MES PILLAI COLLEGE OF EDUCATION AND RESEARCH
CHEMBUR NAKA.

HACKAHOLIC – S.Y.B.ED (2016-17)

HACKING

Origin of hacking

It all began in the 1960s at MIT, origin of the term “hacker”, where extremely skilled individuals practiced hard-core programming in FORTRAN and other older languages. Some may ignorantly dub them “nerds” or “geeks” but these individuals were, by far, the most intelligent, individual, and intellectually advanced people who happen to be the pioneers and forefathers of the talented individuals that are today the true hackers.

The true hackers amongst our societies have an unquenchable thirst for knowledge. Boredom is never an object of challenge for hackers. They have an almost anomalous ability to absorb, retain, and exert vast amounts of knowledge with regard to intricate details

Hackers used to be viewed as people who sat locked in a room all day programming nonstop, hours on end. No one seemed to mind hackers back in the 1960s when this was the most widely excepted reputation. In fact, most people had no idea what hacking was.

The term hacker was accepted as a positive label slapped onto computer gurus who could push computer systems beyond the defined limits. Hackers emerged out of the artificial intelligence labs at MIT in the 1960s.

A network known as ARPANET was founded by the Department of Defense as a means to link government offices. In time, ARPANET evolved into what is today known as the Internet...

INTRODUCTION

A hacker is an individual who uses computer, network or other skills to overcome technical problem.

Hackers have developed methods to exploit security holes in various computer systems. As protocols become updated, hackers probe them on a never ending mission to make computing more secure when hacking first originated, the urge to hack into computer systems was based purely on curiosity.

Hackers find and release the vulnerabilities in computer systems which, if not found, could remain secret and one day lead to the downfall of our increasingly computer dependant civilization.

Hackers come up with useful new computer systems and

What’s inside?

Hacking team

- Anusha Devi Sekar– (01)
- Roshini Maria Joseph -(22)
- Sivaranjani Ganeshan- (32)
- Shilpa waghe (39)

TYPES OF HACKERS

Hackers can be classified into different categories such as white hat, black hat, and grey hat, based on their intent of hacking a system. These different terms come from old Spaghetti Westerns, where the bad guy wears a black cowboy hat and the good guy wears a white hat .

Black hat hackers

- The black hat hacker is the one who hacks for malicious intent - he is the bad guy.
- This type of hacker uses his or her skills to steal money or data, knock a computer system offline, or even destroy them.
- Some of these hackers love to see their work and name in the news, so they would try to target big name organizations and companies.
- Black hats also try to break into computer systems to steal credit card information and possibly steal valuable information to sell on the black market.
- The black hat works outside of the law.
- They work alone wolf, or with a team.

White hat hackers

- White hat hacker's use their skills to improve security by exposing vulnerabilities before malicious hackers can detect and exploit them
- Although the methods used are similar, if not identical, to those employed by malicious hackers, white hat hackers have permission to employ them against the organization that has hired them
- White hat hackers are usually seen as hackers who use their skills to benefit society.
- An organization can hire these consultants to do tests and implement best practices that make them less vulnerable to malicious hacking attempts in the future.
- For the most part, the term is synonymous with "ethical hacker.

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.
- Many people see the world of IT security as a black-and-white world.
- However, grey hat hacking does play a role in the security environment.
- One of the most common examples given of a grey hat hacker is someone who exploits security vulnerability in order to spread public awareness.

HOW DO PEOPLE HACK

- **Part 1**

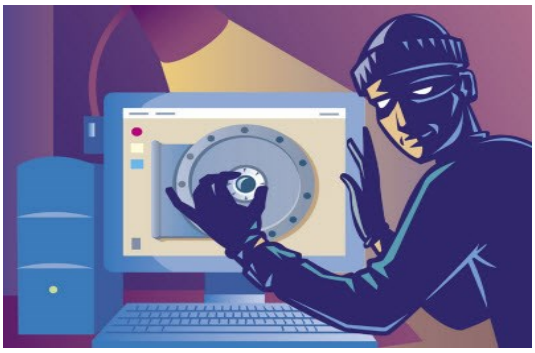
1. Before you hack

- Learn a programming language
- Know your target

Part 2

2. Hacking

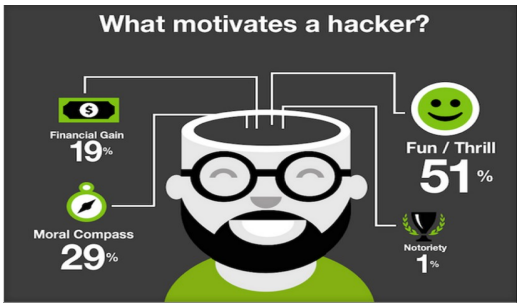
- Use a nix terminal for commands
- Secure your machine first
- Test the target
- Determine the operating system
- Find the path or open port in the system
- Crack the password or authentication process
- Get super user privileges
- Use various tricks
- Create back doors



WHAT MOTIVATES A HACKER

Understanding the motives of potential attackers has long been a problem for many people. While there are infinite possible motives, Its believe it's most important to understand that no matter the situation, there is always something that another wants, an agenda that someone wants to further, or a belief that someone disagrees with.

