Hacking

Hacking: any unauthorized access to a computer or a computer system.
Traditionally, hackers have been categorized as "white-hat hackers"- aka "good guy hackers"- and "black-hat hackers"- "bad guy hackers". (A third category, "grey-hat hackers" was identified as having both tendencies.) While these distinctions may still be seen in some of the literature, they have been replaced by the general term "hacker".
Hacker skill levels:

1) Script kiddies: Computer novices with only minimal skills necessary to carry out their attacks. They use free documentation, tools, and vulnerability scanners available on the internet; they are sloppy in their work and leave identifying traces on the computers and/or systems they penetrate.
2) Criminal hackers: Sometimes called "crackers", these are computer experts who ***cr***iminally h***ack*** into computers and networks and leave no traces of their invasion; they can make it appear that someone else cracked into the computer or network. They are often members of groups who prefer to remain anonymous. They create some of the hacking tools that script kiddies use; they write malware they use to crack into computers and/or systems.
3) Security researchers: Highly technical security experts who monitor and track computer network vulnerabilities, and write code to exploit such vulnerabilities. They may be employed in business or corporate IT units to maintain network security.

Hacker motivations: there are numerous motivations behind hacker activity.
Many times hackers hack just because they can; their motivation is simply to prove to themselves and to others that they can do it. However, there are other motivations:

1) Hacktivists attempt to disseminate social and/or political messages in their work. They try to raise public awareness of an issue. Examples include messages about legalized drugs, antiwar protests, big corporations, income inequality, and many others.
2) Terrorists attack critical corporate or government computers and/or public utility networks to steal classified information or expose information about personnel employed in these structures. Examples include attempts to disrupt electricity power grids, air traffic control towers, or obtain classified government documents.
3) Hackers for hire are organized computer crime figures who contract with individuals or groups to crack networks or systems. Their motivation is very basic- money.

Hacker anonymity: Hackers can remain anonymous on the internet in a variety of ways.

1) Borrowed or stolen accounts of friends, previous employers, or other individuals or groups;
2) Public computers at libraries, schools, or hotels;
3) Open wireless networks (example- the network one can log into in a shopping mall);
4) Anonymous or disposable email accounts;
5) Infected computers (zombies or bots) at other organizations;
6) Workstations or servers on the victim’s own network.

Common Security Weaknesses that Criminal Hackers Target

Gullible and overly-trusting users

Unsecured building and computer room entrances

Discarded documents that have not been shredded and computer disks that have not been destroyed

Network perimeters with little to no firewall protection

Poor, inappropriate, or missing file and share access controls

Unpatched systems that can be exploited using free tools such as Metasploit

Web applications with weak authentication mechanisms

Guest wireless networks that allow the public to connect into the corporate network environment

Laptop computers with no full disk encryption

Mobile devices with easy to crack passwords or no passwords at all

Weak or no application, database, and operating system passwords

Firewalls, routers, and switches with default or easily guessed passwords