GEORGIA | PEACH STATE PATHWAYS

Career, Technical, & Agricultural Education

BUSINESS & COMPUTER SCIENCE

PATHWAY: Computer Systems and Support
COURSE: Information Technology Essentials
UNIT 8: Introduction to Security

INTRODUCTION

Annotation:

In this lesson, students will receive an overview of computer security issues including malware, hacking, encryption, and physical security issues.

Grade(s):

	9th
X	10th
X	11th
X	12th

Time:

17 hours

Author:

Emil L. Decker

Students with Disabilities:

For students with disabilities, the instructor should refer to the student's IEP to be sure that the accommodations specified are being provided. Instructors should also familiarize themselves with the provisions of Behavior Intervention Plans that may be part of a student's IEP. Frequent consultation with a student's special education instructor will be beneficial in providing appropriate differentiation.

FOCUS STANDARDS

GPS Focus Standards:

BCS-ITE-19. Students will identify the fundamentals and principles of security.

a) Identify names, purposes, and characteristics of hardware and software.
b) Identify names, purposes, and characteristics of wireless security.
c) Identify names, purposes, and characteristics of data and physical security.
d) Describe importance and process of incident reporting.
e) Recognize and respond appropriately to social engineering situations.

BCS-ITE-20. Students will install, configure, upgrade, and optimize security.

a) Install, configure, upgrade, and optimize hardware, software, and data security.

BCS-ITE-21. Students will identify tools, diagnostic procedures, and troubleshooting techniques for security.

a) Diagnose and troubleshoot hardware, software, and data security issues.

BCS-ITE-22. Students will perform preventive maintenance for computer security.

a) Implement software security preventive maintenance techniques such as installing service packs and patches and training users about malicious software prevention technologies.

GPS Academic Standards:

ELA10RL5 The student understands and acquires new vocabulary and uses it correctly in reading and writing.
ELA10RC3 The student acquires new vocabulary in each content area and uses it correctly.
ELA10RC4 The student establishes a context for information acquired by reading across subject areas.
ELA10LSV1 The student participates in student-to-teacher, student-to-student, and group verbal interactions.
SCSH3 Students will identify and investigate problems scientifically
SCSh7 Students will analyze how scientific knowledge is developed.
SCSh3 Students will identify and investigate problems scientifically.
SCSh6 Students will communicate scientific investigations and information clearly.
MM3P3 Students will communicate mathematically.
MM3P4 Students will make connections among mathematical ideas and to other disciplines.

National / Local Standards / Industry / ISTE:

ITEA - 1 Students will develop an understanding of the characteristics and scope of technology.
ITEA - 2 Students will develop an understanding of the core concepts of technology.
ITEA - 4 Students will develop an understanding of the cultural, social, economic, and political effects of technology.
ITEA - 8 Students will develop an understanding of the attributes of design.
ITEA - 9 Students will develop an understanding of engineering design.
ITEA - 10 Students will develop an understanding of the role of troubleshooting, research and development, invention and innovation, and experimentation in problem solving.
ITEA - 11 Students will develop the abilities to apply the design process.
ITEA - 17 Students will develop an understanding of and be able to select and use information and communication technologies.

UNDERSTANDINGS & GOALS

Enduring Understandings:

Students will be able to identify the fundamental principles of data security. Students will be able to demonstrate installation, configuration, optimization, and upgrades of security measures. Students will demonstrate tool identification, diagnostic procedures, and troubleshooting techniques for data security, as well as perform preventive maintenance for computer security.

Essential Questions:

- What are the basics of computer security?
- How do I secure my network?
- What are the risks to my network?
- What is malware, and how is it spread?

Knowledge from this Unit:

Students will be able to:

- Create acceptable passwords.
- Cite features of malware and take preventative measures against infection.
- Recognize possible viral infections and remove them.
- Identify various methods of backing up data.

Skills from this Unit:

- Students will be able to install, use, and troubleshoot security software and hardware.

ASSESSMENTS

Assessment Method Type:

X Pre-test
X Objective assessment - multiple-choice, true- false, etc.
_X_ Quizzes/Tests
__ Unit test
____ Group project
____ Individual project
X Self-assessment - May include practice quizzes, games, simulations, checklists, etc.
__ Self-check rubrics
__ Self-check during writing/planning process
__ Journal reflections on concepts, personal experiences and impact on one's life
__ Reflect on evaluations of work from teachers, business partners, and competition judges
_X_ Academic prompts
__ Practice quizzes/tests
X Subjective assessment/Informal observations
__ Essay tests
_X_ Observe students working with partners
__ Observe students role playing
____ Peer-assessment
__ Peer editing & commentary of products/projects/presentations using rubrics
__ Peer editing and/or critiquing
X Dialogue and Discussion

__ Student/teacher conferences
_X_ Partner and small group discussions
_X_ Whole group discussions
__ Interaction with/feedback from community members/speakers and business partners

X Constructed Responses
__ Chart good reading/writing/listening/speaking habits
_X_ Application of skills to real-life situations/scenarios

X Post-test

Assessment(s) Title:

Malware Project

Assessment(s) Description/Directions:

Students will research and present to the class a report on a specific known malware infection that has been introduced by hackers.

