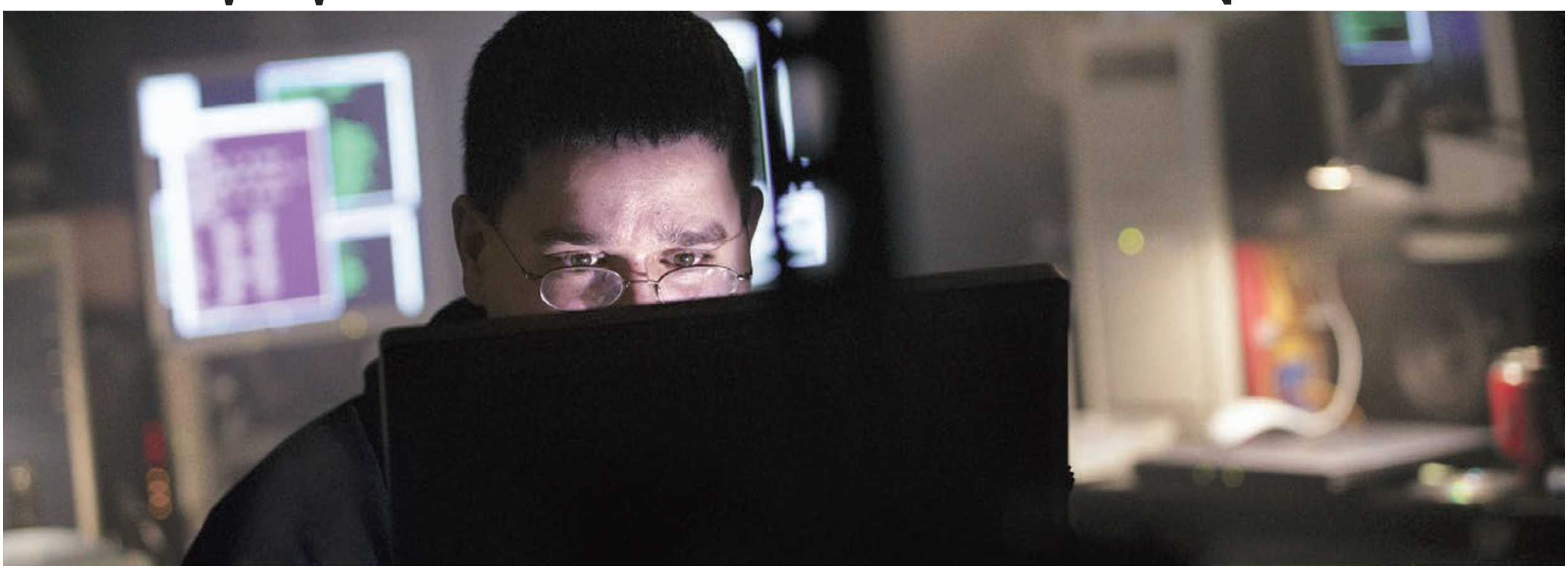
17 OCTOBER 2015

Business Standard

WEEKEND



ONE HACK OF A JOB

Hackers have begun to emerge from the shadows of suspicion, writes **Dhruv Munjal**

Ankit Fadia, the ethical hacker, deeply divides public opinion. He has been described as a child prodigy and a security charlatan. He has written books on cyber-security and offers online courses on the subject, yet his own site has been hacked at least nine times, including once by a Pakistani hacker collective, and on at least two occasions, the website was taken over by spammers selling Viagra. His claims of being consulted by FBI and CBI remain unverified, though security agencies are unlikely to advertise such engagements.

But all that scepticism did not stop the Narendra Modi government from appointing him a brand ambassador last month for its Digital India campaign. It was tacit acknowledgment of hacking as an acceptable activity — a legitimate career option, an honest way to earn one's livelihood.

Even before this official approval could be stamped, India's smart small entrepreneurs had seen the opportunity and started to train youngsters in hacking, and companies had begun to employ them.

Inside a slender classroom at the Net Hub computer institute in New Delhi's South Extension, a bespectacled red-turbaned man writes furiously on a white board. His students frantically take down notes to keep up with him. His squeaky voice is occasionally punctuated when a student raises his hand and asks a question. "Somebody out there will be smarter than most. But you have to be smarter than him," he spells out the magic mantra, as the enraptured group listens keenly.

