Casey Farmer

CS-405

7-1 Journal

08/14/2025

7-1 Journal: Consider the Motive for the Attack

Cybersecurity threats are a growing concern in today's digital landscape, with hackers exploiting technological vulnerabilities for various motives and ethical frameworks. There are three types of hackers: black hat, white hat, and grey hat. Black hackers exploit system vulnerabilities for personal gain, while white hat hackers identify and fix security flaws within legal and ethical boundaries. Grey hat hackers breach systems without permission but may not have malicious intent.  
  
Motivations for hacking range from personal gain to ideological expression, with financial gain being the most common motive. Ideological beliefs and activism target organizations to promote political, social, or environmental agendas, while corporate espionage involves stealing proprietary data or disrupting business operations.  
  
Reputation and challenge are another motivation for hackers, with some motivated by overcoming complex security systems or gaining recognition within the hacking community. Disruption and sabotage are designed to cripple infrastructure, interrupt services, or cause widespread chaos, often without a clear financial motive. Common attack methods include phishing, UI redress, denial of service, DNS spoofing, SQL injection, brute force attacks, and man-in-the-middle interception.  
  
Understanding the types of hackers and their motivations is crucial for developers and cybersecurity professionals to build resilient systems and respond effectively to threats. Studying real-world examples and familiarizing oneself with common attack methods can help anticipate vulnerabilities and contribute to a safer digital environment.