Sentencing

As in any criminal trial, if a defendant pleads guilty or is found guilty, the court imposes a punishment in the form of a sentence. So it is in cases of cybercrime. The purpose of punishment in the criminal justice system is subject to debate, with the following justifications having been offered historically:

1) Deterrence of the offender and others who would commit the same offense in the future;
2) Rehabilitation of the offender;
3) Denunciation of the criminal act itself;
4) Retribution or vengeance for the offender having committed the offense;
5) Incapacitation of the offender;
6) Restitution or compensation to the victim(s) of the offense;
7) Reconciliation and potential reintegration of the offender.

Courts are also expected to impose sanctions that are proportional to the offense- that is, that reflect the seriousness of the crime. They are also expected to take into account the particular background characteristics of the offender when imposing sentence.

Like defendants in traditional criminal trials, cybercriminals who go to trial will be punished with some sort of sentence. And, the sentence imposed, whatever end the court may have in mind, is expected to be proportional to the seriousness of the offense and to be related to the background of the offender.

There have not been any large-scale studies of cybercrime sentencing, but the following observations apply to such cases.

Because there are numerous different types of computer and internet crimes, there are also a wide range of potential penalties. Some computer crimes have minor penalties associated with them, while more serious crimes can impose significant fines and lengthy prison sentences.

Fines. Fines for a conviction of various computer and internet crimes range widely. A misdemeanor conviction can result in relatively minor fines of a few hundred dollars, and possibly up to a $1,000 or more, while felony convictions can have fines that exceed $100,000.

Jail or prison. A person convicted of certain internet or computer crimes may also face a jail or prison sentence. The most serious crimes, such as possessing child pornography, can result in a prison sentence of 20 years or more.

Probation. Probation sentences for computer crimes are also possible as either individual penalties or in addition to jail or fines. Probation terms can differ widely, but typically last at least one year and require the person on probation to not commit more crimes, maintain employment, report to a probation officer, and pay all court costs and fines.

Somewhat more specific illustrations of punishments for cybercrime are presented on the next slide.

•Illegally accessing computers (hacking) – jail sentence from 6 months to 5 years.
•Intercepting communications – possible jail sentence for 1-5 years. However, DDoS attacks, for instance, can only be punished if there were some breakdowns in network. No punishment for an attempted crime.
•Hacking computer and changing source code – fine and/or jail sentence for 1-10 years, depending on the damage caused. Second offense can get up to 20 years in prison.
•Hacking government information system – up to 10 years and high fines.

Judges take certain properties of the cybercrime itself in deciding on a sentence. Among those properties:

1) Loss- in financial or property crime, what was the dollar value lost to the victim(s) of the crime?;
2) Number of victims- how many people were victimized in the crime?;
3) Extraterrirorial conduct- was the crime carried out over state or national borders?;
4) Sophisticated means- "sophisticated means" is appropriate if the offense includes "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense." ;
5) Trafficking in access devices- an "access device" includes computer passwords and credit cards.;
6) Risk of death or injury- did the offender compromise vital infrastructure, such as electric power grids, water systems, etc.?;
7) Private information- did the offender obtain and/or disseminate sensitive or private information involving an identifiable person (including such information in the possession of a third party), including (i) medical records; (ii) wills; (iii) diaries; (iv) private correspondence, including email; (v) financial records; (vi) photographs of a sensitive or private nature; or (vii) similar information.

New Jersey | *2C:20-23, et seq.* |
Defined Offenses: *Defined computer crimes to the degree.*
Penalty Profile: *Up to 18-months prison to 10-years prison.*
* Note: Section does not specifically classify crimes listed as either felony or misdemeanor. Offenses listed in misdemeanor or felony columns are based on the levels of punishments imposed rather than by explicit classification.

For an understanding of cybercrime in New Jersey, go to:

https://codes.findlaw.com/nj/title-2c-the-new-jersey-code-of-criminal-justice/nj-st-sect-2c-20-23.html