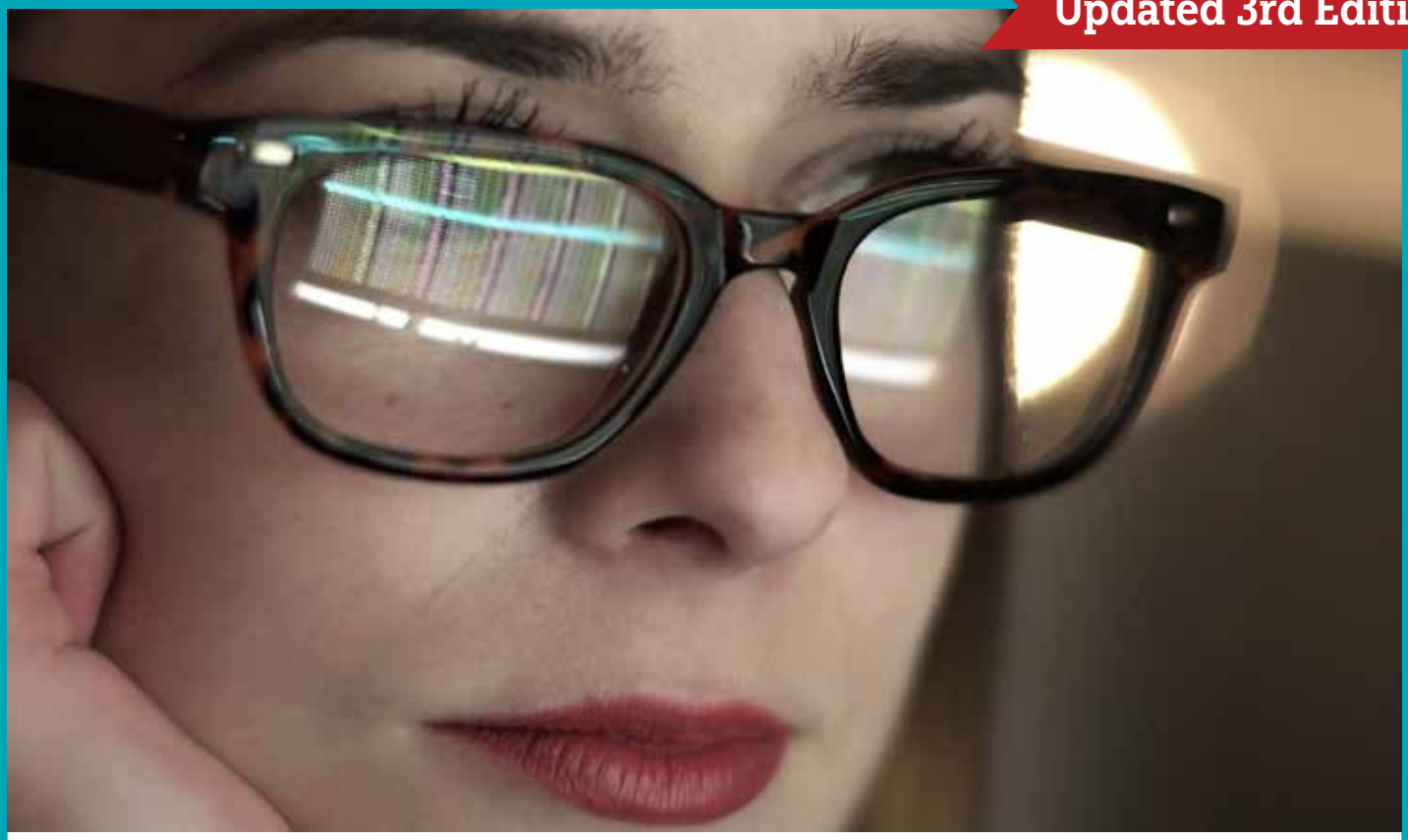
Updated 3rd Edition!



Cyber Career Awareness Program (CyberCAP)

STUDENT WORKBOOK

DISCOVER AND LEARN:

What is cybersecurity and why should I care?

What can I do to stay safer online?

