Activity Summary

Girls break into teams of 10 and will complete 4 of the following activities—other activities will be added depending on speaker expertise.

Cell Phone Forensics:

Students will use a SIM card reader to retrieve deleted files from a cell phone. This can lead to a discussion about secure communications or the permanence of digital information.

Cryptography:

Students will decrypt a message using a frequency chart and cryptography wheel. Students will learn the importance of encryption in every day life: UPC, credit card transactions, and texting.

Wireless:

Students will access a wireless data stream and investigate the data. The vulnerability of wireless technologies will be connected to instruction on how to identify safe wireless hotspots.

Robotics:

Students will program a "human robot" to retrieve a package. This activity links to a conversation about the many disciplines required for a successful robotics program including: electrical, and mechanical engineers and mathematicians and computer scientist.

Malware:

Students will perform diagnostics on a machine and find a key logger. Risky behaviors that put student data, information and identities in jeopardy will be explained.

Steganography:

Students will use diagnostic tools and skills to determine if photographs have been altered. Connections to digital forensic investigations will be explored.

Computer Hardware

Students will assemble a computer. Students will name the part and function of each computer part.

Logic

Students will solve logic puzzles use Venn diagrams and make logical arguments. The principals of logic and solving puzzles will be connected to careers that use these skills.

Systems Engineer

Students will review the list of evidence with an system's perspective to analyze what other evidence would be needed to identify the criminal. This connects with the analysis role of the systems engineer.

Cool Careers for Girls in Cybersecurity Summit 2011

Activity Summary

Girls break into forensic teams to complete 4 of the following activities.

Cell Phone Forensics:

Students will use a SIM card reader to retrieve deleted files from a cell phone. This can lead to a discussion about secure communications or the permanence of digital information.

Cryptography:

Students will decrypt a message using a frequency chart and cryptography wheel. Students will learn the importance of encryption in every day life: UPC, credit card transactions, and texting.

Wireless:

Students will access a wireless data stream and investigate the data. The vulnerability of wireless technologies will be connected to instruction on how to identify safe wireless hotspots.

Robotics:

Students will program a "human robot" to retrieve a package. This activity links to a conversation about the many disciplines required for a successful robotics program including: electrical, and mechanical engineers and mathematicians and computer scientist.

Malware:

Students will perform diagnostics on a machine and find a key logger. Risky behaviors that put student data, information and identities in jeopardy will be explained.

Steganography:

Students will use diagnostic tools and skills to determine if photographs have been altered. Connections to digital forensic investigations will be explored.

Computer Hardware

Students will assemble a computer. Students will name the part and function of each computer part.

Logic

Students will solve logic puzzles use Venn diagrams and make logical arguments. The principals of logic and solving puzzles will be connected to careers that use these skills.

Systems Engineer

Students will review the list of evidence with an system's perspective to analyze what other evidence would be needed to identify the criminal. This connects with the analysis role of the systems engineer.