Computers have initiated many changes in the world we live in today. The introduction of computers has changed many definitions and how one may interact with the world. This paper will go over three topics: computer crimes, computer security, and privacy related to computers. For each topic, a definition will be given, an example court case and its importance, and then how to protect one’s self before or after a violation of the topic.

The first topic discussed will be computer crimes. Computer crimes, also called cybercrimes, are crimes that are done with the assistance or by the use of a computer or network (1). There are many different types of computer crimes: hacking, piracy, stalking, identity theft, child abuse, and more (1). Hacking is when one enters into a computer or related system that they are not authorized to use (1). It can be thought of trespassing for computers and networks; either way someone is where they do not belong. Hacking violates one’s privacy, which will be delved more into later, and can result in more than just observation; a hacker can steal sensitive data and implant a virus. Piracy is the distribution of copyrighted content without consent from the creator/owner (1). Piracy tends to only be when they content is downloaded or able to be kept by a user, but it varies by content and copyright law. Another computer crime is stalking, which is when one uses the internet to track someone’s location without the victim’s knowledge/permission (1). Identity theft is when someone impersonates another individual to gain access to the resources the victim has, like money (1). Child abuse is very rampant on the internet and is normally of a pornographic nature (1). As you can tell these crimes vary on the actions taken by the perpetrator and can be synonymous with some physical crimes.

There are many examples of cyber crimes to be found. One that I have chosen to review is a smaller court case about when PlayStation Network got hacked and other actions of the hackers. The summary of the crimes is that a group of individuals hacked PSN, possibly stole payment information from users, and some members were involved in being paid to threaten victims on their phone with calls (2). The group committed many violations of privacy and security against their victims. The retrieval of payment information could be used for identity fraud to steal money from PlayStation users. The hack also shut down PlayStation Network for a while, so its customers could not receive the service they expected. The hacking of PlayStation alone costs money for not only the business but also the customers who used it. On another note, the threatening calls violated the safety of the victims and disturbed their mental health. As one can see, cyber crimes do not only affect elements in cyberspace, but also has impact on things in the world of reality.

With so many threats to one’s self from computer crimes, it is likely one will be targeted by a computer crime of some sort. The best way to deal with computer crimes are preventative maintenance, meaning it is better to know how to avoid viruses and hacks since dealing with them when you are already a victim becomes more difficult. One way to help prevent some computer infections through malicious software is to have an antivirus and antimalware installed on a system. This precaution will help keep one’s system from being infected as easily. Another method of protection is done through being smart and not clicking on links or downloading files from untrustworthy sources. However, if one becomes the victim of an attack, there are ways to get through it. One such way is to contact police about the attack, they will know the steps to take and can help identify the threat if it is something like stalking. Another method is to go to an IT professional to clean a virus off of a system as soon as possible.

The second topic of discussion is computer security. Computer security is the guarding of systems from theft and damage to the hardware, software, and information on the system, as well as the services that the system provides (3). There are four main components of computer security: confidentiality- only authorized access to the data, integrity- only authorized modification to the data, availability – data is there when required, and authentication- knowing who is on the line is actually who they say they are (3). Computer security is making sure one’s system is safe and not being take advantage of without one’s consent. The previous topic, computer crimes, are can be easier or harder to commit depending on the computer security of a victim. Computer security is important because it reduces the chance for the misuse of one’s system, meaning your system is less likely to be used to attack other systems if your computer is secure (3). Computer security is also what helps one be secure from the unauthorized access a system, similar to how opening someone else’s mail is a crime.

The example case for computer security is found in the Carpenter v. United States supreme court case. The summary of the case is that four men were arrested for committing robberies, one of the men gave over his cell and numbers that were associated with others involved in the crime, the FBI—without a warrant-- used this to track down Timothy Carpenter and tried to convict him of the crime as well, but Carpenter argued that it violated his rights to have his cell records looked into without a warrant (4). The supreme court concluded that the warrantless access of Carpenter’s records was unconstitutional because it was an “unreasonable search” of his records (4). This case is involved in security since the FBI agents did not have authorized access to Carpenter’s records, which is a violation of authorization, a keystone for computer security. Without such a case to decide a warrant was needed to get cell access, individuals in police enforcement would be able to conduct investigations that violated the privacy of one’s personal data without probable cause to access the records. A reality with that type of enforcement would make cell data even less secure.

One’s computer security is important to keep up to date. Violation of computer security can come in many ways, especially from computer crimes. As is the same with computer crimes, it is best to prevent computer security violations. The violation prevention measures are going to echo much of the methods found in preventing cybercrimes. Another method to help prevent security from being compromised is by the use of a firewall, which would help filter out possibly dangerous data from entering your network. However, if one does find their security compromised, there are ways to combat it. As always one can turn to law enforcement, but there are some local things one can do as well. For instance, many sites that require sign in can be set up for dual factor authentication, which means that for someone to access your account they will have to also have access to another communication method—often a phone or email. One should also change their passwords and any similar password to a compromised account; this will help reduce the chance of repeated violations of security that stem from an original one.

The last topic of discussion is privacy. Privacy, much like in real life, pertains to one’s right to his or her own self; this includes communications and actions (5). Privacy protection allows users to know about what is being monitored and recorded by a service or product (5).

While most of the previous cases can be seen as a violation in privacy, this topic will review a different court case between Sony BMG and the Electronic Frontier Foundation (EFF). To summarize the case, Sony had software on music CDs that would install itself on a system and record data along with create undisclosed and hidden files (6). This method created new weaknesses third parties could exploit on a user’s system (6). The CDs End User Licensing Agreement (EULA) was found unreasonable (6). In the end Sony had to reimburse and change its product for those affected (6). This is an important case since it shows that even if it is in a EULA, it can still be challenged. This also shows that software developers have to keep in mind the effect their software has on privacy. Another significant part of this case is how it reinforces how the user must be notified of the data that is being recorded, but the users of the CDs were unaware of just how much was being recorded.

There are many ways to prevent your privacy from being compromised. As before, many of the methods for avoiding cyber crimes can be used here. Some other privacy protection methods are disabling java, disabling flash, updating software, and updating the operating system (7).

As one can determine, computer crimes, computer security, and computer privacy are all interconnected. These three topics influence and overlap one another.

References

1. <https://jsberrylaw.com/blog/common-types-of-computer-crimes/>
2. <https://www.justice.gov/usao-ndil/pr/american-and-dutch-teenagers-arrested-criminal-charges-allegedly-operating>
3. <http://www.contrib.andrew.cmu.edu/~dabousen/Default%20-%20Copy%20(4).html>
4. <https://www.oyez.org/cases/2017/16-402>
5. <https://research.uci.edu/compliance/human-research-protections/docs/privacy-confidentiality-hrp.pdf>
6. <https://www.eff.org/cases/sony-bmg-litigation-info>
7. <https://privacyrights.org/consumer-guides/securing-your-computer-maintain-your-privacy>