How do I know if I like or can do cybersecurity?

How do I figure out if a career in cybersecurity could be right for me?

Find the answers to these questions — and more! — inside.

Start Engineering

CHAPTER ONE

What Is Cybersecurity and Why Should I Care?

What do you think is worse? Having 1,000's of dollars – or more – of financial crimes attached to your name because of identity theft. Or having revealing pictures of yourself posted online for all the world with an internet connection to see.

If you are a teenager, you might not have to choose.

Every year, cyber criminals steal sensitive, personal data belonging to over 1 million kids and use it to open fake bank accounts and credit cards in the kids' names. In most cases, underage victims of identity theft like this will not even know about these crimes until they try to open up their own, real accounts and find their names attached to acts of fraud they did not commit.

Meanwhile, in 2014, cyber criminals stole almost 100,000 photos and videos delivered through Snapchat. Thousands of these stolen messages contained nudity and explicit messages in-

DECEPTIVE ONLINE COMMUNICATIONS

Cybercriminals are constantly testing and developing new ways to separate internet users from their PII. In the Snapchat case above, malicious hackers broke into a third-party network used to capture and store users' personal information and files. In other cases, they target people rather than networks, trying to trick them into divulging the userids, passwords, and other pieces of information needed to get illegal access to others' personal data. Some of the most common, most effective tactics involve emails and other message types that look innocent or familiar but are meant to deceive. "Phishing," and other forms of "social engineering," all seek to trick people into opening attachments or clicking on links that enable cybercriminals to gain access to PII, which they can use for nefarious purposes.

Identifying a bogus email or website can be challenging. Most social engineering scams seek to present their communications as coming from people or online institutions already familiar or trusted, but they also tend to feature some or all of the same give-away traits:

- **They're too good to be true!** Exciting, out-of-the-blue prizes, offers of money for nothing, and so on should tell you not to click on anything and just delete the email.
- **Act now!** When an unexpected email wants you to take urgent action, the only urgent thing to do is delete it.
- **Funky hyperlinks.** If you hover over a hyperlink, you can see the URL. Look for typos, extra-long URL's, or some other indication of trickery.
- **Unexpected attachments.** A dead give-away in almost every case – if you're not expecting an attachment in an email, don't open it. If you have any questions, follow up with the sender before opening it to confirm validity.
- **Unknown sender.** If you don't recognize the name or address of the sender, don't open it.

ACTIVITY 2: Identify Deceptive Online Communications

From the options on the previous page or others you find on your own, **pick out 3 different online phishing quizzes to take, then come back and complete the exercise below.**

1. What 3 quizzes did you take? Provide the URL's below.

2. How did you do? Write down either the scores you got on all 3 or other forms of feedback you received.

3. Did your performance improve? Why or why not?

4. What was the hardest part about the quizzes? What was the easiest? What was surprising or different from what you'd expected?

5. Have you received phishing emails? Have you or anyone you know ever fallen for a phishing scam? What happened?

TYPES OF MALWARE ATTACKS

Malware that circulates through a device/network:

Virus: Malicious code spread through downloads from websites, email attachments, or portable drives. It reproduces itself in your computer, damaging performance, corrupting data, and harvesting PII, among other nasty things.

Worm: Malware that replicates throughout a network. Unlike viruses, which rely on a user spreading the virus through action, a worm spreads on its own. Worms cause the most damage when they destroy data on a network or allow the attacker remote access.

Malware that collects data:

Adware: Annoying or offensive ad pop-ups, banners, or graphics, adware is usually seen as a "potentially unwanted program" or PUP. It can track online activities or physical locations, and when this kind of information leads to harmful follow-up, adware turns into malware.

Spyware: Tracking software used without the consent of the user to collect data such as keystrokes, browsing habits, location data, or even login information. Spyware data are then harvested and sold, usually to cyber criminals, for them to exploit however they can.

Malware that modifies or deletes data:

Ransomware: Software that encrypts data on a device until the user agrees to pay a fee to unlock it or risk it being deleted.

Backdoor: A piece of code installed without a user's knowledge that allows a malicious user to circumvent system security settings and get illegal access to data in a network.

