Crimes Using a Computer

Bernard Ayuyao

Old Dominion University

CYSE 600 36666 Cybersecurity Principles

July 21, 2021

Crimes Using a Computer

What is your definition of computer crime? From the article titled "Computer Crime", it is defined as "any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation, or prosecution. Computer crime is not considered a single type of crime that is different from other crimes. Rather, nearly all kinds of crimes can be committed through computers or be computer mediated." (Parker & Nycum, 1984, p. 313) I can think of an example where a computer crime that just happened recently on the East Coast of the United States which also affected the Hampton Roads area. One hacker used a computer to shut down a gas line that supplied gas throughout parts of the East Coast. It caused a lot of panic and forced a lot of people to buy and hoard gas because they did not know for how long the Hampton Roads area will be out of gas. It took days to almost a week to get the gas lines running causing gas prices to go up because of someone committing a computer crime. There are four different ways to commit crimes involving a computer and they are attacking the computers itself, using a computer to modify information, using a computer as a tool to conduct or plan a crime, and using the computer itself to intimidate or deceive.

First, a computer can be the object of the attack. When we think of computer crime, sometimes we think of using it to commit a crime. Physically attacking a computer can be a crime as well. "Over the past few years, international terrorists have used bombs and submachine guns to attack at least 28 computer centers belonging to multinational companies and government agencies in Italy and France." (Parker & Nycum, 1984, p. 313) This shows that when destroying the physical asset which is the computer, it is no longer has the availability of use. If a military organization loses all their computer assets from all their computer stations,

they can lose the edge to defending themselves or the country because we heavily rely on computers to give commands to the computer in order to function military assets.

The second type of crime that can be committed using a computer is through modification. "A computer can be the subject of a crime by providing the automated mechanisms to modify and manipulate new forms of assets such as computer programs and information representing money." (Parker & Nycum, 1984, p. 313) This shows that someone with the intention to steal or gain money can use a computer to commit a crime. There is no need to carry a gun and wear a mask to rob a bank for all their money. Someone can do that behind a computer by just modifying their bank account. All the criminal needs to do is to add a few zeros and commas to make their funds on the bank account grow. No one gets hurt or killed and can be done without being seen who they are behind a mask.

The third type of way to commit a crime is using a computer as a tool to conduct or plan a criminal act. "The computer can be used as a tool for conducting or planning a crime. A stockbroker used a computer to produce forged investment statements showing huge profits to deceive his clients and steal $53 million." (Parker & Nycum, 1984, p. 313) This is a great example because just like how a computer can be used for risk analysis, it can be used for committing a criminal act. It allows the criminal to plan their next attack or do something like copying a user's name and password to access private information which will benefit the criminal but take a toll on the victim without their knowing.

Finally, the last way to commit a crime using a computer is to intimidate or deceive. "The symbol of the computer itself can be used to intimidate or deceive. The same stockbroker told his clients that he was able to make such huge profits on rapid stock option trading by using a secret computer program in a giant computer in a Wall Street brokerage firm. Although he had no such

program nor access to the computer in question, hundreds of clients were convinced enough to invest a minimum of $100,000 each." (Parker & Nycum, 1984, pp. 313-314) This shows that the criminal is deceiving the victim by making them believe about a magical software to help them gain money. In reality, it is a false advertisement and a software that does not really work in which he or she can steal the victim's money. We must be careful of what we believe in because not only can the software be something falsely claimed, it can also be malicious.

All in all, we may have our own understanding of what a computer crime is but there are many types of computer crimes out there and many ways a criminal to conduct that act or crime. We must be aware of our surroundings and what we believe in. A crime can be a physical attack to destroy an asset or computer, manipulating that asset, using a computer to plan a crime, and it can be used to deceive a victim for some kind of gain whether it is financial or informational for the criminal.

References

Parker, D. B., & Nycum, S. H. (1984, April). Computer Crime. *27*(4).