

## Teacher's Instruction Guide

# **Securing Cyberspace Grand Challenge: Multi-Factor Authentication**

Created by Team Snow-in:

David Lam | Leo Betts

Praveen Rammohan | Samuel Temple

Sterling Mitchell | Yuzong Gao

*Table of Contents*

<b>Introduction:</b> .....	1
<b>Budget and Materials:</b> .....	1
<b>Technical Background and Presentation:</b> .....	2
<b>Pre-Activity Instructions</b> .....	2
<b>Activity Instructions:</b> .....	4
<b>Post-Activity Instructions:</b> .....	5
<b>Indiana Standards of Mathematics and Science</b> .....	6
<b>Take Home Message</b> .....	6
<b>Appendix A: Presentation Slides</b> .....	7
<b>Appendix B: Estimated Schedule</b> .....	8
<b>Appendix C: Handout</b> .....	9
<b>Appendix D: Handout Key</b> .....	11
<b>Sources:</b> .....	13

## Introduction:

The focus of our module is to introduce elementary school students to cybersecurity, namely account security. More specifically, our module will focus on the current technological trend that is replacing the traditional password: Multi-Factor Authentication. Multi-Factor Authentication is a method used to control access to an online account by combining knowledge, possession, and characteristic to confirm the user’s identity. We plan to use our activity to help students build the foundations of what makes Multi-Factor Authentication effective.

Our demonstration consists of three main stages: a pre-activity introduction, an activity, and a post-activity conclusion. The pre-activity introduction will educate students on the basics of cybersecurity and account security, relating each to the students where applicable. Next, students will participate in an interactive activity that will build the foundations of Multi-Factor Authentication. Lastly, during the post-activity conclusion, students will recognize the effectiveness of Multi-Factor Authentication and the problem of securing one’s personal account is not only relevant today but also a problem for future generations.

## Budget and Materials:

For 50 students, we recommend a minimum budget of \$25. With the minimum budget of \$25, we recommend getting a combination of gummy bears and hard candies. This has taken into consideration that students may have braces. As for other health concerns, we recommend getting sugar free gummies such. If the budget allows, we also recommend getting a variety pack of candy in order to accommodate for all candy preferences. These estimates do not account for the cost of the printing handouts and providing students with writing utilities. Lastly, these estimates are entirely based on Amazon prices. See *Figure 1* for more details.

**Figure 1: Budget Analysis**

Candy Type	Minimum Budget	Optimal Budget
Gummy Bears	\$14.00	\$14.00
Hard Candies	\$11.00	\$11.00
Variety Pack		\$16.00
<b>Total</b>	\$24.00*	\$41.00*

\* *Shipping and Handling are not included in cost calculations.*

## Technical Background and Presentation:

The Heartbleed Bug, a vulnerability in the OpenSSL library, in 2014 affected multiple institutions. Any institution, both large and small, that used OpenSSL, a widely used encryption tool, was left helpless to even a moderate hacker. This vulnerability allowed a hacker access to private information such as company data, user e-mails and passwords, and much more. [1]

Studies show that security breaches are increasing in both frequency and sophistication [2]. That is, attacks exploiting vulnerabilities, such as the HeartBleed bug, are increasingly exposing more and more users online. Furthermore, a 2013 study by Ofcom, a security firm, found that approximately 55% of all online users have the same passwords across all accounts [3]. That is, if a malicious user obtains a password to one personal account, there is a high probability that all accounts are compromised. For this reason, protecting one's user account is of utmost importance in the current age. As users post more and more private information online, both the users and institutions must be cognizant of account protection.

The proposed Multi-Factor Authentication presentation is in the form of a PowerPoint, which can be found *Appendix A*. The presentation will cover the following:

1. What are the standards of security?

The National Institute of Security and Technology proposed four basic levels of security. The lowest level, level 1, is a state in which the system cannot reliably confirm the user's identity as the account owner. On the other hand, the highest level, level 4, is a state in which the system can confirm the user's identity as the account owner with high confidence. [4]

2. What is Multi-Factor Authentication?

Multi-Factor Authentication is a method of securing a user account based on three properties: knowledge, possession, and characteristic. [4][5]

3. Is Multi-Factor Authentication effective?

Multi-Factor Authentication is an effective method of protecting a user's account. Its strength depends on the number of factors that authenticates the user [4][5]. Regardless if one layer of security is compromised, the user can still reliably control access to their account.

