Scenario #1 – Jake and the Bad Virus

The two major C3 concepts this scenario illustrates are:

Cyber Security: Jake compromised his computer's security by providing personal information to an unknown online source, which lead to his computer becoming vulnerable to receiving a virus.

Cyber Ethics: Jake does not act ethically when he is not open with his parents about what happened to his computer. Although it can be scary to admit a mistake and accept possible consequences, it is never a good choice to continue to let possible further harm occur to anyone or anything by "covering up" a poor choice to avoid getting in trouble. This is a perfect example of why it is so important to maintain open communication with parents and guardians, so that when something negative happens online, the focus is on correcting the issue, rather than panic over admitting a mistake because one is worried they will get into trouble or have their computer taken away.

Jake's four mistakes:

1. He opened an email from an unknown source.
2. He took the bate in this phishing scam that promised something too good to be true.
3. He provided personal information to an unknown source
4. He was not honest to his parents or guardians about the negative experience he had online that compromised the family computer's security.

What should Jake have done?

1. Jake's first step should have been to delete the email from the unknown source without opening it.
2. After opening the fraudulent email, Jake's knowledge of the WWW Decision Tool should have made him suspicious when the unknown source started asking for personal information. He could have then stopped, deleted the email, told his parents and even reported the incident to the Federal Trade Commission.
3. The most important step Jake should have taken, was after making the mistake that caused the virus, Jake should have told his parents about the incident so they can restore their computer's security and prevent further loss of private information.

Scenario #2- Emily and Romanita's Long Distance Friendship

The two major C3 Concepts this scenario illustrates:

Cyber Safety- Remember, you don't know people you meet online. Unfortunately, you must be aware that there are individuals who can pretend to be someone they are not in order to do harm.

Cyber Ethics- Acting responsible by honestly following the guidelines and rules your parents or guardians have established for online use. Remember they are designed to keep you and your computer safe!

Questions (set #1)

1. Emily's main error was not following her parent's rules and guidelines. If she had simply followed these 100%, she never would have accepted the unknown friend's request.
2. This unknown person tricked Emily several ways:
   -They saw that she communicates regularly with someone in Boston, so they used a Boston email address. In truth, they could be anywhere in the world.
   -They tried to use common online lingo to build trust by sounding like a fellow student. This is how some individuals trick students in providing personal information.
   -They formed an email that made them appear to be a 12 year old girl.

Questions (set #2)
Emily should take the following steps to be extra safe from this phony online friend:

1. Tell her parents what happened. Her safety and the safety of her true online friends are more important than the possible risk of getting into trouble. The main concern of most parents in student safety.
2. Tell her friend Romanita and her other parent approved online friends about the incident, just in case this person tries to contact them.
3. Block this person to prevent them from contacting her again.

Scenario #3

The major two C3 Concepts that Aimee failed to follow were:

Cyber Ethics- Aimee did not behave ethically by honoring her parent's rules or by following copyright laws.

Cyber Security-Aimee compromised herself and her computer's security by providing detailed personal information to an unknown online source.

Aimee's poor choices:

1. Aimee was dishonest with her parents by disobeying the rules she agreed to follow about the MP3 Player.
2. Aimee went against her "gut" and downloaded something illegitimately just to get the song she wanted. Compromising your ethics for a song is a bad trade off.
3. Aimee provided personal information to an unknown source.
4. Aimee did something illegal by not following copyright laws and showed no regard for the artist who created the album she loved.

Answers to Specific Questions:

1. Aimee's actions were illegal. Many students do not realize that they can be arrested or their parents can be fined hundreds of thousands of dollars for illegal downloading of music. Real lawsuits have already taken place across the country.
2. Aimee's friend does not sound like a true friend. She encouraged her friend to disobey her parents and told her to visit and use a "secret" website, which doesn't sound legal.
3. Aimee's actions are most unfair to the musicians and songwriters who are not getting paid for the hard work they put into creating a song people enjoy listen to. If you worked hard to create something, how would you feel if others dishonestly took advantage and didn't pay you?

C-SAVE

STAYSAFEONLINE.org
National Cyber Security Alliance

Scenario #4

The major C3 Concept that Alex's mom compromised is:

Cyber Security – There are many, many fraudulent websites that try to trick users in providing personal information or install and spread viruses. Alex's mom did not know the important items to look for to verify if a website is legitimate.

How Alex protected his mom from making a mistake:

1. Legitimate websites asking for credit card information will have a symbol that verifies that they protect personal information and typically offer various secure pay options for those concerned about security.

Risks:

2. Alex's mom could have damaged the computer by becoming vulnerable to a virus
3. Alex's mom could have been a victim of Identity Theft by providing personal information.
4. Alex's mom could have lost money and compromised her financial information.

Recommended steps if Alex's mom wants to shop online:

1. Purchase the bag from a legitimate company she is already familiar with and trusts.
2. Go to National Cyber Security Alliance's website for suggested tips on safe online shopping.
3. Make sure the website has security symbols verifying that they protect personal information.

Scenario #5

The two major C3 Concepts that this scenario illustrates:

Cyber Security- Scott's actions could have jeopardized the school's computer and network security.

