**Aa**

**CyberQuest**

Camp Curriculum

Ages: 13-15



Developed for CSS 496

Authored by Kristina Chen

**Table of Contents**

[**Camp Details**](#_hwdnd3vnnkpb) **—----------------------------------------------------------**

**Camp Marketing —------------------------------------------------------------------**

**Theme —-------------------------------------------------------------------------------**

**Goals, objectives, audience, purpose —----------------------------------------**

**Narrative —----------------------------------------------------------------------------**

**Weekly Overview —-----------------------------------------------------------------**

[**MONDAY**](#_obv3u26uwhvm) **—----------------------------------------------------------------**

**Goal —-----------------------------------------------------------------------------------**

**Objectives —--------------------------------------------------------------------------**

**Schedule —----------------------------------------------------------------------------**

[**TUESDAY**](#_4uxk2ijsk4mc)  **—--------------------------------------------------------------**

**Goal —-----------------------------------------------------------------------------------**

**Objectives —--------------------------------------------------------------------------**

**Schedule —----------------------------------------------------------------------------**

[**WEDNESDAY**](#_q8yee17p09v5)  **—----------------------------------------------------------**

**Goal —-----------------------------------------------------------------------------------**

**Objectives —--------------------------------------------------------------------------**

**Schedule —----------------------------------------------------------------------------**

# Camp Details

Camp Marketing Description

Uncover the case of fraud and deception as our friend Sam discovers his credit card information has been compromised. Explore how Sam was deceived. Then learn about how his hacker was able to exploit Sam for his information. Lastly follow the steps of our Cybersecurity hero, Amelia, who was able to recover Sam’s funds

****

Figure 1: Marketing Logo for CyberQuest

Theme:

Internet safety, online engagement, behavior management, information security

Goals:

* To help teens become aware of their own online behavior
* Develop teen knowledge on technical literacy & information security
* Inspire some teens to look into careers in information security

Objectives:

* Recognizing the importance of cybersecurity professionals
* Develop / communicate ways they themselves can engage online safely in their own life
* Be able to identify areas in which they themselves or those around them are vulnerable online.

**Audience:**

12-15 year olds (preteen - young teens)

**Purpose:**

To get students thinking about their engagement with technology, how they can keep themselves safe online, and get them aware of how security specialists work to keep us safe.

Narrative:

Our main character Samuel (18 y/o) has recently discovered he was the target of a scam when his login information for his shopping account was stolen. On our first day our students discover the fraud.

On our second day we will then look into the perspective of Stanley (the hacker) who’s a casual hacker just looking to make some quick money from Sam’s account. Students will learn about different types of hackers and different tools they may use to steal our information.

Lastly on the final day we will look through Talia (our cybersecurity specialist) who’s helping Sam secure his information. On this last day students will learn about ways these professionals help save victims and prevent other potential scams.

Note:

The below figure is created to help direct Educator visualization of the camp week

