Elementary School Cyber Education Initiative

Supplemental Activities

© Air Force Association 2016
Table of Contents

Commissioner's Letter ........................................................................................................ Page 2
Introduction ......................................................................................................................... Page 3
ESCEI BINGO .................................................................................................................. Page 4-11
ESCEI Solve & Swap ......................................................................................................... Page 12-15
ESCEI QR Scavenger Hunt ............................................................................................... Page 16-20

Note: All activities may be reproduced for school, non-profit organization or personal use. All activities and content are property of the Air Force Association and CyberPatriot.

Enjoying our program?
Have questions or comments?
Contact us at: info@uscyberpatriot.org
Or fill out our ESCEI feedback survey: https://goo.gl/iDalvi

The Elementary School Cyber Education Initiative is a component of the Air Force Association’s CyberPatriot National Youth Cyber Education Program, as made possible by its Presenting Sponsor

Materials for the CyberPatriot Elementary School Cyber Education Initiative were funded through a special grant from

NORTHROP GRUMMAN Foundation

RIVERSIDE RESEARCH
Dear Educator,

Thank you for your interest in the Elementary School Cyber Education Initiative (ESCEI) supplemental activities. These activities were specifically created to complement the ESCEI program by enabling students to assess their cybersecurity skills in creative and collaborative ways. Appropriate for grade levels K-6, the ESCEI activities promote students to work independently as well as in group settings to use their cyber safety and cybersecurity knowledge.

The ESCEI supplemental activities are three interactive activities based upon the program’s initial elementary curriculum:

- **ESCEI Bingo** encourages students in grades K-2 to identify and select cybersecurity vocabulary.
- **ESCEI Solve & Swap** has two separate scenario card decks for grades K-2 and 3-6 and offers a comprehensive learning activity that uses scenario cards for students to answer and compare.
- **ESCEI QR Code Scavenger Hunt** enables students to analyze hidden questions in a fun and collaborative activity.

The Elementary School Cyber Education Initiative was launched in July 2015 as a component of the Air Force Association’s CyberPatriot National Youth Cyber Education Program. Since then over 2,500 ESCEI kits have been distributed worldwide as made possible by the generous support of its Presenting Sponsor, the Northrop Grumman Foundation. Materials for the CyberPatriot Elementary School Cyber Education Initiative were funded through a special grant from Riverside Research, a Cyber Gold sponsor.

To request more digital or physical copies of the ESCEI, please go to [https://goo.gl/mMMUwA](https://goo.gl/mMMUwA). Also become a fan of CyberPatriot on [Facebook](https://facebook.com) and follow us on [Twitter](https://twitter.com) to learn more about our special initiatives, promotional giveaways and on-going feedback opportunities.

Once again, I am thrilled to share these new and exciting activities that will continue to encourage and inspire youth nationwide towards careers and education in STEM related fields.

Sincerely,

Bernie Skoch
National Commissioner
CyberPatriot – The National Youth Cyber Education Program
Thank you for requesting the CyberPatriot Elementary School Cyber Education Initiative (ESCEI) kit! These printable ESCEI Supplemental Activities are the perfect complement to the ESCEI lessons and learning modules. Each activity creates an engaging and interactive assessment opportunity that builds upon the learned content from the ESCEI curriculum.

Below are brief descriptions of each activity, along with the appropriate grade level. Each activity can be differentiated for your students’ level of awareness and curiosity.

**ESCEI Bingo (Grades K-3) printable**
Classic game of word recognition and patience! Students will listen for cybersecurity related words and place a marker on their BINGO board. The first student to cover five words in a row, wins. Winning combinations can be horizontal, vertical, diagonal or teacher’s choice.
Required Materials: Scissors, optional laminator or cardstock

**ESCEI Solve & Swap (Grades 2-3/4-6) printable**
Simple and fun cooperative learning strategy for partners or smaller groups, using a deck of scenario cards. Students seated in pairs (or small groups) each take a scenario card, solve the problem, swap task cards, solve the new problem, and then check their answers.
Required Materials: Scissors, pencil/pen, optional laminator or cardstock

**ESCEI QR Scavenger Hunt (Grades 3-6) printable**
Great way to get students moving and learning at the same time! Students use tablets or smart phone capabilities to answer cybersecurity based questions. Each code, when ‘read’ by the mobile device turns into a question relating to ESCEI topics. Some of these questions rely on existing knowledge while some may require a discussion. Students are encouraged to create their own QR codes with teacher direction.
Required Materials: Smart device(s) or tablet(s), optional laminator or cardstock
### ESCEI BINGO

