Cool Careers for Girls in CyberSecurity
Penetration Testing

Duration: Each student session last for 20 minutes. Students will have 5 minutes to travel to their next session.

Session Overview:

Students will connect the analysis required for systems engineering to evidence collection for crime investigation.

Objectives:

- Understand the importance of physical security
- Experience a physical analog to the digital practice of breaking through system security measures

Materials/Supplies (include AV needs):

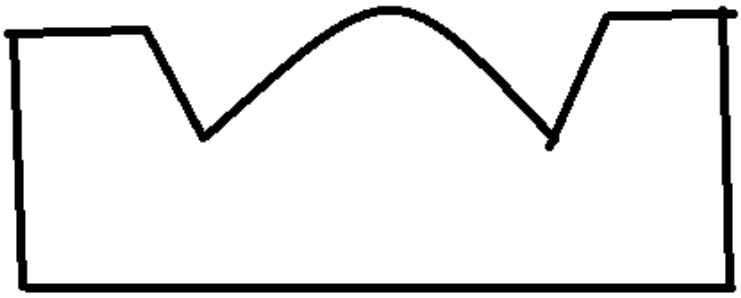
- Soda can
- Scissors
- Locks, usually combination locks

Introduction:

Discuss the legality of penetration testing and lock picking. Penetration testing is legal if you are authorized by an organization or company to test their software or network. It is not legal to practice penetration testing on your family or friends (or any other company/organization) without their permission or knowledge. Lock picking and possession of lock picks differs by state. Having lock picks may be illegal in Washington, DC. You must always have permission of the lock's owner. And remind students to use their powers for good; never evil.

Lesson:

1. Cut off bottom and top ends of the soda can. Trip edges of the remaining rectangle to be smooth.
2. Cut a 2 inch X 2.5 inch rectangle.
3. Cut 2 V's approximately 1 inch deep on one of the long sides of the small rectangle. Space the V's about an inch apart.
4. Cut the center section (between the V cutouts) into a rounded arch.



5. Fold down the edges around the arch and fold up the bottom of the rectangle to make a handle.
6. Wrap the shim around an average size pen or pencil to shape it into a round cylinder at the center (the arched section).
7. Slide the shaped edge down into the space where the lock's spring mechanism is. This is usually on the inner side of the U shape of the lock. For non-combination locks, a shim is needed for each side. Once the shim has been inserted sufficiently far into the locking mechanism, you should be able to simply pull open the lock.

Final Thoughts:

There is usually more than one way in and it does not usually involve digital technology. There is usually an inexpensive method (under $10-$20) to break even the most elaborate security systems.Technologic interventions can only be successful in protecting student identity and data if the student does not engage in risky behavior. Have the students reflect on what behaviors might be risky:

File sharing
Clicking on links
Clicking on attachments
Clicking on pop-up ads
Not using a firewall
Not using and updating the spyware and virus scanning software
Not updating the browser or operating system software

Resources:

- MIT Guide to Lock Picking
  - http://www.blurofinsanity.com/mit/lockpick.html
  - www.lysator.liu.se/mit-guide/MITLockGuide.pdf

- J0hnny Long No-Tech Hacking
- Padlock Shimming
    - http://www.youtube.com/watch?v=fRjNnnLOpmE