Logic bomb: Malicious code added to a legitimate program that is triggered by a specific event. Logic bombs can lie dormant for lengthy periods of time.

Malware used to launch attacks:

Botnets: Bots (individual computers) that form a network of compromised computers, controlled by a third party and used to transmit malware or spam, launch attacks, steal data, or to spy on user activities.

ACTIVITY 4: Research Malware

Pick out one of the types of malware identified on previous pages. In online research, gather information as described below:

1. What type did you pick? What is it?

2. How does it make its way onto users' machines?

3. Find and describe two examples of real-world incidents in which this malware caused damage or disruption to computer networks.

4. How can people prevent this type of malware from infecting their computers? Identify as many methods of prevention as you can. When you consider preventive measures, assess how feasible they are and what tradeoffs they involve between keeping information secure versus keeping it accessible.

ONLINE BEHAVIOR

A cybersecurity incident almost always starts with a choice someone makes to do the wrong thing. From criminal penetrations of guarded networks to sloppy password habits to clicking on virus-infected attachments or bogus website links, cybersecurity breaches result from a myriad of causes. But they almost universally reflect the failure of people to follow ethical principles meant to preserve the safety, reliability, and privacy of online network.

In 1992, the Computer Ethics Institute put forth a set of ten "commandments" for people to follow in the use of computers and information technology:

TEN COMMANDMENTS FOR COMPUTERS AND INFORMATION TECHNOLOGY

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

PERSONALLY IDENTIFIABLE INFORMATION

Cyber attacks of most concern to individuals are those that target personally identifiable information, or PII. This is the online asset that all users have and all cybercriminals want. Keeping it safe allows us to go where we want to go online and do what we want to do, just as a bicycle helps us move around town on our desired rounds. And just as bicycle owners put behaviors and protective devices to work keeping their property safe and accessible only to them, internet users have many ways to do the same with their sensitive data. Not only is learning how to stay safe online in our personal lives a fundamental requirement in this internet age, it is also a good way to start building the skills and knowledge that could lead to a career in cybersecurity.

Here's a generally safe assumption: **everything you do online, any information you post, could be made public or visible to someone else.** With any luck, not in a way that harms you. But it's always a possibility. For this reason, it's important to take steps to make sure you keep important personal information protected or offline altogether, and practice sound safety with anything you do put online.

You should treat personally identifiable information, or PII, with extreme care online. PII includes things like your:

- **Social Security Number**
- **student identification data**
- **passwords**
- **financial account information**
- **address information**
- **any other data that could allow people to connect your online activities to you and things you value in the physical world**

ONLINE SAFETY 101

1. **Change your password regularly.** Don't re-use old passwords or use the same passwords for multiple accounts. Figure out a system to remember your passwords. Write them down and hide the list. Use a password manager.

2. U**se strong passwords.** Use passphrases or abbreviations and avoid words found in the dictionary. Use random special characters and numbers to avoid being the victim of a brute force attack. Passphrases should be at least 8 characters long. Don't share passwords; if you wouldn't give the person the key to your most valuable possessions, don't give them your passwords.

3. **Use two/multi-factor authentication, if available.** This adds another layer of protection. It may take slightly more time but is becoming more and more common to avoid compromise.

4. **Beware of phishing attempts.** If an offer seems too good to be true, it is. Be a skeptic. Don't give personal information out over the phone without verifying identity of the caller. Do not click or open emails that appear suspicious. Slow down!

5. **Cover up your webcam and practice basic safety.** Close or at least lock your device when you leave it. Never leave a device alone in public and avoid unknown devices such as random thumb drives or other plug-ins.

6. **Be aware of location settings on your device.** Turn off location settings and bluetooth when not in use. Do not allow apps access to data if they do not need access to function. Turn off location settings on your camera. Do not post while on vacation. In general, do not overshare on social media.

7. **Run antivirus software.** Be sure to use valid software and keep it updated.

8. **Avoid public WiFi.** At the very least run a good VPN to add another layer of protection. Be conscious of the websites you visit while on public WiFi. Be especially careful in areas of high traffic (coffee shops, airports, hotels, etc.).