#### Board 1

<table>
<thead>
<tr>
<th>B</th>
<th>I</th>
<th>N</th>
<th>G</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>browser</td>
<td>remote access</td>
<td>software</td>
<td>characters</td>
<td>worm</td>
</tr>
<tr>
<td>Sasser Worm</td>
<td>ILoveYou virus</td>
<td>firewall</td>
<td>CyberPatriot</td>
<td>infection</td>
</tr>
<tr>
<td>pop-up</td>
<td>Trojan horse</td>
<td>Free!</td>
<td>malware</td>
<td>social media</td>
</tr>
<tr>
<td>symbol</td>
<td>security</td>
<td>network</td>
<td>attack</td>
<td>anti-virus software</td>
</tr>
<tr>
<td>phishing</td>
<td>cybersecurity</td>
<td>malware</td>
<td>scam</td>
<td>data</td>
</tr>
</tbody>
</table>

#### Board 2

<table>
<thead>
<tr>
<th>B</th>
<th>I</th>
<th>N</th>
<th>G</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>email</td>
<td>CyberPatriot</td>
<td>malware</td>
<td>infection</td>
<td>software</td>
</tr>
<tr>
<td>Sasser Worm</td>
<td>password</td>
<td>remote access</td>
<td>scam</td>
<td>website</td>
</tr>
<tr>
<td>worm</td>
<td>virus</td>
<td>Free!</td>
<td>pop-up</td>
<td>characters</td>
</tr>
<tr>
<td>Trojan horse</td>
<td>anti-virus software</td>
<td>symbol</td>
<td>social media</td>
<td>firewall</td>
</tr>
<tr>
<td>security</td>
<td>files</td>
<td>malware</td>
<td>ILoveYou virus</td>
<td>attack</td>
</tr>
</tbody>
</table>

#### Board 3

<table>
<thead>
<tr>
<th>B</th>
<th>I</th>
<th>N</th>
<th>G</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>cybersecurity</td>
<td>security</td>
<td>remote access</td>
<td>worm</td>
<td>software</td>
</tr>
<tr>
<td>characters</td>
<td>email</td>
<td>scam</td>
<td>Sasser Worm</td>
<td>malware</td>
</tr>
<tr>
<td>user account</td>
<td>internet</td>
<td>Free!</td>
<td>virus</td>
<td>infection</td>
</tr>
<tr>
<td>firewall</td>
<td>CyberPatriot</td>
<td>attack</td>
<td>data</td>
<td>Trojan horse</td>
</tr>
<tr>
<td>social media</td>
<td>browser</td>
<td>website</td>
<td>password</td>
<td>symbol</td>
</tr>
</tbody>
</table>

#### Board 4

<table>
<thead>
<tr>
<th>B</th>
<th>I</th>
<th>N</th>
<th>G</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>pop-up</td>
<td>infection</td>
<td>network</td>
<td>files</td>
<td>remote access</td>
</tr>
<tr>
<td>software</td>
<td>user account</td>
<td>attack</td>
<td>email</td>
<td>virus</td>
</tr>
<tr>
<td>phishing</td>
<td>Sasser Worm</td>
<td>Free!</td>
<td>malware</td>
<td>anti-virus software</td>
</tr>
<tr>
<td>scam</td>
<td>CyberPatriot</td>
<td>social media</td>
<td>characters</td>
<td>symbol</td>
</tr>
<tr>
<td>browser</td>
<td>data</td>
<td>Trojan horse</td>
<td>website</td>
<td>worm</td>
</tr>
</tbody>
</table>
### ESCEI BINGO

**Board 9**

<table>
<thead>
<tr>
<th>B</th>
<th>I</th>
<th>N</th>
<th>G</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>scam</td>
<td>cybersecurity</td>
<td>Trojan horse</td>
<td>security</td>
<td>attack</td>
</tr>
<tr>
<td>data</td>
<td>password</td>
<td>symbol</td>
<td>network</td>
<td>pop-up</td>
</tr>
<tr>
<td>social media</td>
<td>Sasser worm</td>
<td>Free!</td>
<td>remote access</td>
<td>firewall</td>
</tr>
<tr>
<td>characters</td>
<td>CyberPatriot</td>
<td>files</td>
<td>user account</td>
<td>website</td>
</tr>
<tr>
<td>infection</td>
<td>malware</td>
<td>virus</td>
<td>phishing</td>
<td>anti-virus software</td>
</tr>
</tbody>
</table>

