

Course Learning Outcomes for Unit II

Upon completion of this unit, students should be able to:

1. Explain how criminal justice theories and technologies impact the commission and solution of crime.
4. Examine causes, methods, and criminal justice agency counteractions to terrorism.
 - 4.1 Elaborate on the various cyberterrorism risks, past, present, and future.
 - 4.2 Relate the culture and perceptions of the hacker.

Reading Assignment

Chapter 3: The Criminology of Computer Crime

Chapter 4: Hackers

Unit Lesson

Introduction to Perceptions and Theories of the Hacker

The general population of the world probably has only a very basic understanding of the difference between cybercrimes, cybercriminals, and hackers. Probably, most people think all hackers are criminals and that all cybercrimes are closely related and broadly defined. This unit lesson will discuss the different theories of criminal justice and what they have to do with cybercrimes, criminals, and hackers.

Culture and Perceptions of the Hacker

The hackers and their culture, or subculture as it is frequently called, are very misunderstood. In fact, an entire course of study could be dedicated to understanding and explaining hackers. Surprisingly, not all hackers are criminals. Some hackers are beneficial. Some hackers hold very important and high positions within the government and corporations. What is important to understand is that the classification of hacker is not limited to one definition, as we will learn in this unit.

That is not to say that all hackers are awesome brainiacs whose underlying altruistic goal is one that will save the world. This does not mean that this cannot or will not happen, but there are cybercriminals out there. Whether labeled a hacker or not, these individuals can do serious damage.

Some hackers are adamant that they are peaceful, non-threatening individuals who operate within the law, usually as they chose to recognize it. Other hackers are not so warm and fuzzy. For example, it could probably be stated that all cybercriminals are hackers, but not all hackers are cybercriminals. This will be explored more in this unit with a detailed explanation of the classifications of hackers and the various theories behind why they do what they do.

The Theories of Criminal Justice

Let us move away from the broad, generic use of the word *hacker* and visit some real truths. There are cybercriminals, bullies, and terrorists out there and they are all a hybrid of each other. A cyberterrorist is certainly a cybercriminal. The problem with the cyber aspect is classifying them and identifying them for the purposes of law enforcement. The whole concept of a cyber world has put a spin on local, national, and global law enforcement. It is for this reason that we must understand how to identify and classify these individuals. Individuals who usually have a technological head start.

What are the biggest targets? The first targets that come to mind are banks and media. The fruits of these large scale crimes can be used to fund terrorism or simply enrich the cybercriminal. Individual targets are probably more randomly chosen than large targets simply because it is probably easier to target Aunt Sally's identity than to break through the super systems at Bank of America. It is safe to say that no one is immune. All a citizen can do is their best. Organizations have to stay on top of the new threats and their vulnerabilities. The truth is, more often than not, the cybercriminals are on the cutting edge of the threats and vulnerabilities. This is precisely why the government and large corporations might employ *hackers* to maintain their databases.

The Role and Limitations of Law Enforcement

Cybercrimes against large segments of the community may seem like a nebulous and unpredictable problem, similar to an earthquake. However, there are cybercrimes that hit closer to home, happening in communities around the world. These are the crimes that local law enforcement are more likely to encounter. These crimes are those that usually affect our most precious and vulnerable targets: the children. From ripping off someone on Craigslist to using the Internet to exploit children, there is a new realm for criminals.

Identifying proactive and preventative measures: Click on the following link to view an interactive presentation detailing measures used to identify and remedy cyber vulnerabilities:

<http://www.pearsoncustom.com/mct-enterprise/asset.php?isbn=1256689785&id=16056>

Implications and Solutions

The Internet has opened up a whole world of information that grows exponentially every day. As the world becomes more open, so do children and the threats against them. This is where parents and communities need to be responsible in monitoring their children's access. Does your child have an Instagram account? Is it set to private? Look through their followers list sometime, and make sure it is set to private. When is someone old enough for Facebook or a smart phone? Does your child have the Internet in their room? Parents need to be vigilant about teaching their children about Internet safety, and they need to properly moderate the level of access a child has based on their age and level of responsibility. As a parent, you have a right to the password. That is not to say that you should not trust your child, but to educate them rather than allow the computer to babysit them and teach them the ways of the world.

Conclusion

How does cyberbullying happen on social media? What can parents do about it? What is the role of law enforcement when something goes tragically wrong? In this unit lesson, some of the criminal justice theories related to these issues, the role of the criminal, and the role and limitations of law enforcement have been identified.

Suggested Reading

Chapter 3 PowerPoint: The Criminology of a Computer Crime
Click [here](#) for a PDF version of the Chapter 3 Presentation.

Chapter 4 PowerPoint: Hackers
Click [here](#) for a PDF version of the Chapter 4 Presentation.