Cool Careers in Cyber Security
Lock Picking

Delivery: Can be used as a table demo (hands-on) activity or during a presentation session. Can have materials pre-cut or for older students have them cut their own pattern.

Session Overview:

Physical security

Objectives:

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

Lock picking is the art of unlocking a lock by analyzing and manipulating the components of the lock device without the original key.

Materials/Supplies:

- Soda cans or pre cut soda cans
- Locks. Cheap combination locks work best.
- Markers to draw pattern
- Scissors

Introduction:

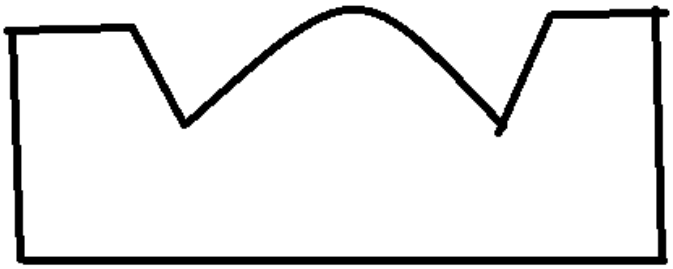
Discuss the legality of lock picking. Lockpicking and safecracking are almost always legal hobbies when you own the lock or safe you are attempting to open. It is not legal to practice lock picking or penetration testing on your family or friends (or any other company/organization) without their permission or knowledge. The legality of possession of lock picking tools differs by state. Having lock picking tools may be illegal in some states. You must always have permission of the lock's owner. Remind students to use their powers for good; never evil.

Scenario:

Physical security is important! Copies of the trade secrets are kept under lock and key.
But how safe is the lock?

Lesson:

1. Cut off bottom and top ends of the soda can. Trim 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.

Resources:

- How to open a padlock with a coke can
  - http://www.youtube.com/watch?v=fRjNnnLOpmE
  - http://www.youtube.com/watch?v=1vDV4G1XXhw
  - http://www.youtube.com/watch?v=EmQMO8U_0G0
- 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

A **penetration test**, occasionally referred to as **pentest**, is a method of evaluating computer and network security by simulating an attack on a computer system or network from external and internal threats.

Final Thoughts:

Points you might want to make:

- 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.
- Make the bridge from lock picking to penetration testing. Discuss the legality of penetration testing. 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.

Recommendations:

How safe is the lock? What recommendations does the team have for physical security access?

Have the students reflect on what behaviors might be risky:
Not password protecting mobile devices
Leaving computers/mobile devices unattended
Not encrypting files (may have to explain encryption)
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