## Pre-Activity Instructions

1. Begin the activity by asking students what they know about cybersecurity. Ask students if they have any accounts such as Facebook, Twitter, YouTube, Playstation, Xbox, etc. Ideally, most students can relate to having an account with an email and password.
2. Now, ask students if they have anything in place that would protect them if someone had gained access to their account. Most likely, students do not have much to protect themselves and they would be upset if they lost access to their established account.

3. To ensure that all students have a proper understanding of account security, use the analogy of a locked door and a key. A locked door is used to prevent unwanted entry into a private area storing precious items and a key controls entry from one end to another. If the key is lost or stolen, the precious items behind the door are likely to be lost or stolen.
4. Once students have a firm understanding of account security and its functions, pass out the attached worksheet. See *Appendix C* and *Appendix D*.
5. Begin the presentation and introduce students to the concept of the levels of security proposed by the National Institute of Security and Technology. Refer to *Appendix A* for this presentation slide. Be sure to use examples and analogies of each and have students fill out the table on the worksheet.
  - a. Level 1 is as if you were walking through the entrance and exit of a supermarket. No one is there to stop you and you are assumed to be there for business.
  - b. Level 2 is what most accounts use: a password. There is some confidence that you are who you say you are if you can enter the password to the right account.
  - c. Level 3 is like having a password and a PIN code. If you can correctly type in the password and PIN code each time you login, there is a higher confidence that you are the owner of this account.
  - d. Level 4 is a stage where there is absolute confidence in the user's identity. Imagine your typical spy action movie. Usually, top secret information is behind some hallway that scans the entire body of an individual; there may be a retinal scan, voice confirmation, and many other things.
6. Ask the students to brainstorm ways to protect an account and write them on the worksheet. Encourage students to be creative. It does not have to be implemented in the real world but at least plausible (Example: To gain entry into a clubhouse, a member must perform a secret knock on the door while saying the password in a certain melody). See *Figure 2* for actual student generated ideas.

**Figure 2: Actual Student Ideas**

long complicated passwords with lots of numbers and symbols  
Use words that are rarely used such as "xylphone"  
Have many passwords  
Fingerprint  
Blood  
Voice  
Eye scan  
Footprint  
PIN

7. After three minutes, ask students to share their answers and write them on a whiteboard/projector (see *Figure 2*). To encourage participation, give each student that answers a piece of candy (if the budget allows). Once you have a sizeable list, ask the students to write down what they think are the top 3 security measures.

### Activity Instructions:

1. Divide the teams into groups of around 3-6 members, depending on the size of the class. We recommend having at least 3 teams; however, it is possible to do this with 2. Assign each team a number.
2. Tell the students that they need to be able to create a **text-only** password that will be used to guard a pile of candy that belongs to the team. Each team member will need to be able to remember this password. They can write it down if they wish. Be sure to inform each student to keep their passwords appropriate and there will be a penalty if they are unable to memorize their own password.
3. Once a team has created their password, they should tell the instructor, who will keep track of each team's password, quietly. They have 8 minutes to do this. Announce after each minute the time they have left. To stimulate ideas, the instructor and/or assistance may walk around from group to group (have someone waiting for passwords to keep track of). Be sure that each team member is participating.
4. Once all teams have submitted a password, re-assign one member of each team to a new team. This way, each of the new teams will know the password of another team. [Go to slide 2 of the presentation at this time.] Inform each team that they are not allowed to change their password but may add onto it. For example, with a password, a team may require a member to rub their stomach while saying their password to access their candy stash. Be sure to inform students that these will later be done by a randomly selected teammate in order to access their stash of candy. Make sure students keep their security measure simple (no fingerprint being read, blood drawn, or any other extensive security measure). Inform the students that they are permitted to spy on other teams. Once they have a set of security measures, have them send one representative to the instructor who will take note of their security measures. They will have 10 minutes to do this. Be sure to announce after each minute how much time is left. Again, instructors and/or assistants are encouraged to walk from group to group to stimulate ideas. Be sure to have someone ready to take note of these new security measures.
5. To keep track of each team's candy stash, assign each group a point value. Each point represents one piece of candy per student. We recommend 4 points to start for a sizeable group, but this may vary. The students will not know the candy-to-point ratio. Inform the students that the more points their team earns, the more candy they will receive. To earn a point, a student may make use of his or her observations and collaborate between teams (trade information with teams who have successfully breached another team's stash or collaborated with former teammates) to guess the other team's password and security measure. Once they have a guess, they will come up to the instructor and state their team number, the defending team's number, and the password and security measure of the

defending team's (they must perform it, not say it). If they are correct, the defending team loses a point and the attacking team gains a point. If they fail, there are no penalties except that they cannot guess again until another team has guessed (this can be changed if there are too few teams or too few guesses). Note, students from other teams are encouraged to observe these attempts also.