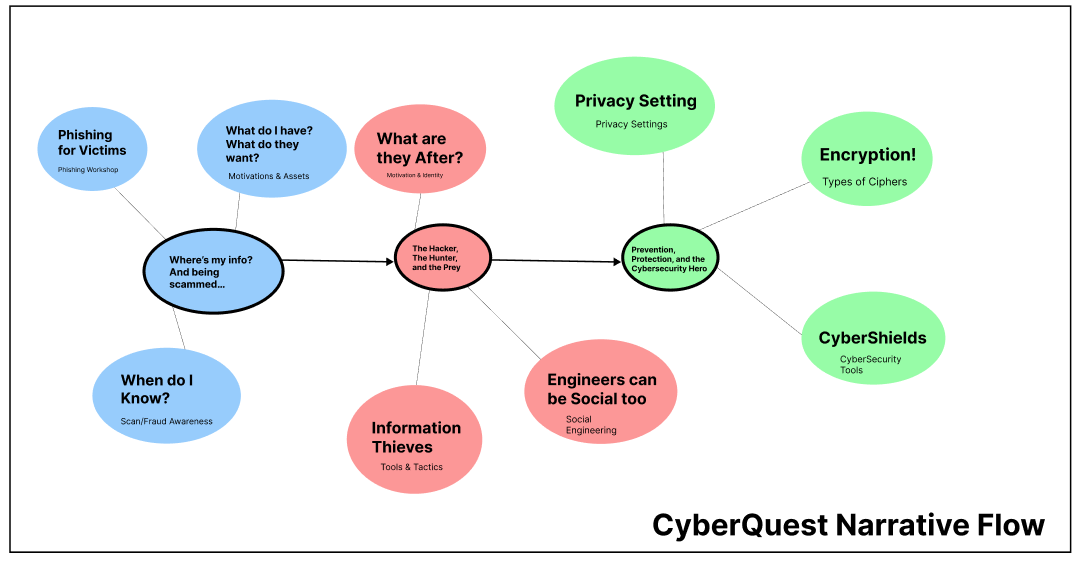
****

Figure 2: CyberQuest Narrative FLow

Overview of the Week

| Day 1 | The lost, the Thief, and the Journey |
| --- | --- |
| Day 2 | The Hacker, The Hunter, and the Prey |
| Day 3 | Prevention, Protection, and the Cybersecurity Hero |

Educator Notes:

* The curriculum goes by a story-line thus the activities introduced need to primarily stay in the same order, however if needed activities could be swapped by connecting or tweaking said storyline to match.

# Monday | The lost, the Thief, and the Journey

Goal:

* Develop awareness of where we engage with digital information
* Teens will be able to recognize possible fraud scenarios and what behaviors enable attackers to seize their information

Objectives:

Schedule

| **Activity** | **Time** |  |
| --- | --- | --- |
| [Drop Off + Name tags](#_4h22e76wppi2) | 30 | 8:45-9:15 |
| [WhatApp? (Ice Breaker)](#_ccvy7vm8srl5) | 30 | 9:15-9:45 |
| [Expectations](#_6lkoc2vl0j5v) | 15 | 9:45-10:00 |
| [Snack](#_19lfg19qiixy) | 15 | 10:00-10:30 |
| [Opening Narrative](#_o3umgnp7m239) | 45 | 1030-11:15 |
| [PWNED!!](#_i8k6eztbo4j5) | 30 | 11:15-12:00 |
| [Lunch/Recess](#_4ffsykscz32n) | 60 | 12:00-1:00 |
|
| [Password Manager](#_286laomu8ukq) | 45 | 1:00-1:45 |
| [Phishing for Victims](#_w8msovexxgbg) |  |  |
|
| [Snack](#_r5k50iuewl8w) | 15 | 2:45-3:00 |
| [Who are we on the WWW?](#_c9nq986fxo9b) | 30 | 3:00-3:30 |
|
| [Clean-Up](#_khy21hotrtyx) | 15 | 3:30-3:45 |

**Bolded Activities are Key Activities to the CyberQuest Narrative Curriculum**

# Tuesday | The Hacker, The Hunter, and the Prey

Goal:

* Develop awareness of where we engage with digital information
* Teens will be able to recognize possible fraud scenarios.

Objectives:

| **Activity** | **Time** |  |
| --- | --- | --- |
| Drop Off | 30 | 8:45-9:15 |
| Opening Narrative | 45 | 9:15-10:00 |
|
| Snack | 15 | 10:00-10:15 |
| Motivation of the Hunter / Hacker | 45 | 10:15-11:00 |
|
| Engineers can be Social too! | 60 | 11:00-12:00 |
|
| Lunch/Recess | 60 | 12:00-1:00 |
| Infiltrating the Perimeter | 60 | 1:00-2:00 |
|
| Snack | 15 | 2:00-2:15 |
| Viruses and other Illnesses | 45 | 2:15-3:00 |
|
| Clean-Up | 30 | 3:00-3:30 |
| Drop Off | 30 | 8:45-9:15 |

**Bolded Activities are Key Activities to the CyberQuest Narrative Curriculum**

# Wednesday | Prevention, Protection, and the Cybersecurity Hero

Goal:

* Develop awareness of where we engage with digital information
* Teens will be able to recognize possible fraud scenarios.