Cyber Ethics- Scott signed the school's acceptable use policy agreeing to follow school rules for computer use. He did not honor his responsibility when he chose to go against school rules to get something he wanted for free.

Questions: (set #1)

1. Making your computer vulnerable to a virus.
2. It is hard to verify if a "free download" is legitimate. Here are a couple of possible tips: -Ask yourself if the free offer is from a reputable company. If so, verify with the company by phone that they are truly making this offer.
   -Ask yourself if this offer is too good to be true. If it sounds too good to be true, it probably is. Your antenna should go up that his may be a phony attempt to do harm to you or your computer.
3. It is hard to say. By simply accessing the link to accept the free download, it is possible that he made the school network security vulnerable.
4. Scott could have compromised his own protection as well as that of his classmates by allowing private information to be passed through the school network. He could also have been charged with vandalizing school property if his actions damaged the school's computer.

Questions: (set #2)

1. This is a difficult ethics question. As tough as it might be, Scott should act in the school's best interest and inform his teacher of the mistake he made. By doing so, the school can correct the situation immediately to limit any further threat to security of the computer or to the school's network.

2. Who is asking for the personal information?
   What are they asking for?
   Why do they need this information?

Scenario #6

The major C3 Concept his scenario illustrates is:

Cyber Security – Illegal "hackers" who intend harm to others and to their computers can be very clever. This was an obvious attempt to trick Roxanna into compromising her computer's security by posing to be a legitimate update. This is a common way viruses or malware are spread onto a computer.

Questions (set #1)

1. Roxanna did not attempt to do anything wrong. She simply thought she was doing her job of making sure the computer's security software remained up to date.
2. One important thing Roxanna could have done to be extra careful, is to think of the last time her security software was updated and which company they use. If it is her job to keep the software updated, her parents or guardians need to make sure she knows the schedule for how often updates occur. This alone can help her recognize an attempt to get her to download a possible virus through a phony anti-virus update.

Questions (set #2)

Some possible risks associated with accepting these pop-up links include:

1. Roxanna could have downloaded a virus, malware or spyware.
2. Roxanna could have allowed a clever computer hacker to follow her future keystrokes and track her family's personal information.
3. Roxanna could have compromised her computer's hard drive.

Explanations:

1. No computer hacker is ever going to make it obvious that they are trying to spread something harmful to your computer. Instead they will often try to pose themselves as a legitimate action a C3 savvy computer user might not recognize as harmful.
2. One type of hacker is specifically trying to "hijack" your computer to track your keystrokes. These criminals are often trying to gain access to personal information including passwords or credit card information.
3. Some hacker's main goal is simply to ruin or crash your computer's hard drive so you lose all valuable information.

Scenario #7

The major C3 Concept this scenario illustrates is:

Cyber Security- Curtis gave up his computer's security by allowing his "friends" to know his password. These are never to be shared with anyone other than a parent or guardian. It is a good idea for parents and guardians to keep passwords to make sure you remain safe and secure.

Questions (set #1)

1. Curtis' friends made themselves vulnerable in two ways by sharing their personal information: A. They opened their computer's security and their safety to these "friends". B. They opened their computer's security and their safety to anyone else these "friends" choose to share this private information with, now that it is available.

3. No, Curtis should not share this information with these "friends". Just because you spend time with friends, doesn't mean you have to follow everything they do. If they are doing something that doesn't seem right, you should feel completely comfortable standing up for what you think is right.

Questions (set #2)

1. Each of Curtis' classmates should reset their passwords immediately, and should be sure to choose new passwords that are not similar to the old passwords.
2. Who is asking for the information? What are they asking? Why do they need this information?
3. Curtis' friends are not acting like friends. True friends will never push you to do something you are not comfortable with, such as revealing personal information that could be harmful to you, possibly your family, and definitely your computer.

Scenario #8

The two major C3 Concepts this scenario illustrates:

Cyber Ethics: It is absolutely unethical to use the Internet to intend to hurt or threaten anyone. It is not funny or entertaining at all and shows lack of computer ethics and responsibility. If it is something you know would hurt or embarrass someone in person then it is something that is also not okay to do or say online.

Cyber Safety: Cyberbullying is extremely unsafe and in some cases has led to very serious consequences for both the cyberbullies and the victims they are harassing.

Questions (set #1)

1. Not only is cyberbullying extremely unethical, but laws also protect students from being bullied either in person or online. Because of certain serious consequences that have resulted from cyberbullying, local law enforcement as well as Federal authorities such as the United States Secret Service, can now prosecute students and families who cyberbully.
2. Stop responding immediately to anyone online who makes you feel uncomfortable or who you don't trust and know well in person.
3. Block this person from ever contacting you again.
4. Tell your parents or guardians, and in this case, because it involves classmates at school, tell your teacher.

Questions (set #2)

1. Caroline could tell her own parents about the incident and inform their teacher at school so she can avoid future situations such as these with this group of unkind girls.
2. Cyberbullies – People who use the Internet bully people online.
3. (Each school's answer might be different.) Some students may be very aware of the school's rules regarding cyberbullying, while other students may not be aware at all. There is still large variation between how schools are handling cyberbullying cases across the country.