Article on Hacking

Name	Gaurav
College	D.N. College, Meerut
Subject	Hacking
Roll No.	190328121023

The history of hacking

When hacking first started it was not thought of as that serious. The hackers were not even known as hackers but as practical jokers. The very first hack came in 1878 when the phone company, Bell Telephone, was started. A group of teenage boys, hired to run the switchboards, would disconnect or misdirect calls.

The first authentic computer hackers came in the 1960s. During those times, computers were mainframes, locked away in temperature controlled, glassed in areas. It cost a lot of money to run these machines, so programmers had limited access to them. The smarter students, usually MIT students, had an insatiable curiosity about how things worked. So, the smartest ones created what they called "hacks", programming shortcuts, to complete computing tasks more quickly. In some cases the shortcuts were better than the original program. One of the hacks that was created in the 60s, 1969 to be exact, was created to act as an open set of rules to run machines on the computer frontier. It was created by two employees from the Bell Lab's think tank. The two employees were Dennis Ritchie and Ken Thompson and the "hack" was called UNIX.

What is Hacking ?

Hacking refers to activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks. And while hacking might not always be for malicious purposes, nowadays most references to hacking, and hackers, characterize it/them as unlawful activity by cybercriminals—motivated by financial gain, protest, information gathering (spying), and even just for the “fun” of the challenge.

Hacking tools: How do hackers hack?

Hacking is typically technical in nature (like creating malvertising that deposits malware in a drive-by attack requiring no user interaction). But hackers can also use psychology to trick the user into clicking on a malicious attachment or providing personal data. These tactics are referred to as "social engineering."

In fact, it's accurate to characterize hacking as an over-arching umbrella term for activity behind most if not all of the malware and malicious cyberattacks on the computing public, businesses, and governments. Besides social engineering and malvertising, common hacking techniques include:

Types of hacking/hackers

Broadly speaking, you can say that hackers attempt to break into computers and networks for any of four reasons.

- There's criminal financial gain, meaning the theft of credit card numbers or defrauding banking systems.
- Next, gaining street cred and burnishing one's reputation within hacker subculture motivates some hackers as they leave their mark on websites they vandalize as proof that they pulled off the hack.
- Then there's corporate espionage, when one company's hackers seek to steal information on a competitor's products and services to gain a marketplace advantage.
- Finally, entire nations engage in state-sponsored hacking to steal business and/or national intelligence, to destabilize their adversaries' infrastructure, or even to sow discord and confusion in the target country. (There's consensus that China and Russia have carried out such

attacks, including one on Forbes.com. In addition, the recent attacks on the Democratic National Committee [DNC] made the news in a big way—especially after Microsoft says hackers accused of hacking into the Democratic National Committee have exploited previously undisclosed flaws in Microsoft's Windows operating system and Adobe Systems' Flash software. There are also instances of hacking courtesy of the United States government.)

Latest news on hacking

A new report from Microsoft has revealed that at least six separate Russian nation-state actors have launched damaging cyber-attacks against Ukraine since the invasion began earlier this year.

The study (PDF), released yesterday (April 27), detailed how Microsoft researchers have tracked at least 237 “cyber operations” originating from Russia.

These attacks “have not only degraded the systems of institutions in Ukraine but have also sought to disrupt people’s access to reliable information and critical life services on which civilians depend, and have attempted to shake confidence in the country’s leadership”, Microsoft states.

It comes more than two months after Russian troops invaded neighboring Ukraine, sparking the beginning of a war that has so far claimed tens of thousands of lives.