9. **Back up your data.** Then back it up again. Use an external hard drive, even if you use cloud storage.

10. **Update/patch your devices.** Yes, it might be annoying. However, it's necessary. Run the updates. If you question the validity of the update, be sure to run it straight from the source.

ACTIVITY 3: Building Passwords

In this exercise, you will build several passwords of different lengths, estimate how long it would take to crack them, and then test them online to find out how long it would actually take to crack them.

Fill out the table below with 3 sets of 3 passwords each, running 6, 9, and 12 characters.

For the first password in each set, use only **letters.**
For the second, use **letters and numbers.**
For the third, use **letters, numbers, and special character**s.

For each password, guess how long it would take a hacker to crack it.

PASSWORD	ESTIMATED CRACKING TIME	ACTUAL CRACKING TIME
_ _ _ _ _ _		
_ _ _ _ _ _		
_ _ _ _ _ _		
_ _ _ _ _ _ _ _ _		
_ _ _ _ _ _ _ _ _		
_ _ _ _ _ _ _ _ _		
_ _ _ _ _ _ _ _ _ _ _ _		
_ _ _ _ _ _ _ _ _ _ _ _		
_ _ _ _ _ _ _ _ _ _ _ _		

ACTIVITY 1: Numbers, Numbers, Numbers

To solve these problems, you'll have to look at and think about numbers in imaginative, unfamiliar ways. Sometimes numbers might not be what they seem, and sometimes the answer might be "hidden" in plain sight.

A. What is the answer to the last equation?

12 x 21 = 9

13 x 31 = 16

14 x 41 = ?

Hint: Sometimes a number shows up whole, sometimes it shows up in parts.

B. What is the next number in this sequence?

3, 6, 10, 15, 21, _____

Hint: Remember, it's the differences among us that make life interesting.

C. What is the next number in this sequence?

2, 12, 1112, 3112, 132112, _____

Hint: Each successive number will point you back to the number just before it, if you can read it in the singular way required and take one thing at a time.

D. A credit card has 16 numbers on it. Look for a pattern to figure out the last two digits on a card with these numbers:

1248 1632 6412 82 ____ ____

Hint: Numbers don't always belong together, even if they're right next to each other.

In the next exercises, use addition, subtraction, multiplication, and division to construct the given number out of the others presented. Use each operation and each number only once. For example, making 6 out of 3, 2, and 1 could be (3 x 2) / 1 = 6.

E. Make 43 out of 2, 5, 7, and 8 _____

F. Make 4 out of 1, 1, 6, and 7 _____

G. Make 80 out of 1, 3, 6, and 9 _____

H. Make 32 out of 4, 7, 7, and 9 _____

ACTIVITY 3: Reasoning

These puzzles can all be figured out using just the information presented. Using logic and attention to detail, can you solve them?