**Objectives:**

| **Activity** | **Time** |  |
| --- | --- | --- |
| Drop Off | 30 | 8:45-9:15 |
| Opening Narrative | 45 | 9:15-10:00 |
|
| Snack | 15 | 10:00-10:15 |
| CyberShields | 45 | 10:15-11:00 |
|
| Privacy Setting | 60 | 11:00-12:00 |
|
| Lunch/Recess | 60 | 12:00-1:00 |
| Encryption! | 60 | 1:00-2:00 |
|
| Snack | 15 | 2:00-2:15 |
| Deploying our Defenses! | 45 | 2:15-3:00 |
|
| Clean-Up | 30 | 3:00-3:30 |
| Drop Off | 30 | 8:45-9:15 |

**Bolded Activities are Key Activities to the CyberQuest Narrative Curriculum**

# Monday

# The lost, the Thief, and the Journey

Schedule

| **Activity** | **Time** |  |
| --- | --- | --- |
| [Drop Off + Name tags](#_4h22e76wppi2) | 30 | 8:45-9:15 |
| [WhatApp? (Ice Breaker)](#_ccvy7vm8srl5) | 30 | 9:15-9:45 |
| [Expectations](#_6lkoc2vl0j5v) | 15 | 9:45-10:00 |
| [Snack](#_19lfg19qiixy) | 15 | 10:00-10:30 |
| Opening Narrative | 45 | 1030-11:15 |
| PWNED!! | 30 | 11:15-12:00 |
| Lunch/Recess | 60 | 12:00-1:00 |
|
| Password Manager | 45 | 1:00-1:45 |
| Phishing for Victims | 60 | 1:45-2:45 |
|
| Snack | 15 | 2:45-3:00 |
| Who are we on the WWW? | 30 | 3:00-3:30 |
|
| Clean-Up | 15 | 3:30-3:45 |
| Pick Up (Depends on Location) | 15 | 3:45-4:00 |

**Bolded Activities are Key Activities to the CyberQuest Narrative Curriculum**

## Teacher Notes:

## Drop-Off + Name tags + Camp Shirts

Objective: Students will be coming in for the morning, since this is the first morning, have them write name-tags and socialize amongst each other.

In addition it may help to engage campers with a question of the day!

Materials:

| D |  | Sign, PacSci branded | 1 | 1/camp |  |
| --- | --- | --- | --- | --- | --- |
| C |  | Pen, Wet Erase | 1 | 1/camp |  |
| C |  | Tape, Blue (roll) | 1 | 1/camp |  |
| C |  | Index Cards | 20 | 1/camper |  |
| C |  | Sharpie | 1 | 1/camp |  |
| C |  | Crayons, assorted colors (gallon) | 0.5 | 0.5/camp |  |

Time Required:

30 minutes

Process:

*Drop off & Name Tags*

1. Prepare a piece of paper at each seat for campers to write names once they have found a seat.
2. Write your camp name on a PacSci branded sign if a printed one is not available.
3. Check in campers, welcoming each one, and confirming information with parents including:
   1. Medical/behavioral notes (allergies, specific needs, tips)
   2. Lunch - If they brought/will need a lunch; if they paid for one this week
   3. Kid code confirmation
   4. Extended Care – are they signed up for AM and/or PM care?
   5. Releases - photo, med form/first aid, sunscreen/bug spray
4. Bring 10 campers inside with one educator while the other stays until 9:10 for late drop offs.

Educator Notes:

* Prepare blue tape with camper names. **DO NOT** write camper names on camp tees, as some parents don’t wish to have their child’s name on these tees after camp.
* Some great questions to start the day could include. (Try to cater it to the day’s theme)
  + “Have you heard of cybersecurity? What do you know?”
  + “Have you encountered scam mails?”
  + “What sort of apps have you used?”
* It’s helpful to have a fun fact on the board as well as a schedule to let campers know what to expect.

## Ice-breakers: WhatApp?

Purpose:

Engage students and familiarize them with their classmates. For this icebreaker we will have students gear their thinking towards the main theme of the camp.

Lesson Duration:

15-30 minutes

Lesson Outline:

What Apps?