**Board 10**

<table>
<thead>
<tr>
<th>B</th>
<th>I</th>
<th>N</th>
<th>G</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>internet</td>
<td>Sasser worm</td>
<td>Trojan horse</td>
<td>cybersecurity</td>
<td>network</td>
</tr>
<tr>
<td>pop-up</td>
<td>browser</td>
<td>virus</td>
<td>email</td>
<td>attack</td>
</tr>
<tr>
<td>website</td>
<td>phishing</td>
<td>Free!</td>
<td>security</td>
<td>data</td>
</tr>
<tr>
<td>user account</td>
<td>characters</td>
<td>firewall</td>
<td>symbol</td>
<td>CyberPatriot</td>
</tr>
</tbody>
</table>

**Board 11**

<table>
<thead>
<tr>
<th>B</th>
<th>I</th>
<th>N</th>
<th>G</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>pop-up</td>
<td>infection</td>
<td>Sasser worm</td>
<td>firewall</td>
<td>email</td>
</tr>
<tr>
<td>network</td>
<td>phishing</td>
<td>Trojan horse</td>
<td>data</td>
<td>ILOVEYOU virus</td>
</tr>
<tr>
<td>scam</td>
<td>virus</td>
<td>Free!</td>
<td>files</td>
<td>symbol</td>
</tr>
<tr>
<td>social media</td>
<td>software</td>
<td>user account</td>
<td>CyberPatriot</td>
<td>attack</td>
</tr>
</tbody>
</table>

**Board 12**

<table>
<thead>
<tr>
<th>B</th>
<th>I</th>
<th>N</th>
<th>G</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>user account</td>
<td>attack</td>
<td>browser</td>
<td>remote access</td>
<td>Trojan horse</td>
</tr>
<tr>
<td>Sasser worm</td>
<td>email</td>
<td>phishing</td>
<td>cybersecurity</td>
<td>scam</td>
</tr>
<tr>
<td>symbol</td>
<td>files</td>
<td>Free!</td>
<td>firewall</td>
<td>data</td>
</tr>
<tr>
<td>website</td>
<td>malware</td>
<td>password</td>
<td>CyberPatriot</td>
<td>ILOVEYOU virus</td>
</tr>
</tbody>
</table>
ESCEI BINGO

Board 13

Board 14

Board 15

Board 16

© 2016 Air Force Association
ESCEI BINGO

Board 17

Board 18

Board 19

Board 20
### ESCEI BINGO

#### Board 21

<table>
<thead>
<tr>
<th>B</th>
<th>I</th>
<th>N</th>
<th>G</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>phishing</td>
<td>infection</td>
<td>symbol</td>
<td>virus</td>
<td>social media</td>
</tr>
<tr>
<td>CyberPatriot</td>
<td>user account</td>
<td>anti-virus software</td>
<td>password</td>
<td>cybersecurity</td>
</tr>
<tr>
<td>data</td>
<td>Free!</td>
<td>browser</td>
<td>worm</td>
<td></td>
</tr>
<tr>
<td>remote access</td>
<td>attack</td>
<td>pop-up</td>
<td>email</td>
<td>malware</td>
</tr>
<tr>
<td>software</td>
<td>scam</td>
<td>files</td>
<td>security</td>
<td>Sasser worm</td>
</tr>
</tbody>
</table>

#### Board 22

<table>
<thead>
<tr>
<th>B</th>
<th>I</th>
<th>N</th>
<th>G</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>scam</td>
<td>user account</td>
<td>firewall</td>
<td>remote access</td>
<td>website</td>
</tr>
<tr>
<td>data</td>
<td>ILOVEYOU virus</td>
<td>cybersecurity</td>
<td>virus</td>
<td>social media</td>
</tr>
<tr>
<td>Sasser worm</td>
<td>characters</td>
<td>Free!</td>
<td>browser</td>
<td>attack</td>
</tr>
<tr>
<td>security</td>
<td>email</td>
<td>pop-up</td>
<td>CyberPatriot</td>
<td>internet</td>
</tr>
</tbody>
</table>