6. At the end of the game, a randomly chosen member of each team will have to use their own password and security measures to access their own candy stash. If this member cannot recall their team's password and security measure correctly, their team will lose one point (each member gets one less piece of candy).
7. Announce the scores of each team and award the appropriate amount of candy. It is intended that no one will score a point if the security measures are done well.

### **Post-Activity Instructions:**

1. Conclude the module by asking the students about how the game went. Discuss the strategies of the successful teams (if there were any), and link any of these strategies to real life strategies commonly used in cybersecurity. For example, teams were allowed to eavesdrop. Link this with how cyber criminals commonly attempt to listen in on network traffic between two hosts and obtain sensitive information. If there were no successful teams, ask why it was difficult and what made it difficult. The answer should revolve around the idea that students were given a large pool of possibilities for their security measure and it is difficult to guess the security measures even if the password itself was compromised.
2. [Go to slide 3 of the presentation at this time.] Now, introduce Multi-Factor Authentication to the students and explain that they had been using it throughout the activity. Have the students write down the definition of Multi-Factor Authentication on the worksheet. Be sure to give examples of knowledge (password, PIN, security question answer), possession (cellphone, key, card), characteristic (fingerprint, eyes, voice). Also note to the students that Multi-Factor Authentication meets all levels of security depending on the number of factors used.
3. Next, ask students to predict the results of the game if they were to play it again. Give them some time to write their responses on the worksheet.
4. Explain a likely answer is that the game will end with varying scores for each team every time it is played because teams will get better at both protecting their candy and getting into each other's candy stashes. Link this with the idea that cybersecurity is constantly evolving.
5. Lastly, end the module by asking them to answer the concluding question on the worksheet to help ensure that they understand the lesson of the module. If someone disagrees ask them why. For example, having more and more security measures requires an individual to be able to recall each of them. If the individual is unable to, there is an obvious penalty as Multi-Factor Authentication is rendered useless.

---

## **Indiana Standards of Mathematics and Science**

Our module focuses on fulfilling several elements of the Indiana Standards of Mathematics and Science. Within the Standards of Mathematics, this module focuses on Problem Solving and Reasoning and Proof.

Students are given a task: protect their candy stash. To accomplish this, students must discuss with their teammates and determine what makes a strong password and security measure. In addition, students are able to test their results as they attempt to decipher other team's security measure. Lastly, students will then recognize that they had been using the basic ideas of Multi-Factor Authentication. In the end, students will be given a problem in which they develop a solution and test the results.

In addition, our module also follows the Communication standards. Our activity requires high levels of engagements. Students are obligated to communicate with their whole team during the design of the passwords and additional security measures as a randomly selected team member will be chosen to present their security solution once the activity is over. Furthermore, students are encouraged to collaborate with the opposing teams to gain and trade information.

Furthermore, our module also supports the Scientific method. Before the activity, students will brainstorm ideas to protect something of high importance. They will then hypothesize what security measures are the most effective. Their hypothesis will then be tested throughout the activity with the results being determined by the scores of each team. Once the activity is over, students will predict what the results will be if the activity were to be done again. We then conclude that Multi-Factor Authentication is a strong security measure.

### **Take Home Message**

After going through this activity, the students will have some knowledge of cybersecurity and the risks associated with it. They will understand Multi-Factor Authentication and how it is applied today in the cyber world. Students will understand how to protect their accounts beyond the traditional password. Lastly, this activity will inspire students to consider their future career and educational choices; they can be the engineers or computer scientists that solve the grand challenges of tomorrow.