1. Count off campers as 1(s) and 2(s)
2. Have group 1 form a circle, then group 2 form an outer circle.
3. Once each camper has a pair, have them:
   1. Introduce themselves
   2. What they’re excited to learn from this camp
   3. Discuss what application “apps”they may use.
   4. Have them talk about maybe what sort of information they might have to use to create an account on those apps.
   5. Then have them discuss why they use such an application?
      1. Entertainment? Shopping? Education? Etc.
4. Then have the outer circle rotate to their right, then they will have a new partner.
5. Repeat steps 3-5 at least 2 more times

Reflection

Gather all campers into a circle again

## Expectations (~15 minutes)

## Snack Break (~30 minutes)

## Opening Narrative

Purpose:

To introduce students to a narrative where our friend “Sam” finds out he is hacked. In addition we introduce the topics of camp such as introducing information security concepts and what it means to be online safely.

Lesson Duration:

30-45 minutes

Lesson Outline:

Educators will go ahead and introduce the theme/narrative of the class with a presentation linked [here](https://www.canva.com/design/DAGFXxOUMxo/Q8tzl2oVPzi8LGc0wsJ4SQ/edit?utm_content=DAGFXxOUMxo&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton)

After this presentation educators will lead into the discussion about how we as individuals may get hacked. In addition we will introduce different types of malware and what a virus vs malware actually means.

Educator Notes:

* Educators please clarify to student the meaning of encryption (in simpler terms for today’s lesson)
* Pulling up different types of malware and introducing differences and similarities could be interesting. Educators will need to do additional research prior to differentiate the different terms.

## PWNED!

Purpose:

For this lesson we will move on from malware to finding out how else Sam could’ve discovered ways his devices could’ve been breached.

Lesson Duration:

15-30 minutes

Lesson Outline:

1. For this lesson we will be introducing students to the meaning of being “pwned”
2. Then project your computer and go to the following [site](https://haveibeenpwned.com/) (haveibeenpwned)
3. Once on this site, discuss the purpose of this site and give a demonstration of finding out if their email has been “pwned”.
   1. This simply involves putting a password in.
4. Then feel free to discuss recent breaches and the other resources on this site.
5. Lastly, have students themselves input their own emails and explore the site themselves!

Educator Notes:

* Educators please look up what “pwned” means to better explain and understand student questions
* The better security drop-down after using your email on the pwned site will be a great leadway to our next discussion on password protection!

## Lunch Break (~60-90 minutes)

## 

## Password Manager

Purpose:

* Teach students about the importance of secure login credentials.
* Introduce password managers as a solution for managing multiple passwords effectively.

Lesson Duration:

45 minutes

Lesson Outline:

1. Introduction (10 minutes)
   * Explain why passwords are essential for online security.
   * Discuss common challenges related to remembering and managing passwords.
2. What Is a Password Manager? (15 minutes)
   * Define what a password manager is.
   * Highlight the benefits of using password managers (e.g., convenience, security).
   * Mention popular password manager tools like [1Password](https://1password.com/haveibeenpwned/goodnews/), [LastPass](https://www.lastpass.com/?utm_source=google&utm_medium=cpc&utm_campaign=19546987156&utm_term=lastpass&utm_content=146499740633&gad_source=1&gclid=CjwKCAjwo6GyBhBwEiwAzQTmcyglHd0wi7VmypGcxZZvnz9rRY0HAFHAPnoOolJRDckF-3b3gKoaHRoCbikQAvD_BwE), [BitWarden](https://bitwarden.com/go/password-management-business-sales/?utm_source=google&utm_medium=cpc&utm_campaign=AW_USCA_NU_CL_Bitwarden_en_GSN_DTMB_Brand_KW:Brand_Exact&utm_content=591476247789&utm_term=bitwarden%7Ckwd-947848666764&hsa_acc=2567950947&hsa_cam=10358965841&hsa_grp=103286805535&hsa_ad=591476247789&hsa_src=g&hsa_tgt=kwd-947848666764&hsa_kw=bitwarden&hsa_mt=e&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=CjwKCAjwo6GyBhBwEiwAzQTmc5slHEVIVJJJfRLCOopRbqDuF7J3ZI7k1qvYPAeJ5QkM8stYpzfXCxoC-LQQAvD_BwE) (plugin).
3. How Password Managers Work (10 minutes)
   * Describe the process of setting up and using a password manager.
   * Show examples of password manager interfaces.
   * Emphasize the importance of a strong master password.
4. **Practice and Hands-On Activity (10 minutes)**
   * Have students create a simple password using the “Dos and Don’ts” tips discussed earlier.
   * [Share their new passwords with the group](https://www.tesd.net/cms/lib/PA01001259/Centricity/Domain/999/powerfulpasswordslesson.pdf). [Emphasize, not to do this on a regular case]
   * Have students try using one of the listed password managers!
5. Security Considerations (5 minutes)
   * Address common questions:
     + What if the password manager company gets compromised?
     + How does trusting a password manager compare to not using one?
6. Conclusion (5 minutes)
   * Recap key points.
   * Encourage students to explore password managers for their personal use.