At Rooman Technology next door, a marble staircase opens into a narrow, dingy corridor where the institute holds its classes. Students, in a small group, are staring intensely at their computer screens — they have been given a test they need to finish in 30 minutes. The classrooms here are tiny, and no chair is unoccupied. The teachers have little time to talk to outsiders. More students, carrying backpacks, saunter in as I make my exit.

Most students at these institutes, all in their late teens or early twenties, will go on to become experts in cyber-security, while some will pick up the skills to get the thrills of a joyride in cyberspace.

Mohit Chaudhry of Net Hub, dressed in a navy blue shirt and beige trousers, his table bedecked with a line of Apple products and a splashy silver watch on his wrist, says earlier he would get "people who wanted to get into hacking because it was a hobby for them. Now, they want to make a career out of it". Net Hub offers graduate students a host of certified hacking courses that start from about ₹30,000 (for a 40-hour course).

There may be nothing fanciful about these schools but they have given India a rock-solid reputation for training in hacking. Koenig Solutions, nestled in a relatively quiet corner of west Delhi's Moti Nagar, is the place where National Security Council contractor-turned-whistleblower Edward Snowden sharpened his programing and hacking skills in September 2010.

Folks here downplay the Snowden connection, but then hackers prefer to fly under the radar — it's a part of the work ethic. It is clear that Koenig attained critical mass a while ago. The beige sofas in its waiting lounge are elegant and the air conditioning just right. A section of the walls is painted in fulgent red, with massive television screens gently hanging on them. Koenig offers ethical hacking courses in as many as 80 classrooms. It is hard to find an empty seat in the evening.

India is in the midst of the Internet revolution: e-governance, e-commerce and net banking are expanding by the day. While this has made life easier for people at large, it has posed a serious security threat. Cases of data theft, defacing of government and university websites, and hacking of social media accounts for sheer adventure are rampant.

The proof of malice on the Internet was blatantly exposed this past week when cyber criminals duplicated the email address of Oil & Natural Gas Corporation and convinced a Saudi Arabia-based firm to transfer ₹197 crore to their account.

In June, a group called TeamUnknown hacked into the website of app-based taxi aggregator Ola, gaining access to sensitive credit card information of customers and unused vouchers. The company later denied any breach.

KOENIG SOLUTIONS IN WEST DELHI IS WHERE NATIONAL SECURITY COUNCIL CONTRACTOR-TURNED-WHISTLEBLOWER EDWARD SNOWDEN SHARPENED HIS PROGRAMING AND HACKING SKILLS

According to a report published by security services firm FireEye earlier this month, India is quickly becoming a "strategic target" for cyber criminals, with nearly 38 per cent of Indian organisations being at the receiving end of some form of cybercrime in the first half of 2015.

This is where the hackers come in. They check the information technology systems for breaches and weak points and then secure them. But their numbers are woefully short of the demand. In 2013, the Union ministry of information technology estimated that India would require up to 500,000 cyber security professionals by 2015 — a goal that has been far from fulfilled. According to Sandeep Sengupta, founder of the Indian School of Ethical Hacking in Kolkata, that number is around 40,000 at present.

In spite of the shortfall, the rise of ethical hacking in India has been undisputed. Institutes such as Net Hub and Rooman are proof of that. There has been a mushrooming of ethical hacking training institutes in areas such as Pitampura, Patel Nagar and Rohini in the national capital in the last few years.

Fadia says that things have changed dramatically since he started out. "Earlier, hacking was limited to only a few students from top colleges like the IITs and NIITs. Now, with greater awareness and the pitfalls of the technology world, that trend is changing."

There is a little doubt that ethical hackers have greater acceptability than a decade ago. However, the stigma attached with a "hacker" refuses to fade away completely. Most employers choose to call them "risk-assessment" or "cyber-security" experts. Social buy-in is not yet absolute, and industry leaders are desperate to turn around the negative image of the profession.

