Hacking: Illegal but ethical?

Ethical Hacking, is the buzz word going around these days, especially among the youth. Youngers have a fancy to learn something to flaunt their knowledge, to project their technological supremacy over others or at least to point out to others how weak their computer system or their data is. It is in this context that the words "Ethical Hacking" assume significance.

The word "hacking" literally meant, earlier, 'to cut into pieces in a rough and violent way' and was most often used in the context of 'hacked to death' referring to a savage attack on a victim. However, of late, the word is very popularly used in technological parlance, to refer 'computer hacking' only. In this context, it refers to 'the activity of using a computer to access information stored on another computer system without permission' generally with a malicious intention. This usage of hacking and its derivatives like 'hacker', 'ethical hacker', 'black-hat hacker' or 'blue hat hacker' are the ones we are going to discuss here.

From a legal perspective, our Information Technology Act, 2000 in its earlier version defined the activity of hacking in Section 66 as follows:

> **Sec.66:** Hacking with computer system.
>
> (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or delete or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack;
> (2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.
>
> (***This section has since been amended and is no longer there, as explained in the later part of this article***).

From the above, we can easily understand that hacking per se is an offence with the Act even defining the punishments for the illegal activity. However, it is common these days that most training institutes in computer network and Internet technology, offer training courses titled "Ethical Hacking". Such courses include theory classes with some practical training sessions too on IP Addressing (the number with which a computer in a network can be identified) pattern, tracing an IP Address, and such other hands-on training and practical inputs on the nuances of the technology.

Is hacking really ethical? Some training courses claim and admit that while these skills can be used for malicious purposes the inputs will contain only the ethical and legal aspects of the associated technologies. They say that by and large, the training offers inputs on how to protect your computers and safeguard the data, thwarting any attempt of criminals to hack into it. On the flip side, however, the problem starts when one acquires the skills with which one can hack into the computer systems of others.

Crime as a Service: It is common knowledge that many crimes in the physical world can be organized, managed and committed by hired hooligans with the real mastermind not coming out at all and mercenaries are engaged to commit even deadly and heinous crimes on a contract basis. Similarly, in the recent years, Crime as a Service (like SaaS meaning Software as a Service) is gaining in popularity, nay, notoriety. The services of young misguided 'qualified' tech-savvy criminals are normally engaged, sometimes in cross-border assignments too. Interestingly, to facilitate such 'trade' across national currencies avoiding national financial regulations, the payments in these cases are made in crypto currencies like Bitcoins, Litecoins, Ethereums etc (which do not have a physical format and are only digital currencies not coming under the regulatory monitoring of any nation).

Now comes the interesting question: If hacking is a crime, how can some one teach the technology under the name of "Ethical Hacking"? In other words, does the prefix "Ethical" sanctify any illegal activity? Does any crime become a legal activity, just because the word "Ethical" is prefixed to it and taught in institutes under the garb of teaching the self-defence technique only. On similar lines, if one were to teach the art of self-defence say in a martial art like karate or kung-fu, can the course be called "Ethical Attack" or "Ethical Arson" or even "Ethical burglary"? Sounds crazy?

Perhaps, to put an end to this kind of interpretations, the Information Technology Amendment Act, 2008 removed the word "hacking" in its Section 66, though the description of the activity of illegally trespassing or accessing others' computer resources still remain an offence and continues to be punishable, as much as in the original Act. As stated in the beginning of this article, the Section 66 as stated therein is no longer there though the revised section still deals with the illegality of hacking, (without mentioning the word 'hacking') and stipulates punishment for it.

Types of hackers: Popular and widely accepted technology books use the word "Ethical Hacking" to denote the activity of accessing the computer resources (data or information in storage or in transit etc) **with the permission of the data owner** to prove to the owner that their computer security system is vulnerable. As opposed to this, if the same activity is carried out WITHOUT the knowledge of the owner or with a criminal intention (what in legal circle is referred to as "***mens rea"***) it is referred to as 'cracking'. Hence we can say that cracking is an offence and ethical hacking is not, since it is done with the knowledge of the data owner. Such ethical hackers use their skills for good purposes and are also mostly referred to as "White Hat Hackers". Crackers are malicious people and are always referred to as "Black Hat hackers" operating mostly underground in what in technology circles is called "dark web". Sometimes there are some categories between these two, called "Grey Hat hackers" and "Blue Hat hackers" referring to those who find out the weaknesses in the system though not with any specific intention or effort, but AFTER finding the

vulnerability, bring it to the notice or use it or misuse it, too! Let us not go deeper into all these.

Since hacking has always been an interesting topic all these years, we find many youngsters often in late teens and early twenties well versed in hacking technology practicing it as an art ie a natural art like drawing, painting kind of skill etc.

We interviewed a nationally acclaimed and popular Ethical Hacker Shri Sai Satheesh, a young entrepreneur, founder and CEO of Indian Servers, Vijayawada, who is an author of widely read books and articles on hacking and, whose interview has appeared in most of the national print and electronic media. He has given hacking demo in various fora and addressed very high profile audience and gathering like IPS officials, top government officials all over India, especially in Andhra Pradesh and Telengana states. He states that "Hackers are the people who think out of the box" though sometimes they do malicious operations with the data they have collected, often breaching the privacy of ordinary people by accessing the computer resources which may even stop the services ie deny the services to genuine people who access such websites.

On the question of safety of mobile phones from the point of view of hacking and unauthorized access, Shri Sai Satheesh adds that 'Smart phones are not safe when compared with normal phones' since they are more powerful than even most of the computers and critical data like banking information, travel related information, stocks or other investment related data and personal chats containing sensitive information are all normally stored there, which would be very handy for the criminals to hack.

When enquired about safety tips, the young techie says that 'We should have utilities like 'applocker' in our phones, which will ensure that unauthorized apps are not getting downloaded in our mobiles. We should also have multiple authentications as well as multiple passwords as one password for each application. When children use the mobile, we should ensure that family safety apps and parental control apps are also in place. In the case of iphones, (Apple phones), he adds that we should ensure that 'jailbreaking' is not there ie the mobile should have only the official and authorized AppStore only. 'Jailbreaking' permits access to the apple phone's iOS allowing installation of software which is not available through the official AppStore. It circumvents the controls of the iOS and permits any app to be downloaded.

To conclude, perhaps it is time that the governments, more particularly the Central Government had some enactment in place to define and regulate the activity of hacking and unauthorized access to the computer resources. The proposed Data Privacy Act has provision for a Data Privacy Authority, to serve as a national level data protection authority to supervise and regulate data fiduciaries who handle the data, process them and transmit them. We hope that when the Act is in place, more clarity, more regulations and control may emerge on the storage, access and transmission of data among the various stake holders.

*****.*****