Attachments for Assessment(s):

Malware Project.doc

LESSON PLANS

• LESSON 1: INTRODUCTION TO COMPUTER SECURITY

1. Identify the standards. Standards should be posted in the classroom.

   BCS-ITE-19. Students will identify the fundamentals and principles of security.
   a) Identify names, purposes, and characteristics of hardware and software.
   b) Identify names, purposes, and characteristics of wireless security.
   c) Identify names, purposes, and characteristics of data and physical security.
   d) Describe importance and process of incident reporting.
   e) Recognize and respond appropriately to social engineering situations.

2. Have students fill out Anticipation Guide to determine Pre-existing knowledge: (See Attachment: **Anticipation Guide.doc**)

3. Review Essential Question(s). Post Essential Questions in the classroom.

   - What are the basics of computer security?
   - What are the risks to my network?

4. Identify and review the unit vocabulary. Terms may be posted on word wall.

   - Have students identify and correctly pronounce each vocabulary word. Have students monitor class lessons and write definitions for each word as they come up in the lessons. (See Attachment: **Malware Vocab.doc**)

5. Interest approach – Mental set

   Ask students if their computer ever picked up a virus. What were the symptoms? Did it do permanent damage to their data? How does a computer get infected?

6. Show Malware presentation #1. Discuss what malware is. (See Attachment: **Malware1.ppt**)

• LESSON 2: MALWARE

1. Review Essential Questions. Post Essential Questions in the classroom.
    - What is malware, and how is it spread?
2. Show Malware presentation #2. Discuss different types of malware. (See Attachment: **Malware2.ppt**)
3. Show Malware presentation #3. Discuss spyware and malware hoaxes. (See Attachment: **Malware3.ppt**)
4. Show examples of malware and hoax emails. (See Attachment: **Congratulations for Winning.rtf** & **Egyptian.rtf** & **Lotto International.txt** & **PLEEEEEASE READ.doc** & **Urgent assistance.doc** & **Very Confidential.doc** & **Virus_Hoax.doc** & **Work Klez_E.doc**

• LESSON 3: PASSWORDS

1. Review Essential Questions. Post Essential Questions in the classroom.
    - How do I secure my network?
2. Show Password presentation. Discuss password netiquette. (See Attachment: **Passwords.ppt**)
3. Hand out Security Wordfind document to review major concepts. (See Attachment: **Security Wordfind.pdf** & **Security Wordfind Answers.pdf**)

• LESSON 4: I.D. THEFT

1. Review Essential Questions. Post Essential Questions in the classroom.
    - What are the risks to my network?
2. Discuss what ID theft is. How can your ID be stolen, and what might the consequences be?
3. Use the Ohio Attorney General Lesson plan to teach about ID Theft. (See Attachment: **ID-Lesson-Plan.pdf**)

• ATTACHMENTS FOR LESSON PLANS

Anticipation Guide.doc
Malware1.ppt
Malware2.ppt
Malware3.ppt
Malware Vocabulary.doc
Malware Vocabulary Answers.doc
Passwords.ppt

Security Wordfind.pdf
Security Worfind Answers.pdf
Congratulations for Winning.rtf
Egyptian.rtf
Lotto International.txt
PLEEEEEASE READ.doc
Urgent assistance.doc
Very Confidential.doc
Virus_Hoax.doc
Worm Klez_E.doc
ID-Theft-Lesson-Plan.pdf
Malware Project.doc

Notes & Reflections:

ID theft is now the most prominent theft of information currently happening. It affects individuals more than companies, but information can be retrieved through company sources. Students should be aware of how detrimental this can be to their personal finances.

When having students sign up for their malware project, determine some fair method of insuring there is no duplication of virus names. If a student cannot find enough info on a given virus, it might be a good idea to swap for another, or add another to the first virus, at the teacher's discretion.

Most school systems have an antivirus program running on their network. If possible, have students open and look at the structure of the program. Invite the network administrator or a technician to come speak to the class on the proper use and maintenance of antivirus software, past problems in the network, etc.

There are some good free antivirus and anti spyware software available online. Download and install these packages on your lab computers. AVG, Avast, AdAware, Spybot, & Microsoft Windows Defender are available. Caution when dealing with unknown software listed as free. There are some Rogue/Suspect (fake) antivirus packages out there that start to download immediately when you visit a site. Most spyware and antivirus software do not see them as threats. These programs run, and tell you that you have infections, and to click "here" to remove them.....now.....quick!!!!! These rogue programs with their false positives will hound you until you get them removed.

CULMINATING PERFORMANCE TASK

Culminating Unit Performance Task Title:

Install Antivirus software

Culminating Unit Performance Task Description/Directions/Differentiated Instruction:

Students will download and install a good antivirus software and Spyware software.

Attachments for Culminating Performance Task:

UNIT RESOURCES

Web Resources:

http://www.microsoft.com/protect/default.aspx
http://www.labrats.tv/episodes/ep95.html
http://www.howstuffworks.com/virus.htm

http://www.brainpop.com/technology/computersandinternet/computerviruses/
http://www.snopes.com/computer/virus/virus.asp
http://vil.mcafee.com/hoax.asp
http://computer.howstuffworks.com/worst-computer-viruses.htm
http://computer.howstuffworks.com/virus.htm
http://computer.howstuffworks.com/spyware.htm

Materials & Equipment:

What 21st Century Technology was used in this unit:

X	Slide Show Software		Graphing Software		Audio File(s)
	Interactive Whiteboard		Calculator		Graphic Organizer
	Student Response System		Desktop Publishing	X	Image File(s)
	Web Design Software		Blog		Video
	Animation Software		Wiki	X	Electronic Game or Puzzle Maker
	Email	X	Website		