Criminal profiling is both art and science based on generalizations that categorize various types of computer criminals. Profiling uses statistical data for inductive profiling and deductive profiling. **Inductive profiling** assumes established patterns: criminal offenders tend to follow a common background and motive. **Deductive profiling** seeks to reconstruct the offender’s actions: hypothesizes the offender’s actions before, during, and after committing a crime.

Stereotypical cybercriminals range from unsophisticated “script kiddies,” who lack programming skills, to expert criminals who create custom exploits and attack tools. Many cybercriminals disregard computer crime laws and often rationalize why those laws are invalid or inapplicable, especially when espousing political agendas against corporate practices or national policies.

Recurring types of attackers include the following:

* **Cracker:** A malicious attacker who deliberately intrudes upon systems or networks to gain unauthorized access or unauthorized resources.
* **Hacker:** An individual who enjoys breaking systems or software without causing harm, presumably with the intent to better understand and improve security.
  + Hat colors are often attributed to depict the mentality of a hacker or a cracker. **Black hat** corresponds to a harmful system intruder. **White hat** corresponds to a helpful security practitioner. **Gray hat** corresponds to a hacker who may act in goodwill, but also crosses the line to commit illegal acts.
  + A gray-hat hacker may gain unauthorized access to a computer system to raise awareness—expose flaws to improve security—of a stubborn or uninformed administrator. Although there is no malicious intent, the lack of authorization creates a criminal act that can be prosecuted if received poorly.
* **Identity thieves and Internet scammers:** People looking to steal personal identities or steal money from unwitting victims. This includes criminals that use phishing, pharming, spam, and other types of deception-to-swindle individuals.
* **Cyberterrorists and drug traffickers:** Attackers who target government sites or commit federal crimes using the Internet as a platform for black market commerce or trafficking offenses. Cyberterrorists and traffickers both use the Internet to facilitate criminal activity locally and abroad.

Cybercriminals may be motivated by one or several influences, which may include money, emotion, political or religious beliefs, social acceptance, sexual impulses, or immature amusement. An attacker may have some personal grievance against the way a country handles international affairs or how a corporation treats certain individuals. Political and religious grievances are often the primary drivers for unsophisticated “defacers,” that is script kiddies, who want to raise awareness of their beliefs. Sophisticated criminals are comparatively less juvenile and trend toward monetary gain, sexual deviance, or self-entitlement issues.