HACKING

By Abi & Pavi

Contents

What is hacking?

- Hacking is the gaining of access to a computer and viewing, copying, or creating data without the intention of destroying data or maliciously harming the computer.
- Hacking refers to activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks.

Who is hacker?

- A hacker is any person engaged in hacking.
- A hacker is a person skilled in information technology who uses their technical knowledge to achieve a goal or overcome an obstacle, within a computerized system by non-standard means.

History

- First computer hack was in late 1960's when Bell Labs successfully hacked and modified a UNIX operating system.
- In 1980's people started to hack computer system to gain access to confidential information.
- Several groups formed to tap into sensitive information.
- Gangs began fighting in early 1190's.
- In late 1990's law enforcers began to take hacking seriously by making stricter laws against hacking.

Types of Hacking

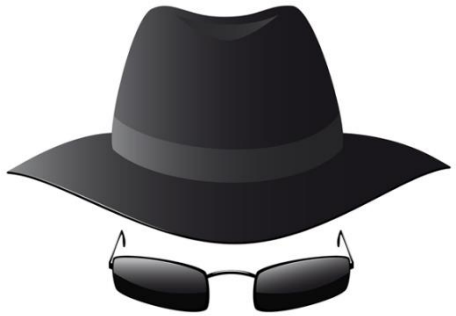
1. Website Hacking
2. Network Hacking
3. Ethical Hacking
4. Email Hacking
5. Password Hacking
6. Online Banking Hacking
7. Computer Hacking

Type of hackers

1. Black hat hackers
2. White hat hackers
3. Grey hat hackers

Black Hat Hackers

- Black hat hackers are **malicious hackers, sometimes called crackers.**
- Black hats lack ethics, sometimes violate laws, and break into computer systems with malicious intent, and they may violate the confidentiality, integrity, or availability of an organization's systems and data.
- They Hacks system for malicious purposes or self-gain.
- Some wipe memory off of other computers for fun.



Grey Hat Hackers

- A grey hat hacker is **someone who may violate ethical standards or principles, but without the malicious intent ascribed to black hat hackers.**
- Grey hat hackers may engage in practices that seem less than completely above board, but are often operating for the common good.

White Hat Hackers

- A white hat hacker or ethical hacker is **an individual who uses hacking skills to identify security vulnerabilities in hardware, software or networks.**
- However, unlike black hat hackers or malicious hackers white hat hackers respect the rule of law as it applies to hacking.
- A white hat is an ethical security hacker.
- The good guys in the hacking world.

The dark side of Hacking

- To gain unauthorized access in order to tamper with or destroy information.
- Gain unauthorized access to system or computer services in order to steal data for criminal purposes.
- Terrorism.

Why do hackers hack?

i. Money: lot of hackers are simply motivated by money. Hackers don't just hack businesses and ask for a ransom.

ii. Steal/Leak Information: One of the most common reasons for hackers to hack is to steal or leak information.

iii. Disruption: These hackers don't care about money or data; they seem to feel that they have a higher purpose in life.

iv. Espionage: Espionage is another type of theft except, instead of direct financial gain, the hackers are seeking protected information. Stolen information can be either sold or used by adversaries to gain tactical advantages.

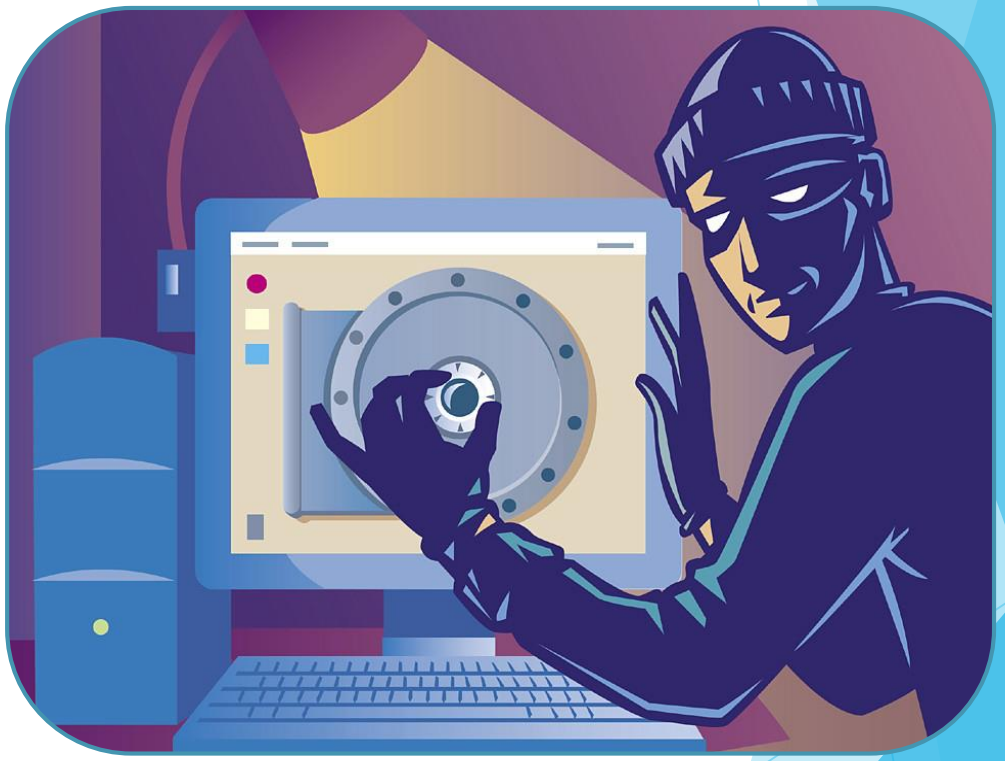
v. Fun: A lot of hackers will tell you that breaking into a secure system is an enjoyable hobby that tests their knowledge and skills.

What to do when system got hacked

1) First thing to do is to disconnect your system from internet.
2) Run anti-virus scan on your computer.
3) Take it to a professional if problems persist.

Crackers

- Person who enter into others system and violet the system, damage the data, create havoc is called CRACKER.



Hackers vs. Crackers

Hackers	Crackers
It’s ethical	It’s unethical
Some hackers do have ethical certificates	Crackers do not have ethical certificates
It is use for good purposes too	Not used for good purposes

Hacking tools

- **Scanners:** Program that automatically detects security weakness in remote host. Port scanners are used for hacking.
- **Telnet:** It’s a terminal emulation program that allows us to connect to remote system.
- **Ftp:** File transfer protocol is also used for hacking too.

Prevention

- Install anti-virus software.
- Install a firewall/ make sure you have one.
- Have backups of any important information on your computer stored separately.
- Use unique and strong passwords.
- Don’t use unauthorized applications.
- Don’t click unauthorized website links.

Prevention - Firewall maintanance

- Block all access by default. When configuring a firewall, it's important to start by blocking access to the network from all traffic. ...
- Regularly audit firewall rules and policies. ...
- Keep the firewall up-to-date. ...
- Keep track of authorized users.

Advantages of Hacking

- To recover lost information, especially in case you lost your password.
- To perform penetration testing to strengthen computer and network security.
- To put adequate preventative measures in place to prevent security breaches.
- To have a computer system that prevents malicious hackers from gaining access.

Disadvantages of Hacking

- Massive security breach.
- Unauthorized system access on private information.
- Privacy violation.
- Hampering system operation.
- Denial of service attacks.
- Malicious attack on the system.

Thank you !!