A. Your parents have six daughters, including you. Each daughter has one brother. How many people are in your family?

_____

B. If 3 cats can catch 3 mice in 3 minutes, how long will it take 30 cats to catch 30 mice?

_____

C. Rearrange the letters of NEW DOOR to make one word out of them.

_____

D. A farmer had nine sheep, and all but seven died. How many did he have left?

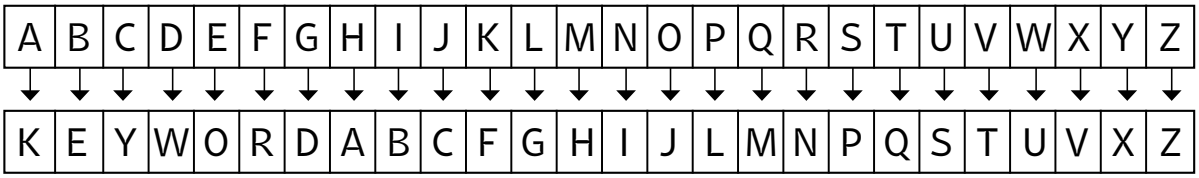
_____

E. If a doctor gave you three pills and told you to take one every half hour, how long would they last?

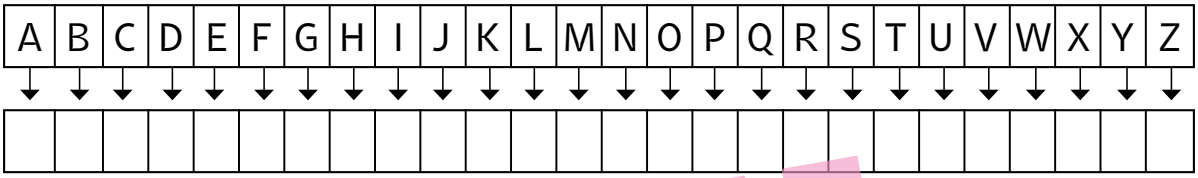
_____

ACTIVITY 6: Cryptography — Keyword Cipher

The Keyword cipher is identical to the Caesar cipher with the exception that the coded alphabet is shifted by using a keyword. To create a substitution alphabet from a keyword, you first write down the alphabet. Below this you write down the keyword (omitting duplicate letters if the word contains two or more of any letter) followed by the remaining unused letters of the alphabet.



Create your own keyword cipher using the grid below and then write a secret message to a friend!

