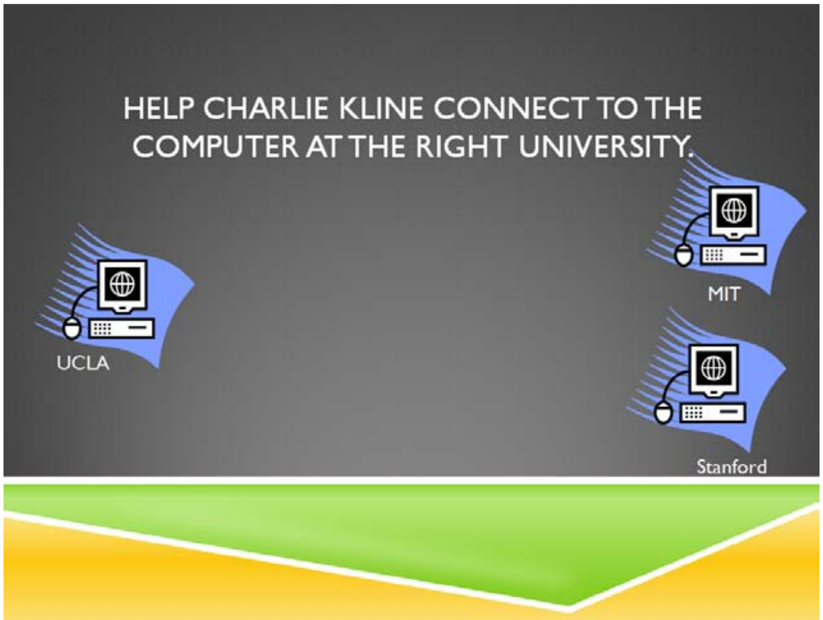
1. Discuss the history of the Internet including the circumstances of its creation and evolution.
2. Define basic terms such as hacking, passwords, Internet, cybersecurity, cryptography, network, and virus.
3. Understand network protocols such as HTTP, IP, and SMTP.



UNSCRAMBLE THE FOLLOWING TO REVEAL THE NAME OF THE ONE OF THE FIRST NETWORKS.

ANTRAEP

Figure 1 : A sample quiz question



HELP CHARLIE KLINE CONNECT TO THE COMPUTER AT THE RIGHT UNIVERSITY.

Figure 2: A sample quiz question

To achieve Outcome 1, students will be shown a 10-15 minute presentation on the history of the Internet and interactive quiz questions after every 2-3 slides to review the material presented. Two examples of quiz questions are shown in Figures 1 and 2. In addition, each group of 2-3 students will be assigned to read specific excerpts from (Richards, 2002), which detail the history of the Internet starting from Vanevar Bush's article "As We May Think" (Bush, 1945). The students will be given ample time to discuss the events occurring in the articles. Once the excerpts have been read and discussed, the groups will make informal 5 minute presentations to the class on the concepts they read.

Table 1 Sample Terms.

Terms
antivirus, authentication, authorization, backup, cookie, cryptography, cyberbullying, cybersecurity, denial of service attack, encryption, firewall, hacking, identity theft, Internet, IP address, intrusion, MAC address, network, password, permissions, privacy, protocol, virus, worm, zombie

Outcome 2 ensures that students become familiar with some basic Internet security terms. This is to ensure that the students are able to communicate to each other in the jargon of Internet security. Sample terms are listed in Table 1. The students will learn basic terms by listening to short lectures and video clips. The students will participate in a game such as Vocabulary Jeopardy (similar to the popular television game show). Utilizing a game ensures that a rather mundane task of learning definitions is achieved in a fun manner.

Outcome 3 for this module requires the students to understand basic network protocols such as HTTP, IP, and SMTP. Short lectures and hands on laboratory exercises will be used to introduce networking concepts and protocols. During the laboratory exercises, we will use a network sniffer such as Wireshark[7] to intercept and analyze network packets.

2.2 Module 2 - Cryptography and Ciphers (Why Math is Cool!)

In this module, the students will learn about cryptography concepts. The main concepts covered are:

1. Caesar cipher, mono-alphabetic and poly-alphabetic ciphers,
2. Symmetric key cryptography and public key cryptography.
3. The core principles of security: confidentiality, integrity, availability, authenticity and non-repudiation.

