Cybersecurity Threat Landscape (Part 3 - Verizon)

In this part, you should primarily use the *Verizon Data Breaches Investigation Report* plus independent research to answer the below questions.

---

1. What is the difference between an incident and a breach?
   Incident is a security event that compromises the integrity, confidentiality or availability of an information asset.
   Breach is an incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.

2. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?
   69%. 34%.

3. What percentage of breaches were perpetrated by organized criminal groups?
   39%

4. What percentage of breaches were financially motivated?
   71%

5. Define the following:

   Denial of Service: **Any attack intended to compromise the availability of networks and systems. This includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service.**

   Command and Control: **The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Also called C2.**

   Backdoor: **Any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (aka root access) on a computer system, network or software application.**

   Keylogger: **A keylogger (short for keystroke logger) is software that tracks**

or logs the keys struck on your keyboard, typically in a covert manner so that you don't know that your actions are being monitored.

6. The time from an attacker’s first action to the initial compromise of an asset is typically measured in which one? Seconds, minutes, hours, days?
   Minutes.

7. When it comes to phishing, which industry has the highest click rates?
   Education.