"The word 'hacker' has always had a negative meaning. In actuality, a 'hacker' is someone who can build stuff and solve real-life problems," says Sachin Gupta, the 25-year-old founder and CEO of HackerEarth, a Bengaluru-headquartered online platform for developers from across the world. "The term 'ethical hacking' had to be devised to separate the good from the bad."

Earlier this year, HackerEarth posted a petition on *www.change.org* — aimed especially at the media — to highlight the difference between a "hacker" and a "cracker": a "cracker" is someone who is adept at security breaking, whereas a "hacker" prevents such incidents, says the petition.

Saket Modi, ethical hacker and CEO of Lucideus Tech, a cyber-security consultancy that helps some of the biggest banks in the world secure their data, says the general perception of a hacker must change. "A hacker is somebody who can make anything do something that it is not meant to do," he says. "People must understand that there is nothing wrong in hacking. For me, Steve Jobs remains the greatest hacker of our time."

Modi proudly adds that he has a dedicated team of hackers that prevents fraud. "We hack for a living and we are proud of it."

There is evidence that perceptions are changing and hackers could soon be mainstream.

Rishiraj Sharma is perhaps India's youngest independent ethical hacker and cyber security consultant. At 18, his services have been acknowledged by more than 50 companies, including Google, Microsoft and Nokia. The moment he starts talking about what he loves doing, the boyish enthusiasm is palpable. But the amateurishness dissipates quickly, giving way to a stern, unbiased professional voice. "At present," he says, "hacking is an unavoidable part of any technology that deals with information, people or data. This is why there is special emphasis on 'security'."

The hacking sector, in the last few years, has grown faster than technology itself. Sharma says that is due to the unique nature of the profession. "The hacking ecosystem is simple but unique. A hacker is always above all security measures, since he has to always be first," he says. "A secure system/network can only be developed after all the possible methods to hack it have been accounted for."

"A HACKER IS ALWAYS ABOVE ALL SECURITY MEASURES, SINCE HE HAS TO ALWAYS BE FIRST. A SECURE SYSTEM CAN ONLY BE DEVELOPED AFTER ALL METHODS TO HACK IT HAVE BEEN ACCOUNTED FOR"
RISHIRAJ SHARMA
Ethical hacker

An invention is useless unless it is fully secured. Hence, job opportunities in the cyber security sector have opened up. Companies such as Tech Mahindra, KPMG, Snapdeal and Flipkart regularly hire professionals for their cyber-security vulnerability threat and assessment operations. "But such people are not the easiest to find," says an executive of one such company.

In spite of the growing interest, India is not yet up to speed with the kind of talent that is required to thwart serious cyber-attacks. Most successful hackers operate individually and are seldom available to big companies to tackle security threats.

Moreover, the lack of talent coming through is a grave concern. "Hacking," says Trishneet Arora, a young ethical hacker who heads TAC Security Solutions, "is a lot like acting. You have both mediocre as well as brilliant actors. It all depends on how good you are." (The 20-year-old's outfit claims it has provided security services to CBI, Punjab Police, Reliance Industries and Amul in the past.)

Modi adds that becoming a hacker requires enormous intellect, which is rare to find. "At the end of the day, you have to be better than the person who originally developed a program. And, everybody can't do that."

That's why cyber security expert Rakshit Tandon feels that ethical hacking must mature and evolve. "For youngsters, hacking is still all about the 'thrill' factor. They want to see magic on their screen. That has to change. Intruding on other people's privacy must stop."

For that to change, the industry needs an urgent overhaul in the way youngsters are trained and nurtured. For long, the industry has been grappling with one major problem — the lack of good teachers. Sengupta says that he has been recruiting for the last 16 years, but still finds it difficult to the find the right members for his team.

He adds that at his institute, more than 500 ethical hackers are trained every year who can also teach, but that number is still not sufficient. "In the near future, every computer will require an individual guardian. This demand will only grow," says Tandon.

Fadia tells me that the one thing missing from the hacking ecosystem is a full-fledged government-recognised hacking institute . "A university that can offer a two-year master's degree in cyber security, or even a PhD, will be a game changer. I hope the government comes up with something like that," he says.

Ethical hacking in India may have made large strides, but there is still some distance to cover.