The completion of the worksheet and the activity will instill the following concepts:

1. The different levels of security
2. How different security measures meet different levels of security
3. The definition of Multi-Factor Authentication and how it applies to cybersecurity
4. How issues of cybersecurity is relevant to them

## Appendix A: Presentation Slides

### Level Standard of Security

Level	Security	Description
Level 1	Low	System has no confidence in user's identity.
Level 2	Medium	System has some confidence in user's identity.
Level 3	High Medium	System has moderate confidence in user's identity.
Level 4	High	System has high confidence in user's identity.

### Rules:

- Make new security measures
- Passwords cannot be changed
- Spy on other teams to learn their security measures
- Collaborate with former teammates and other teams
- Trade information
- Go up to the instructor when you are ready to guess another team's password

#### Multi-Factor Authentication:

a method to control access to an account using three properties: knowledge, possession, and characteristic.

Something You Know



Something You Have



Something You Are



*Brain Picture: [6] | Phone Picture: [7] | Fingerprint Picture: [8]*

**Appendix B: Estimated Schedule**

<b>Scheduled Activity</b>	<b>Expected Time</b>
Introduction	15 minutes
Worksheet and Brainstorming	5 minutes
Password I Activity	8 minutes
Rearrange Teams	2 minutes
Making Security Measures	10 minutes
Cracking Security Measures	10 minutes
End of Activity	5 minutes
Worksheet Time and Conclusion	10 minutes
<b>Total</b>	<b>65 minutes</b>

---

**Appendix C: Handout**

Name: \_\_\_\_\_

Fill in the table below:

Level	Security	Description
Level 1		
Level 2		
Level 3		
Level 4		

**Hypothesize:** List what you think are good security measures.

**Predict:** Choose the top 3 from the board

**Post-Activity**

Define Multi-Factor Authentication:

**Predict:** the results of subsequent runs of the activity. Will the scores be similar, equal, or more unequal?

**Conclude:** Is Multi-Factor Authentication a strong security measure? Explain why or why not using the results from the activity and above questions.

**Appendix D: Handout Key**

Name: key

**Fill** in the table below:

Level	Security	Description
Level 1	Low	System has no confidence in user's identity.
Level 2	Medium	System has some confidence in user's identity.
Level 3	High Medium	System has moderate confidence in user's identity.
Level 4	High	System has high confidence in user's identity.

**Hypothesize:** List what you think are good security measures.

- Complicated passwords
- Linking it to other accounts
- Require a PIN
- Have caps and numbers
- Biometrics

**Predict:** Choose the top 3 from the board

*Up to student*

## Post-Activity

Define Multi-factor Authentication:

Method to control access to an account using three properties: knowledge, possession, and characteristic. (Something you know, something you have, something you are)

**Predict:** the results of subsequent runs of the activity. Will the scores be similar, equal, or more unequal?

*Lead students to the idea that students will likely get smarter in their guesses (attacks) and adapt to the changing situation to note that Cybersecurity is constantly changing.*

*Ideally, the scores should be similar.*

**Conclude:** Is Multi-Factor Authentication a strong security measure? Explain why or why not using the results from the activity and above questions.

*Up to the students. (Ideally, yes but this should generate discussion)*

## Sources:

[1] Codenomicon, "The Heartbleed Bug", 2014. [Online]. Available: <https://heartbleed.com/>. [Accessed: 06- Feb- 2016].

[2] J. Parns, "Prepare for the Worst: How to Create a Cyber Security Incident Response Plan", 2016. [Online]. Available: <https://www.business.com/internet-security/prepare-cyber-security-incident-response-plan/>. [Accessed: 06- Feb- 2016].

[3] G. Cluley, "55% of net users use the same password for most, if not all, websites. When will they learn?", 2013. [Online]. Available: <https://nakedsecurity.sophos.com/2013/04/23/users-same-password-most-websites/>. [Accessed: 06- Feb- 2016].

[4] J. Kim and S. Hong, "A Method of Risk Assessment for Multi-Factor Authentication", *Journal of Information Processing Systems*, vol. 7, no. 1, p. 187-198, 2011.

[5] Amazon Web Services, "Multi-Factor Authentication", 2016. [Online]. Available: <https://aws.amazon.com/iam/details/mfa/>. [Accessed: 06- Feb- 2016].

[6] K. Kokelj, "Education brain head icons". 2014.

[7] GSMArena, "Iphone 5". 2012.

[8] Psdfinder, "Fingerprint icon (PSD) - PSDfinder.com". 2015.