- Political Gain
- Moral Disagreement
- Cultural and Religious
- Revenge and Defamation
- Thrill and Entertainment
- Nation state
- Abduction and child crimes
- Intellectual property and trade theft



PHISHING ATTACK– THE NEW TREND

Phishing attacks often use email as a vehicle, sending email messages to users that appear to be from an institution or company that the individual conducts business with, such as a banking or financial institution, or a web service through which the individual has an account.

- Emails from people you know claiming stranded in a foreign country, asking you to wire money so that they can travel home
- Emails claiming to be from reputable news organisation capitalizing on trending news
- Emails threating to harm recipients unless sums in the thousands of dollars are paid
- Emails claiming to be a confirmation of complaints filed by the recipients. The links and attachments, of course ,contain malicious code

Beware of phishing scams.
Don't take the bait! Be suspicious of anyone that asks for your personal information.

Well known hackers in India

Its impossible` said pride

Its risky said experiences.

Its pointless said reason.

If you really are hacker!

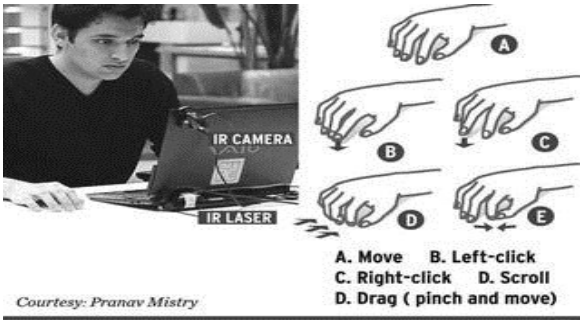
Then give it a try

- Rahul tyagi

Aside from being an expert on breaking and entering computers Rahul tyagi is also an author and a talented actor

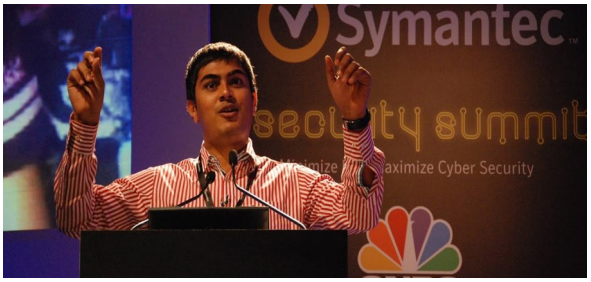
- Pranav mistry

This hacker extraordinaire is also famous for the invention of sixth sense a technology that is used by NASA and also invisible computer mouse



- Ankit fadia

Writing a book titled “unofficial guide to ethical hacking at the age of 15 is a far cry from playing football at the tender age and the rest is history when it come to world renowned Indian ethical hacker



