

Computer crime essay

[Technology](#), [Computer](#)



A major Issue within this Industry Is the fact that citizens, law enforcement officials, prosecutors, and the government don't put cyber crime at the top of their list of dangerous crimes Is because the actual act of computer crime Is not In Itself viewed as being dangerous. This Is a traditional view of computer crime, and the book goes on to explain that, " many [stereotypical] computer criminals are non- threatening, socially challenged Individuals, and 36. % of officers believe that Investigation of computer crime Interferes with their ability to concentrate on rotational' crimes" (Bruit, 7). Because police tend to not look too seriously at these crimes, the general public will form their own, similar opinions on the matter. This gives people an inaccurate belief about the effects of cyber crime. In fact, computer crime can and many times is violent today. One area of computer crime that has become particularly dangerous, especially for younger generations is cyber bullying.

In recent years, we have seen more and more suicides related to cyber bullying then ever before. An example of this can be seen in the case of the United States v. Lori Drew. Lori was an older woman who pretended to be a teenaged boy and began to talk and soon after started an online relationship with a 14-year-old girl. The girl eventually began to fall for the fake 16- year-old boy that Lori Drew created. After a series of conversations, their " relationship" ended with a message from Drew telling the girl that nobody actually liked her and she should instead kill herself.

Unfortunately, the 14-year-old girl, being highly impressionable and because of her feelings for this fake teenage boy, took the device and ended up killing herself. A big issue we have seen with lawmakers Imposing laws to prevent cyber crime is that, it is such an advanced form of crime that many

times it is unclear if there was an actual crime committed and if so where/when it happened. In past situations, "legislative bodies and judicial authorities have been slow to respond" (Bruit, 5).

This slow response allows for those committing crimes in cyberspace to avoid punishment and lets these criminals continue their illegal operations. Another problem within this criminal sector is the gray area teen, "someone who accesses information without authorization and someone who is actually committing an act in cyberspace meant to harm someone or destroy property" (Webster). Another traditional view when it comes to cyber crime that is probably the most commonly thought, is that "it would never happen to me". The average American does not think that they could be a computer criminal's target.

These people believe that because they aren't millionaires and instead an average income American, cyber people aren't taking the proper steps to protect themselves, they are becoming easier targets. In 2004, 54 million Americans were subject to email attacks by "fishers" looking to steal financial information from people. Roughly 4% of these 54 million people gave away their financial information including credit card numbers, addresses, phone numbers, etc.? that is almost 1.7 million people! In the year 2003, 1.2 billion dollars were generated in cyber attacks on average Americans.

But computer criminals are not just using this phishing approach to steal information and money. They are practicing using key logging and spyware to steal passwords and other private information that can allow these people to go unnoticed while spending your money. Despite the fact that we see more

and more security be put in place to avoid these issues, it continues to happen because so many people in our society believe it will not happen to them. But what is instead happening, is more of these average people are being targeted because they are essentially making it easier for these criminals to steal their personal information.

While these criminals certainly could steal more money from millionaires, going after these more average Americans is easier and afar (Wilson). With how technology dependent our society has become, we see more and more hacking crimes today. There even exist groups out there that have members from all over the world that collectively hack different websites. For example, Anonymous is probably the most well known hacking collective in the world. Parry Lesson's book *We Are Anonymous: Inside the Hacker World*, she discusses the history of the group and the attacks that they have done.

This group would like us to believe that they are an activist group that seeks freedom for all people, but has hacked financial institutions such as Papal, Mastercard and Visa. They want us to believe that they are freedom fighters and simply believe in an unregulated Internet, but they tend to go after websites and companies that simply disagree with their message. It is kind of a double-edged sword, because while they are preaching about freedom of speech, they then in turn go after people who disagree with their message. Olson even discusses the fact that the group went after her because of the books she was writing about this organization.

People are definitely becoming more aware of the dangers of computer crime, any Americans still do not see the detrimental effects that cyber

crime can have on society. These people that are blinded by traditional views of computer crime, have become the target of attacks. Their lack of preparations have allowed cyber criminals to go after them and gain money through their computer skills. Bruit, M. T. (2013). Computer Forensics and Cyber Crime and De. , Volvo. 3). Upper Saddle River, NJ: Pearson. Introduction (3rd Olson, Parry.