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?

   An incident is a security event that compromises the integrity, confidentiality or availability of an information asset while a breach is an incident that results in the confirmed disclosure of data to an unauthorized party.

2. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?
   69% by outside actors and 34% by internal actors
3. What percentage of breaches were perpetrated by organized criminal groups?
   39%

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

5. Define the following:

   Denial of Service: A Denial of Service attack makes a machine or network completely inaccessible by flooding it with traffic or via other mechanisms that will cause a crash.

   Command and Control:A command and control server is a computer controlled by a hacker, used to send commands to other systems that they have already compromised.

   Backdoor:a hidden entrance to a computer system that a hacker can use to gain access to the system

   Keylogger: is a type of malware that will record every stroke a person makes on their computer.

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 industry