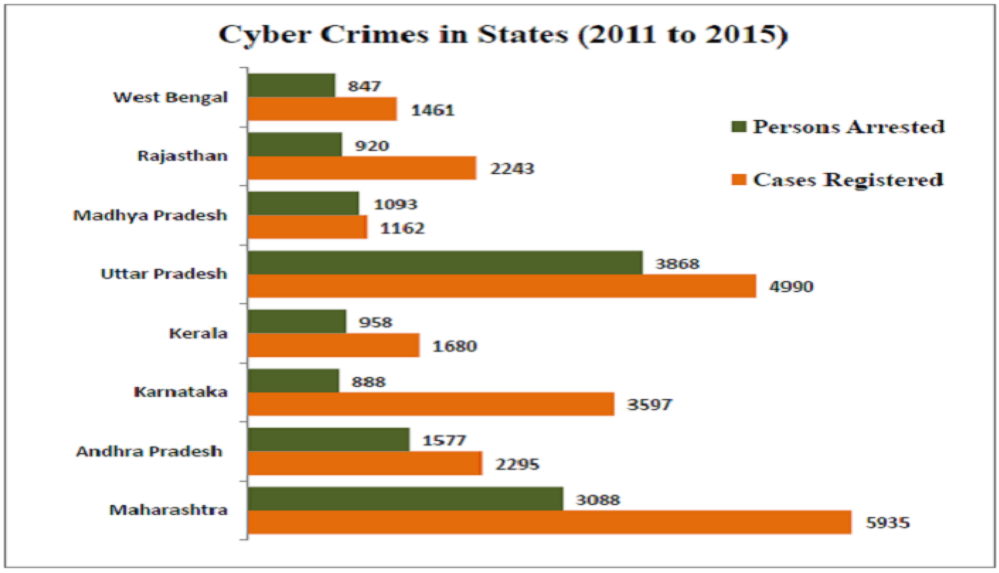
- Vivek ramachandran

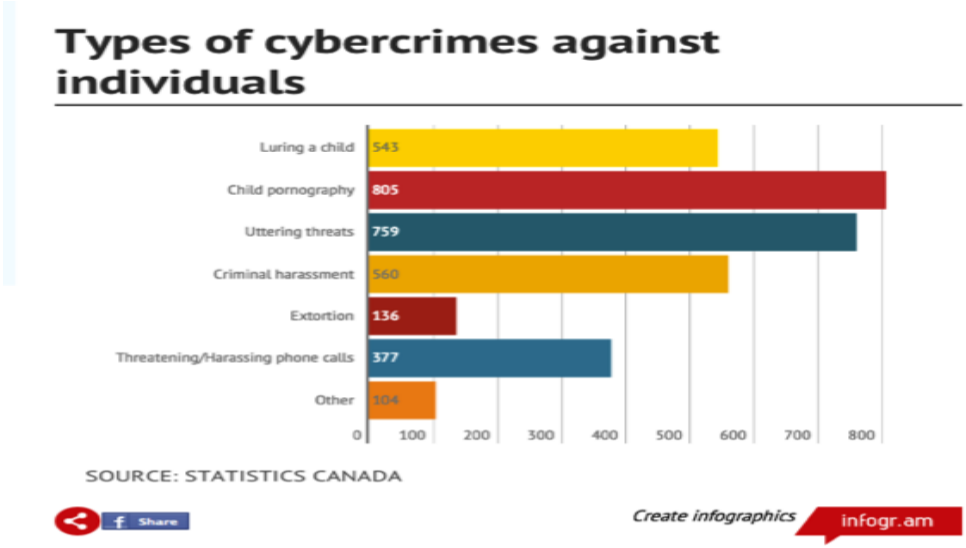
Having won many awards including one from both Microsoft and cisco.

- Jayant krishnamurthy

This real hacker has interest Ranging from information extraction to knowledge representation and common sense reasoning in artificial intelligence. He is also a computer theorist and researcher.

Statistical data





HOW TO PROTECT YOURSELF FROM BEEN HACKING

Part 1

- Keeping your accounts secure

Create complex pass-words

Use password manager

Don't give out your pass-words

Change your password often

Read privacy policies carefully

Logout accounts once done

Part 2

- Keeping your Phone secure

Use touch id

Change phone passcode often

Part 3

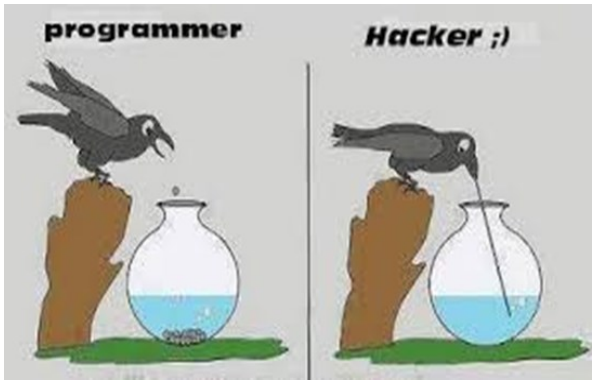
- Keeping your computer secure

Backup your data fre-quently

Avoid clicking suspicious links

Install or activate firewall

Fun zone...



http://TheFunnyPlace.net

Conclusion

As technology has improved our lives have become easier in many ways, but with this blossoming industry new types of criminals have also been created. A criminal does now not even need to leave the house in order to steal money, but can do so simply by hacking into their victim's computer and accessing confidential data.

Hacking is not always illegal though, and this has also looked at the ways in which there is an increasing demand for computer experts to become ethical hackers in order to further promote and protect computer security. This introduction to the world of hacking has revealed that hacking is not a simple activity but a huge spectrum of different behaviors that involve a wide range of techniques and motivations .