This module includes discussions of real life examples that implement cryptography such as ATM cards, e-commerce sites, and passwords. The sessions will consist of very short lectures (no longer than 5 minutes) interleaved with longer hands on activities. The activities involve solving simple ciphers by hand and using environments such as Alice[8] and Scratch[9]. To learn about cryptography and passwords, resources such as[10] will be used. The sessions will also consist of some laboratory exercises where the students work in groups.

The goal of the laboratory exercises is to re-enforce the concepts learned, practice the concepts using simulated and real-world environments and enforce group work and student involvement.

[7] http://www.wireshark.org

[8] http://www.alice.org

[9] http://scratch.mit.edu/

[10] http://triton.towson.edu/~cssecinj/secinj/?page_id=1669

After each laboratory exercise, the students will have a tangible outcome that they create or help create (whether that is a simulated world, a list of scenarios, etc.). The laboratory exercises for this module are described below:

Laboratory Exercise 1 - Caesar, Mono-alphabetic and poly-alphabetic ciphers: During this laboratory exercise, the students will use the Alice environment to practice using the Caesar, mono-alphabetic and poly-alphabetic ciphers. We developed an Alice project that depicts a scenario where two individuals need to communicate in a secure manner. We also implemented two methods for each cipher, encode and decode. The method encode takes the plaintext and produces the corresponding cipher-text and the method decode reverses the process. The students will get a chance to experiment with both methods using different plain-texts and keys and report on the differences between the three ciphers. The students will also have the chance to build on the Alice simulated world by adding new characters and customizing the scenarios.

Laboratory Exercise 2 Symmetric and public key cryptography: In this laboratory exercise, we will use the HTTPS protocol as the case study. This will give us the opportunity to explain the purpose of HTTP and the history of the World Wide Web (interactive learning techniques such as the ones detailed in module 1 will be used in this portion of the lab). We will use the Wireshark network sniffer to capture and analyze all the HTTPS messages exchanged between a local host and a server. The students will then be given detailed instructions that will help them analyze the data captured by Wireshark and write a report about their analysis.

Laboratory Exercise 3 Security principles: This laboratory exercise will consist of two portions. In the first portion of the laboratory exercise, the students will be divided into groups of two or three and given several scenarios where characters need to communicate securely. The groups will then be asked to identify the security principals required for each scenario. In the second portion of the laboratory exercise, the students will be asked to work in groups of two or three and develop their own scenarios and identify the principles required for each of their scenarios. The groups will then share their scenarios with the rest of the class.

2.3 Module 3 - Oh No! I've Been Hacked!

The goal of this module is to educate the students on secure cyber practices. To achieve this, we will cover the main cyber security attacks. The most popular cyber-attacks covered in this module are:

1. SQL injection attacks
2. Cross site scripting attacks
3. Phishing attacks

In this module, we will cover the history and ethics of hacking the Internet and discuss ethical issues related to cyber security. The sessions will consist of very short lectures (less than 5 minutes long) explaining each attack followed by hands on activities. The activities will include using interactive learning games and videos such as Anti-Phishing Phil. The students will also read short articles about cyber-attacks and debate issues related to the ethics of hacking. The sessions will include the following laboratories:

Laboratory Exercise 1- SQL injection attacks: This laboratory exercise consists of two parts. In part 1, the students will learn SQL and practice using it in an emulator that will allow them to create and manipulate tables and records. The second part of the session consists of a hacking exercise where the students will work in groups and use a few simple SQL queries to hack into a site that we have created for this exercise.

Laboratory Exercise 2- Cross site scripting attacks: In this laboratory exercise, we will show the students videos of XSS attacks and guide them through an exercise using a virtual machine. This will give us a chance to talk about the use of virtual machines and their application to cyber security. The students will complete an XSS exercise using the WebGoat[11] application.

Laboratory Exercise 3- Phishing attacks: This laboratory session will consist of two parts. In the first part of the session, the students will use the Anti-Phishing Phil interactive tool, this tool will enable the students to recognize phishing websites and help them learn to always keep good security practices in mind when using the Internet. In the second part of the laboratory session, the students will work in groups on designing a phishing email. The purpose of this exercise is to train the students to pay attention to small details. The groups will then exchange their emails and comment on each other's work.

2.4 Module 4 – What Not to Do on Facebook

This module will include an introduction to social networking and its social, economic, and ethical implications. On completion of this module, the students will be able to:

1. Explain the concept of social networking.
2. Identify positive aspects of social networking.
3. Identify inappropriate, illegal and un-ethical actions on social networking sites.