#### Board 23

<table>
<thead>
<tr>
<th>B</th>
<th>I</th>
<th>N</th>
<th>G</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>characters</td>
<td>firewall</td>
<td>password</td>
<td>symbol</td>
<td>CyberPatriot</td>
</tr>
<tr>
<td>cybersecurity</td>
<td>internet</td>
<td>software</td>
<td>user account</td>
<td>pop-up</td>
</tr>
<tr>
<td>network</td>
<td>browser</td>
<td>Free!</td>
<td>ILOVEYOU virus</td>
<td>website</td>
</tr>
<tr>
<td>scam</td>
<td>remote access</td>
<td>files</td>
<td>Trojan horse</td>
<td>Sasser worm</td>
</tr>
<tr>
<td>attack</td>
<td>social media</td>
<td>security</td>
<td>phishing</td>
<td>anti-virus software</td>
</tr>
</tbody>
</table>

#### Board 24

<table>
<thead>
<tr>
<th>B</th>
<th>I</th>
<th>N</th>
<th>G</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>symbol</td>
<td>virus</td>
<td>scam</td>
<td>infection</td>
<td>password</td>
</tr>
<tr>
<td>Sasser worm</td>
<td>worm</td>
<td>browser</td>
<td>email</td>
<td>pop-up</td>
</tr>
<tr>
<td>attack</td>
<td>internet</td>
<td>Free!</td>
<td>network</td>
<td>user account</td>
</tr>
<tr>
<td>Trojan horse</td>
<td>malware</td>
<td>social media</td>
<td>software</td>
<td>files</td>
</tr>
<tr>
<td>ILOVEYOU virus</td>
<td>remote access</td>
<td>security</td>
<td>website</td>
<td>data</td>
</tr>
</tbody>
</table>
ESCEI BINGO

Bingo Markers

*Educator Tip: Laminate then cut out.
ESCEI BINGO Vocabulary List

1. **pop-up**: a window that contains a menu of commands and stays on the screen only until you select one of the commands and then it disappears.
2. **virus**: a piece of code that has a harmful effect on a computer system, typically corrupting or destroying data.
4. **user account**: a collection of information that tells the computer system which files and folders a person can access, and what changes a person can make to a computer.
5. **security**: protection of information systems from theft or damage to hardware, software and information.
6. **Trojan horse**: a program designed to breach the security of a computer system, that looks like a harmless program but when files are open they contain hidden malware.
7. **cybersecurity**: being protected against the criminal or unauthorized use of electronic data or the act to prevent this type of behavior.
8. **malware**: software that is intended to damage or disable computers and computer systems.
9. **anti-virus software**: computer software used to prevent, detect and remove malicious software.
10. **characters**: symbols, numbers and letters found on a keyboard.
11. **website**: a located connected to the Internet that maintains one or more pages on the World Wide Web.
12. **scam**: a deceptive, dishonest or fraudulent act.
13. **network**: devices exchange data with each other along network links or data connections.
14. **ILOVEYOU virus**: name of a famous virus where 45 million computers were infected and an estimated $10 billion in damage was caused in lost revenue.
15. **infection**: when a worm or virus has copied itself to a part of a computer system.
16. **files**: resource for storing information.
17. **data**: facts and figures and information that is stored in or used by a computer.
18. **firewall**: system designed to prevent unauthorized access to or from a private network.
19. **worm**: malware that replicates itself in order to spread to other computers.
20. **phishing**: online scam where people try to manipulate others into giving up their personal information.
21. **software**: programs and operating information used by a computer.
22. **remote access**: ability to get access to a computer or a network from a remote distance.
23. **password**: a word or combination of characters that must be supplied to gain access to a computer system or a program.
24. **attack**: disrupting, disabling or destroying a computers network or software programs.
25. **internet**: global communication network that allows all computers to connect and exchange information.
26. **symbol**: symbols on a keyboard have special meanings and are used for a strong password.
27. **Sasser worm**: infection more than 1 million computers and shut down numerous companies, causing millions of dollars in damage.
28. **email**: messages distributed by electronic means from one computer user to one of more recipients via a network.
29. **browser**: software application used for retrieving, presenting and moving information on the World Wide Web.
30. **social media**: websites and apps that allow users to create and share content or participate in social networking.
Instructor Directions

1. Laminate or print scenario cards on cardstock.
2. Cut out cards and have one pile of cards for each pair of students.
3. Split students into groups of two and explain student directions.
4. After activity discuss with students their reactions to the scenarios.