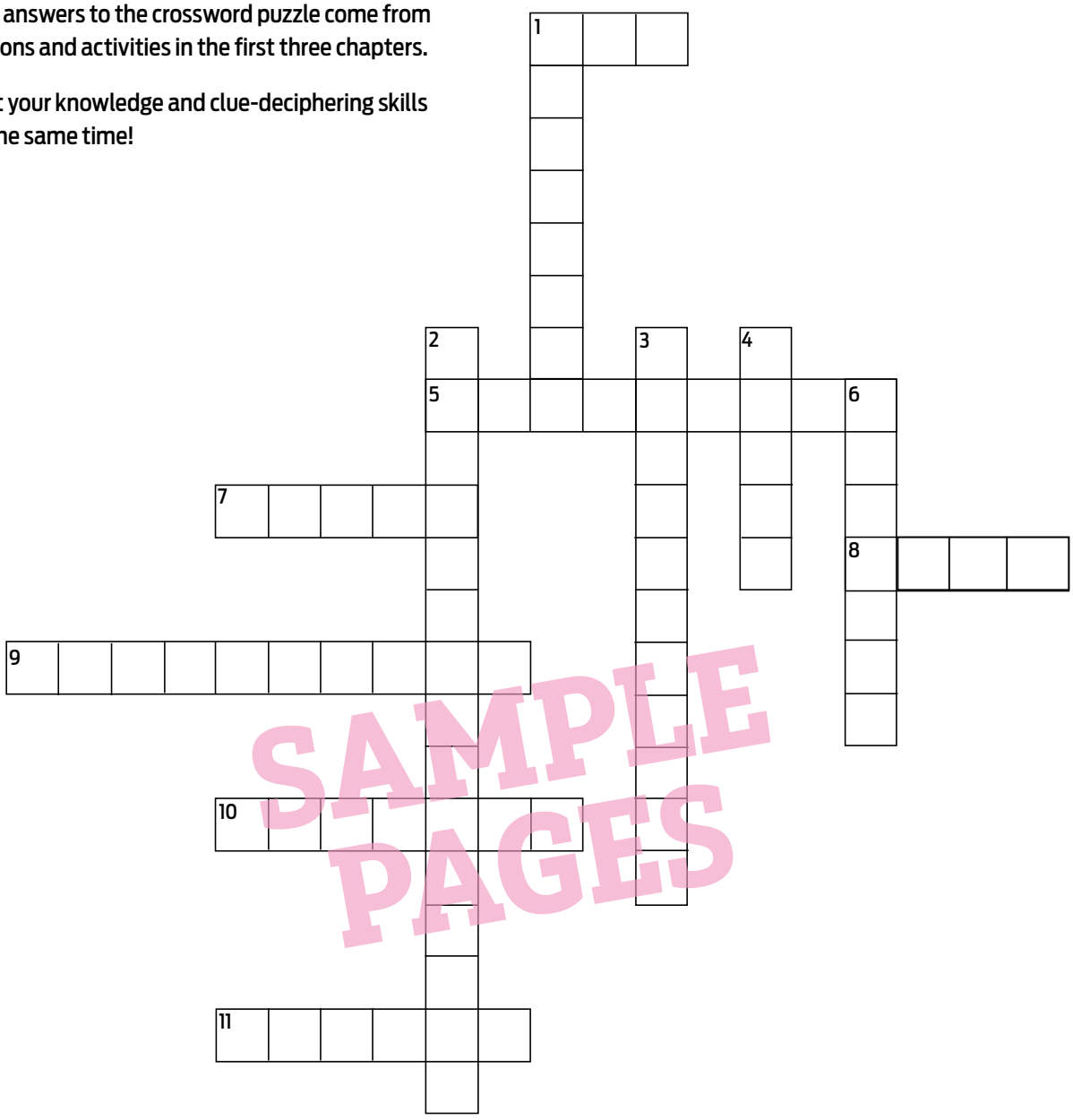


How would a keyword cipher be more secure than a Caesar cipher? How would it be less secure?

ACTIVITY 9: Crossword Puzzle — Vocabulary Review

The answers to the crossword puzzle come from lessons and activities in the first three chapters.

Test your knowledge and clue-deciphering skills at the same time!



ACROSS

1. Valuable data troves of individuals, abbreviated.
5. Linear sequence of steps, to go from A to B to ...
7. Makes a computer "sick".
8. Makes a computer "sick," then another, then another.
9. A tool of extortion, it takes data hostage and locks it up.
10. Secret resident of a hard drive that watches your every move.
11. Actually makes sense, once you know how to read it.

DOWN

1. Tries to "hook" you into trouble.
2. Something to lean on for help with access to online accounts.
3. Could be bearing "gifts" you don't want to live with.
4. Says, "Feel safe, all ye who enter here."
6. Poison software pills that let the bad people into your data.

FINDING YOUR PLACE IN THE FIELD

To get a fix on finding your place in cybersecurity, you can learn more about particular functions or roles people fill in the field. The National Initiative for Cybersecurity Education (NICE) has developed a framework for cybersecurity careers that defines seven basic categories encompassing the different kinds of work people do. Delving into these functions and using them as a filter for your own interests and abilities can help identify the educational and career pathway into cybersecurity that would work best for you.

These seven categories are:

1. **Securely Provision:** Design and build secure IT systems.
2. **Operate and Maintain:** Administer systems and manage the data they house.
3. **Oversee and Govern:** Manage teams; develop elements of the legal, policy, and education environment.
4. **Protect and Defend:** Identify and understand threats, defend networks against attack.
5. **Analyze:** Gather information and translate into usable, accessible intelligence.
6. **Collect and Operate:** Gather information inside and outside systems; execute defensive countermeasures.
7. **Investigate:** Collect and analyze forensic and other data associated with events or crimes directed at IT systems.

These categories can overlap, depending on a person's individual skill set or an organization's structure and needs. Cybersecurity professionals often move in and out of jobs with responsibilities spread across two or more of these categories. The chances for learning and variety can be many, throughout the length of any career in the field.

ACTIVITY 2: Career Exploration continued

CYBERSECURITY WORK ROLES

Look at the tab called "work roles," at https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/workroles.

Now scroll down the pull-down menu and pick out three that seem interesting to you and **write them below, along with the category of the work role.** (Just ignore the Work Role ID.)

1. _____

2. _____

3. _____

Is the category of each work role above one of your highly ranked career preferences?
Add a Y or N to each line.

For each of the Work Roles you've chosen, pick out 3-5 items from the Abilities/Knowledge/Skills/Tasks lists that seem interesting or appealing to you and write them below.

1. _____

2. _____

3. _____

What classes or subjects do you think you would take in school to learn more about these items? Try to come up with 5-8 possible classes or subjects.

1. _____ 5. _____

2. _____ 6. _____

3. _____ 7. _____

4. _____ 8. _____