Outcomes 1 and 2 will be achieved using short introductory presentations on social networking. Outcome 3 will be achieved using a sequence of videos, readings and discussions. The students will be given case studies and asked evaluate whether the actions in the case studies were appropriate, un-ethical or illegal. A sample case study is as follows:

Tina's family is going on a vacation and she is very excited. She posts the following comment on her Facebook status: "We're going on vacation!!!! We're leaving on Monday at 3:30pm and coming back on Saturday at 5:15pm. Hope my plant in my bedroom doesn't die while we're gone!!! LOL!!!"

[11] http://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

In addition, the students will choose articles on social networking and bring them to class for discussion and analysis.

3. WORKSHOP LOGISTICS

This Section gives the logistical details of the outreach program including the schedule, staff and equipment.

3.1 Tentative Schedule

Table 2 gives a preliminary outline for the activities that the students will be involved in every outreach session. The students will be in class for one to two hours during every outreach session (once a month). During the April session, the students will be assigned a group project to work on with the help of the two faculty members and the student mentors. The students will be encouraged to come up with their own project idea and if needed, the faculty and student mentors will help them with develop their ideas, shape them, create a problem formulation and carry out their project and present the results in their posters.

Table 2 Time Outline of Modules and Topics.

Module	Topic	Month
1	History of the Internet and Security The World Wide Web and HTTP	September – October
2	Cryptography Field Trip Using a Programming Environment	November – December
3	Cyber-Attacks Ethics of Cybersecurity	January – February
4	Social Networking	March
Project	Work on Final Project	April
Presentations	Poster Presentations	May

3.2 Middle School Teacher Participation

One of the goals of Cybergirls is to attempt to integrate computer science concepts in the middle and high school curriculum in Indiana. To achieve this, middle and high school teachers will be invited to attend the outreach sessions. We believe that this is a good idea because teachers can not only learn the new material but also observe the student's appreciation for the material. At the end of the program, we will supply materials to the teachers so that they can introduce them to their classrooms.

3.3 Staff

The authors will be the main directors of the Cybergirls outreach program. We will be supported by student mentors from our individual institutions. The student mentors will help students with laboratory exercises and projects, accompany students on the field trip, and manage the Cybergirls website. The mentors will be paid a stipend for participation.

3.4 Equipment and Cost/Funding

We envision that we will need computers for the labs and projects as well as other miscellaneous supplies (poster boards, incentives and gifts, student binders and printouts, and so on). In total, we estimate that we will need $10,000.00 to start the pilot program and a total of $25,000.00 to implement the program in two schools. We have submitted proposals for a few grants and are waiting for a response. We are also in the process of drafting an NSF proposal to cover the cost of the outreach program. Both our institutions have a long history of conducting outreach programs and camps for middle and high school students; we therefore plan to have the presentation day in our institutions.

3.5 Recruitment and Follow-up

We will actively recruit for the program by visiting local middle and high schools and talking to the school officials about the camp. We have shared our program idea with a few school officials and they were all excited about the program and very receptive to the idea. The students will not have to pay any fees to attend the outreach sessions, the entire cost will be covered by the grants.

5. CONCLUSION

This paper presents a new type of outreach program with the goal to attract female students to computing, increase their confidence in hard sciences and entice middle and high school teachers to incorporate some of the program concepts into their curriculum.

REFERENCES

Bush, V. (1945). As We May Think. *Atlantic Magazine*.

Fisher A. and Margolis, J. (2002). Unlocking the Clubhouse: The Carnegie Mellon Experience. *SIGCSE Bulletin, **34**, 2, 79-83*.

Richards, S. (2002). Futurenet: The Past, Present, and Future of the Internet as Told by Its Creators and Visionaries. *John Wiley & Sons, Inc.*

Lee, T. B. L. (2000). Weaving the Web. *Harper Collins*.

Milbourne, L.A. (1999). Encouraging Girls in Science and Math. *The Eric Review K-8 Science and Mathematics Education*, 6(2):45-47.

Groth D. P., Hu, H. H., Lauer B., and Lee, H. (2008). Improving Computer Science Diversity through Summer Camps. *SIGCSE Bulletin* **40**, 1, 180-181.

Nelson J., Turner G., Crittenden, K., and Boudreaux, A. (2009). A Model for High-School Teacher Professional Development and Student Learning. In *Proceedings of the 39th IEEE international conference on Frontiers in Education Conference* (FIE'09). IEEE Press, Piscataway, NJ, USA, 1347-1352.

National Crime Prevention Council (2007). Teens and Cyberbullying, Executive Summary of a Report On Research.