## Phishing for Victims

Purpose:

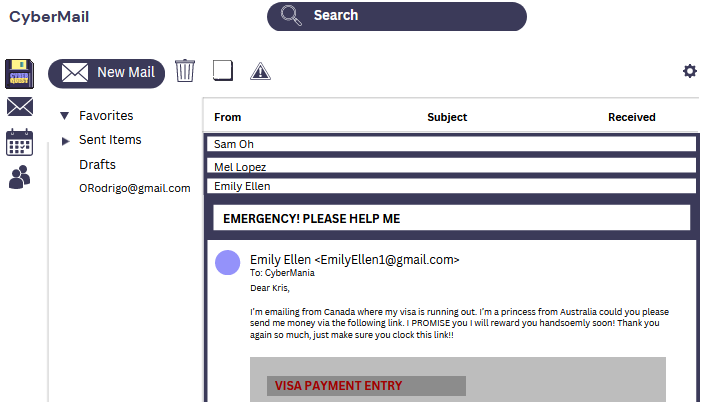
* Develop youth awareness of the possibility of phishing attacks, especially in terms of opportunities that are “too good to be true”
* Adjust attitude towards scams and develop a habit of checking for phishing possibilities.

Lesson Duration:

60 minutes

Lesson Outline:

1. Ask students what they know about phishing? What is the purpose of phishing?
2. Then once they answer and discuss amongst themselves, define phishing formally and introduce them to why scammers perform phishing attacks and where they may see it.
3. Play this [video](https://www.youtube.com/watch?v=a9Q6wHwdKlo) for visual presentation
   1. 0:00-3:09 - What is scam & fraud
   2. 3:10-9:00 - Tips on spotting phishing
4. Then introduce the phishing activity on this [site](https://phishingquiz.withgoogle.com/)
5. Direct students to CyberQuest’s website for additional practice and information
6. Once some online practice has been done, have students then sit in groups, 4 per table and hand out print out copies of the Phishing Emails Activity
7. Lastly once all groups have finished the activity, pull students in for a group discussion where they point out what made them believe an email was a phishing attack versus what may have seemed legitimate.

Ex) 

## Snack Break (~30 minutes)

## 

## 

## Who Are We on the World Wide Web?

Purpose:

* Empower teens with knowledge to act responsibly on social media.
* Develop awareness of harmful behaviors on social media
* Explore the concept of online identities and the risks at hand in the digital world.

Lesson Duration:

30 minutes

## Lesson Outline:

1. Introduction (~ 10 minutes)
   1. Begin by discussing the concept of online identity. Ask students: “Who are you on the internet?” Encourage them to share their thoughts.
   2. Explain that our online presence shapes how others perceive us and impacts our safety. Introduce the idea that we wear different “masks” online.
2. Activity: Digital Masks (~15 minutes)
   1. Distribute index cards or sticky notes to each student.
   2. Ask students to write down three aspects of their online identity (e.g., interests, hobbies, favorite platforms).
   3. Then, have them flip the card and write down three things they keep private (e.g., personal information, passwords).
   4. Discuss as a class: How do these aspects create their digital masks? How can they balance authenticity and privacy?
3. Understanding social media risks (~ 10 minutes)
   1. Present common risks associated with social media:
      1. Oversharing personal information
      2. Cyberbullying
      3. Identity theft
      4. Privacy settings
   2. Show real-world examples (without revealing personal details) to emphasize the importance of caution.
4. Interactive Video Scenario (~4 minutes)
   1. Play this [video](https://www.youtube.com/watch?v=DiI8Lj0_TGQ)
      1. Have students discuss in groups what they think about the video. What parts can they agree or disagree with? Why do they agree or disagree? Do they have online friendships?
5. Overall Reflection
   1. Have students reflect on their own online behavior. Ask: “What changes will you make to protect your online identity?”
   2. Encourage them to commit to at least one action (e.g., reviewing privacy settings, being mindful of posts).

## Prepare for Pick-Up / Pick Up (15-30 minutes)

## 

# Tuesday

# The Hacker, The Hunter, & the Prey

Schedule

| **Activity** | **Time** |  |
| --- | --- | --- |
| Drop Off | 30 | 8:45-9:15 |
| Opening Narrative | 45 | 9:15-10:00 |
|
| Snack | 15 | 10:00-10:15 |
| Motivation of the Hunter / Hacker | 45 | 10:15-11:00 |
|
| Engineers can be Social too! | 60 | 11:00-12:00 |
|
| Lunch/Recess | 60 | 12:00-1:00 |
| Infiltrating the Perimeter | 60 | 1:00-2:00 |
|
| Snack | 15 | 2:00-2:15 |
| Viruses and other Illnesses | 45 | 2:15-3:00 |
|
| Clean-Up | 30 | 3:00-3:30 |

**Bolded Activities are Key Activities to the CyberQuest Narrative Curriculum**

## Teacher Notes:

## Drop-Off

Purpose: Students will be coming in for the morning, since this is the first morning, have them write name-tags and socialize amongst each other.

In addition it may help to gear them towards the theme by introducing a question of the day.

Lesson Duration: 30 minutes

Materials:

* Clipboard
* Classroom roster
* Tablet (w/ Campdoc signed in)

Educator Notes:

* Some great questions to start the day could include. (Try to cater it to the day’s theme)
  + “Have you heard of cybersecurity? What do you know?”
  + “Have you encountered scam mails?”
  + “What sort of apps have you used?”
* It’s helpful to have a fun fact on the board as well as a schedule to let campers know what to expect.

## Opening Narrative (Tuesday)

Purpose:

Kicking off our second day of CyberQuest we recap what happened yesterday to Sam and the ransomware. Then we bring the conversation into the perspective of Stanley, who is the cyber criminal.

Then we move onto discussing what defines a hacker and their motivations.

Lesson Duration:

30-45 minutes

Lesson Outline:

1. Educators will go ahead and introduce the theme/narrative of the today’s class with a presentation linked [here](https://www.canva.com/design/DAGFXxOUMxo/Q8tzl2oVPzi8LGc0wsJ4SQ/edit?utm_content=DAGFXxOUMxo&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton) (Slides 5-10)
2. After this presentation educators will lead into the discussion about different types of hackers. Then ask the students what type of hacker they believe Stanley is.
   1. This is a good time for students to share their experiences with hackers or what they’ve seen in pop culture today about hackers!

Educator Notes:

* Educators please clarify to student the meaning of encryption (in simpler terms for today’s lesson)

Pulling up different types of malware and introducing differences and similarities could be interesting. Educators will need to do additional research prior to differentiate the different terms.

## Snack Break

## 

## Motivation of the Hunter

Purpose:

The purpose of this lesson is to help students understand the various motivations behind hacking activities. By exploring different hacker profiles and their underlying reasons, students will gain insights into the cybersecurity landscape and learn how to protect themselves online.

Lesson Duration:

~45 minutes

Lesson Outline:

* Ask the students for a raise of hands to define what they know about hackers and why they think they do what they do.

Educator Notes:

## Information Thieves!

Purpose:

Lesson Duration:

~45 minutes

Lesson Outline:

Educator Notes:

## Lunch / Recess

## Engineers can be Social too!

Purpose:

The purpose of this lesson is to raise awareness among teenagers about the risks associated with social engineering. By recognizing common tactics used by attackers, students can better protect themselves and their personal information.