Student Directions

1. Take a scenario card from your shared pile.
2. Read the scenario and write how you would solve the problem on your answer sheet.
3. Swap scenario cards with your partner.
4. Read the new scenario and write your solution for the new problem on your same answer sheet.
5. Discuss both answers with your partner. What was the same? What was different?
6. Repeat with new scenario cards.
### Solve & Swap Answer Sheet

Your Name: _____________________  
Partner’s Name: ___________________

<table>
<thead>
<tr>
<th>Card #:</th>
<th>Card #:</th>
</tr>
</thead>
<tbody>
<tr>
<td>____</td>
<td>____</td>
</tr>
<tr>
<td>Switch!</td>
<td>Check!</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Card #:</th>
<th>Card #:</th>
</tr>
</thead>
<tbody>
<tr>
<td>____</td>
<td>____</td>
</tr>
<tr>
<td>Switch!</td>
<td>Check!</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Card #:</th>
<th>Card #:</th>
</tr>
</thead>
<tbody>
<tr>
<td>____</td>
<td>____</td>
</tr>
<tr>
<td>Switch!</td>
<td>Check!</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Card #:</th>
<th>Card #:</th>
</tr>
</thead>
<tbody>
<tr>
<td>____</td>
<td>____</td>
</tr>
<tr>
<td>Check!</td>
<td></td>
</tr>
</tbody>
</table>
**Grades 2-3: Scenario Cards**

**Card #1**
You are at the library with your parents, when the librarian walks up to you and asks your birthday. What do you do? And why?

**Card #2**
You left your lunch at home (again!) and your teacher asks for your mom’s cell phone number so she can bring you your lunch. What do you do? And why?

**Card #3**
Your big brother left his Facebook account open on the family laptop. You know he won’t be coming back right away. What do you do? And why?

**Card #4**
A free game site at school asks you for your address. It’s optional (you don’t HAVE to give it to play). What do you do? And why?

**Card #5**
You need to make a password for your school blog, you think 12345 might be a good idea. Is it? Why and why not?

**Card #6**
Your next door neighbor asks your dad’s work address to send him a note. You know your neighbor, Ann, but you are not sure if your Dad wants to share that info. What do you do and why?

**Card #7**
Your teacher asks everyone when their birthday is at the beginning of the school year. Do you share it with the class? Why or why not? Explain your answer.

**Card #8**
Your grandmother wants to bring cupcakes in for a school celebration. She received an invitation from your teacher but now she can’t remember the address. Do you give it to her? Why or why not? Explain your answer.

**Card #9**
Someone calls during dinner and your mom says it’s okay to answer. The person on the phone asks how many people are in your home and if anyone is under the age of 15. What do you do? And why?

**Card #10**
Your sister just came home from school and she’s late for basketball practice! She can’t remember when Dad gets home but you do. What do you do? And why?
Grades 4-6: Scenario Cards

Card #1
You receive an email from a teacher at your school asking for your password but you don’t recognize the name. What do you do and why?

Card #2
You bought a book online and the web store sends you a survey to fill out about your buying experience. The survey link is 1lovemoney.survey, and you think it looks suspicious. What do you do and why?

Card #3
You missed your favorite show on TV, your friend tells you to just download it off a free website. There’s a big chance that you can obtain malware – but everyone else has seen the episode! What do you do? Why?

Card #4
Your sister borrows your tablet to play a game, she asks for your password to log into your game center. What do you do? Why?

Card #5
You’re surfing the web and a security pop-up comes on your computer screen. You remember your dad updated the computers with anti-malware software and it asks you if you want to continue on a potentially dangerous website. What do you do? Why?

Card #6
You are working on a group project and someone in your group says they know how to disable the firewall to get on an awesome website. It’s the school’s computer and you know that firewalls are necessary to keep malware out. What do you do? Why?

Card #7
You need to create a password for your social media account, but you already have a password for your email. You know passwords shouldn’t be used more than once but you don’t want to remember another complicated password. What do you do?

Card #8
You are at the library and you see an open computer with no one sitting there. Someone left their FaceBook account open, and you are sure they aren’t coming back any time soon. What do you do? Why?

Card #9
You joined a popular website that lets you play all types of online games. It asks you to create a log in but it also asks you to put your address, social security number and your telephone number. This info is optional, what do you do? Why?

Card #10
You receive an email from your friend with a link that says “YOU WON $50!” Your friend says she didn’t send you an email at all. What do you do? Why?
**Instructor Directions**

1. Before the activity, download any free QR reader to tablets or smart devices:  
   - *QR Code Reader and Scanner by ShopSavvy, Inc*  
   - *Quick Scan – QR Code Reader by iHandy Inc.*
2. Cut QR Codes and place them around the classroom.  
   *Tip: Laminate the sheet beforehand for future use!*

---

**Discussion**

Has anyone heard of a QR Code? QR Code is short for Quick Response Code which is a two-dimensional barcode that can be read with an app from a tablet or smartphone with barcode reading capabilities. These codes link directly to text, websites and other types of information.