Lesson Duration:

~60 minutes

Lesson Outline:

1. Introduction (10 minutes)
   * Define social engineering and its impact on individuals and organizations.
   * Discuss real-world examples (e.g., phishing emails, phone scams).
2. Types of Social Engineering Attacks (15 minutes)
   * Present different forms of social engineering:
     + Phishing: Deceptive emails or websites that trick users into revealing sensitive information.
     + Vishing: Voice-based attacks that exploit phone communication.
     + Smishing: SMS-based attacks using text messages.
   * Explain how attackers manipulate human behavior.
   * [Video Example](https://www.youtube.com/watch?v=PWVN3Rq4gzw)
3. Common Tactics (10 minutes)
   * Explore tactics used by social engineers:
     + Pretexting: Creating a fabricated scenario to gain trust (e.g., posing as a bank representative).
     + Tailgating: Following someone into a secure area without authorization.
     + Baiting: Offering something enticing (e.g., free software) to lure victims.
4. Recognizing Red Flags (5 minutes)
   * Discuss warning signs:
     + Urgency or fear tactics in messages.
     + Unexpected requests for personal information.
     + Unsolicited phone calls or emails.
5. Protective Measures (5 minutes)  
   Teach students how to protect themselves:
   * + Verify the legitimacy of requests.
     + Be cautious with sharing personal details.
     + Use strong, unique passwords.
6. Discussion and Reflection (5 minutes)
   * Engage students in a discussion:
     + Share any experiences related to social engineering.
     + Brainstorm ways to stay vigilant online.

Educator Notes:

* Catfishing is another tactic that comes with social engineering, this may be more applicable to teens who often engage in friendships online

## Snack Break

## Viruses & Other Illnesses

Purpose:

The purpose of this lesson is to educate teenagers about various types of malware, their characteristics, and the importance of cybersecurity awareness. By the end of this lesson, students will be able to recognize common malware threats and take preventive measures.

Lesson Duration:

~60 minutes

Lesson Outline:

1. Introduction (10 minutes)  
   Define malware and its impact on computer systems.
   * Discuss the relevance of understanding malware for personal safety.
2. Common Types of Malware (20 minutes)
   * Present the following types of malware:
     + Viruses: Self-replicating code that attaches to legitimate files and spreads.
     + Worms: Standalone programs that replicate and spread across networks.
     + Trojan Horses: Disguised as legitimate software but perform malicious actions.
     + Ransomware: Encrypts files and demands a ransom for decryption.
     + Spyware: Collects user data without consent.
     + Adware: Displays unwanted advertisements.
     + Rootkits: Conceals malicious activities on a system.
3. Real-World Examples (15 minutes)  
   Share case studies or news articles related to malware incidents.
   * Discuss the impact on individuals, organizations, and society.
4. Preventive Measures (15 minutes)  
   Educate students on proactive steps:
   * + Regularly update software and operating systems.
     + Use strong, unique passwords.
     + Be cautious when downloading files or clicking on links.
     + Install reputable antivirus software.

Educator Notes:

* Emphasize the importance of skepticism: Don’t trust unsolicited emails or suspicious attachments.
* Encourage responsible online behavior: Avoid visiting untrustworthy websites.
* Discuss ethical considerations: Malware affects real people and organizations.
* [For additional resources and examples, refer to articles like “12 Types of Malware + Examples That You Should Know” 1](https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/) [and “10 types of malware + how to prevent malware from the start” 2](https://us.norton.com/blog/malware/types-of-malware). These provide further insights into malware prevention and detection.