*This is a QR Code for the CyberPatriot website:*

Who do you think would use a QR Code? Why is a QR Code a great way to share information? Now that you have learned about cybersecurity AND QR Codes, let’s see how you can use them together.

---

**Student Directions**

You are a cyber investigator looking for QR clues to test your cybersecurity skills.

1. With a partner use a tablet or smartphone and search high and low for QR Codes that you can scan. Each code has a unique question that you must answer on your answer sheet. There may be more than one correct answer, so discuss with your partner before writing your answers. There is one answer sheet per team.
2. When finished, use the back of the answer sheet to write five of your own ESCEI scavenger hunt questions.
3. If time allows (and with your teacher’s permission), create your own QR question code to print and post for other students to answer.

---

**Optional Supplementary Activity**

Have students generate their own QR codes using one of these free websites:

- [https://www.the-qrcode-generator.com/](https://www.the-qrcode-generator.com/)
ESCEI Supplemental Activities

ESCEI QR Scavenger Hunt

QR Code Answer Sheet

1. **Name three types of personal information**
   Name, home address, telephone number, social security number, name of your school, your age, birthdate, family members personal information. Answers may vary.

2. **How can you keep personal information safe?**
   You can keep personal information safe by not sharing personal information with strangers or posting information on websites or social media.

3. **Should you share your password with a friend?**
   No, you should never share your passwords with anyone except your parents/guardians.

4. **What information should you not share on social media?**
   You should not share any personal information such as last name, telephone number, birthdate, home address, what school you attend, social security number and information about your family members. Answers may vary.

5. **How do you describe phishing?**
   Phishing is the attempt to obtain sensitive information such as usernames, passwords, and other personal information (and sometimes money), often for malicious reasons, by pretending to be a trustworthy entity in an electronic communication such as an email.

6. **What are two types of malware and what do they do?**
   Virus – spread from machine to machine with the aid of a person
   Worm – can infect and spread without human assistance
   Trojan Horse – can cause computer crash and allow attackers to control a computer remotely
   Other answers may vary.

7. **How is a computer virus spread?**
   A virus is spread from machine to machine with the aid of unwitting humans. Email attachments, malicious websites or spoofed links, downloaded or shared files like “free” movies can all carry viruses.

8. **Can computer worms spread without human assistance?**
   Worms do NOT need human assistance to spread. It scans networks and finds weaknesses to attack.

9. **Why would a hacker use a Trojan horse?**
   Answers may vary.

10. **Give two examples of brand name anti-malware and describe what they do for your computer**
    -McAfee, Symantec, AVG, Bitdefender, etc. Students may be familiar with other anti-malware brands.
    Anti-virus software works by performing scans of all of a computer’s files for malware and if malware is found the software will alert the user and then remove the infected files.

11. **What do firewalls do?**
    Firewalls block malware. Firewalls can be either a piece of computing equipment or software on a computer. They are designed to prevent unauthorized access to a computer.

12. **What is a good combination for a strong password?**
    Strong passwords are ones that are very difficult for other people to guess. Passwords should use many types of characters, like letters, numbers and symbols (!, $, &, etc.) because it makes them more complex for attackers to guess. Passwords should be long because more character mean more combinations attackers have to try to crack.
ESCEI QR Scavenger Hunt

Answer Sheet

Your Name: _____________________       Partner’s Name: _____________________

Directions: With a partner use a tablet or mobile device and search for QR Codes that you can scan. Each code has a unique question that you must answer on your answer sheet. There may be more than one correct answer, discuss with your partner before writing your answers.

When finished, use the back of the answer sheet to write five of your own ESCEI scavenger hunt questions.

1. __________________________________________________________________________

2. __________________________________________________________________________

3. __________________________________________________________________________

4. __________________________________________________________________________

5. __________________________________________________________________________

6. __________________________________________________________________________

7. __________________________________________________________________________

8. __________________________________________________________________________

9. __________________________________________________________________________

10. __________________________________________________________________________

11. __________________________________________________________________________

12. __________________________________________________________________________
For more information on how to participate in the Air Force Association’s CyberPatriot National Youth Cyber Education Program, visit www.uscyberpatriot.org.