## Prepare for Pick-Up / Pick Up (15-30 minutes)

# Wednesday

# Prevention, Protection, & the Cybersecurity Hero

Schedule

| **Activity** | **Time** |  |
| --- | --- | --- |
| Drop Off | 30 | 8:45-9:15 |
| Opening Narrative | 45 | 9:15-10:00 |
|
| Snack | 15 | 10:00-10:15 |
| CyberShields | 45 | 10:15-11:00 |
|
| Privacy Setting | 60 | 11:00-12:00 |
|
| Lunch/Recess | 60 | 12:00-1:00 |
| Encryption! | 60 | 1:00-2:00 |
|
| Snack | 15 | 2:00-2:15 |
| Deploying our Defenses! | 45 | 2:15-3:00 |
|
| Clean-Up | 30 | 3:00-3:30 |

**Bolded Activities are Key Activities to the CyberQuest Narrative Curriculum**

## Teacher Notes:

## Drop-Off

Purpose: Students will be coming in for the morning, since this is the first morning, have them write name-tags and socialize amongst each other.

In addition it may help to gear them towards the theme by introducing a question of the day.

Lesson Duration: 30 minutes

Materials:

* Clipboard
* Classroom roster
* Tablet (w/ Campdoc signed in)

Educator Notes:

* Some great questions to start the day could include. (Try to cater it to the day’s theme)
  + “Have you heard of cybersecurity? What do you know?”
  + “Have you encountered scam mails?”
  + “What sort of apps have you used?”
* It’s helpful to have a fun fact on the board as well as a schedule to let campers know what to expect.

## Opening Narrative (Wednesday)

Purpose:

To introduce students to a narrative where our friend “Sam” finds out he is hacked. In addition we introduce the topics of camp such as introducing information security concepts and what it means to be online safely.

Lesson Duration:

30-45 minutes

Lesson Outline:

Educators will go ahead and introduce the theme/narrative of the class with a presentation linked here

After this presentation educators will lead into the discussion about how we as individuals may get hacked. In addition we will introduce different types of malware and what a virus vs malware actually means.

Educator Notes:

* Educators please clarify to student the meaning of encryption (in simpler terms for today’s lesson)

## Pulling up different types of malware and introducing differences and similarities could be interesting. Educators will need to do additional research prior to differentiate the different terms.

## 

## Snack Time (30 Minutes)

## 

## CyberShields

Objective:

Materials:

Lesson Duration:

Lesson Outline:

## Privacy Setting

Objective:

Materials:

Lesson Duration:

## Lesson Outline:

## 

## Lunch/Recess (60 minutes)

## 

## Encryption & Decryption! (+Caesar Cipher)

Objective:

Students will understand the basic concept of encryption and learn how to encrypt and decrypt messages using the Caesar Cipher.

Materials:

- Whiteboard or chalkboard

- Markers or chalk

- Paper and pencils for each student

- Caesar Cipher wheel templates (optional)

Lesson Duration:

45 minutes to 1 hour

Lesson Outline:

1. Introduction to Encryption (10 minutes)

* Start with a brief history of the Encryption. Then introduce the cipher used by Julius Caesar to send secret messages. Introduce connections to secret messages then and encryption now.
* Define encryption and decryption.

2. Understanding the Caesar Cipher (10 minutes)

* Explain that the Caesar Cipher is a type of substitution cipher where each letter in the plaintext is shifted a certain number of places down or up the alphabet.
* Show an example on the board, shifting the alphabet by 3 places.

3. Interactive Demonstration (10 minutes)

* Write a message on the board and ask the students to encrypt it using a shift of 3.

(Walk around to assist and ensure understanding)

4. Hands-On Activity (15 minutes)

* Distribute paper and pencils. Have students create their own Caesar Cipher wheel or provide templates.
* In pairs, students will write messages to each other and practice encrypting and decrypting using their wheels.

5. Group Challenge (10 minutes)

* Create a game where students race to decrypt a message you've encrypted with a Caesar Cipher.
* Offer small prizes for motivation.

6. Discussion and Reflection (5 minutes)

* Discuss why encryption is important today and how it's used in modern technology.
* Reflect on what they learned and how they might use ciphers in their own lives.

Post-Lesson:

Encourage students to share with their family their encrypted messages and discuss other cipher techniques with students.

***Snack Time (30 Minutes)***

## Deploying our Defenses!

Objective:

Materials:

Lesson Duration:

Lesson Outline:

## 

## Prepare for Pick-Up / Pick Up (15-30 minutes)

## 

# Credits