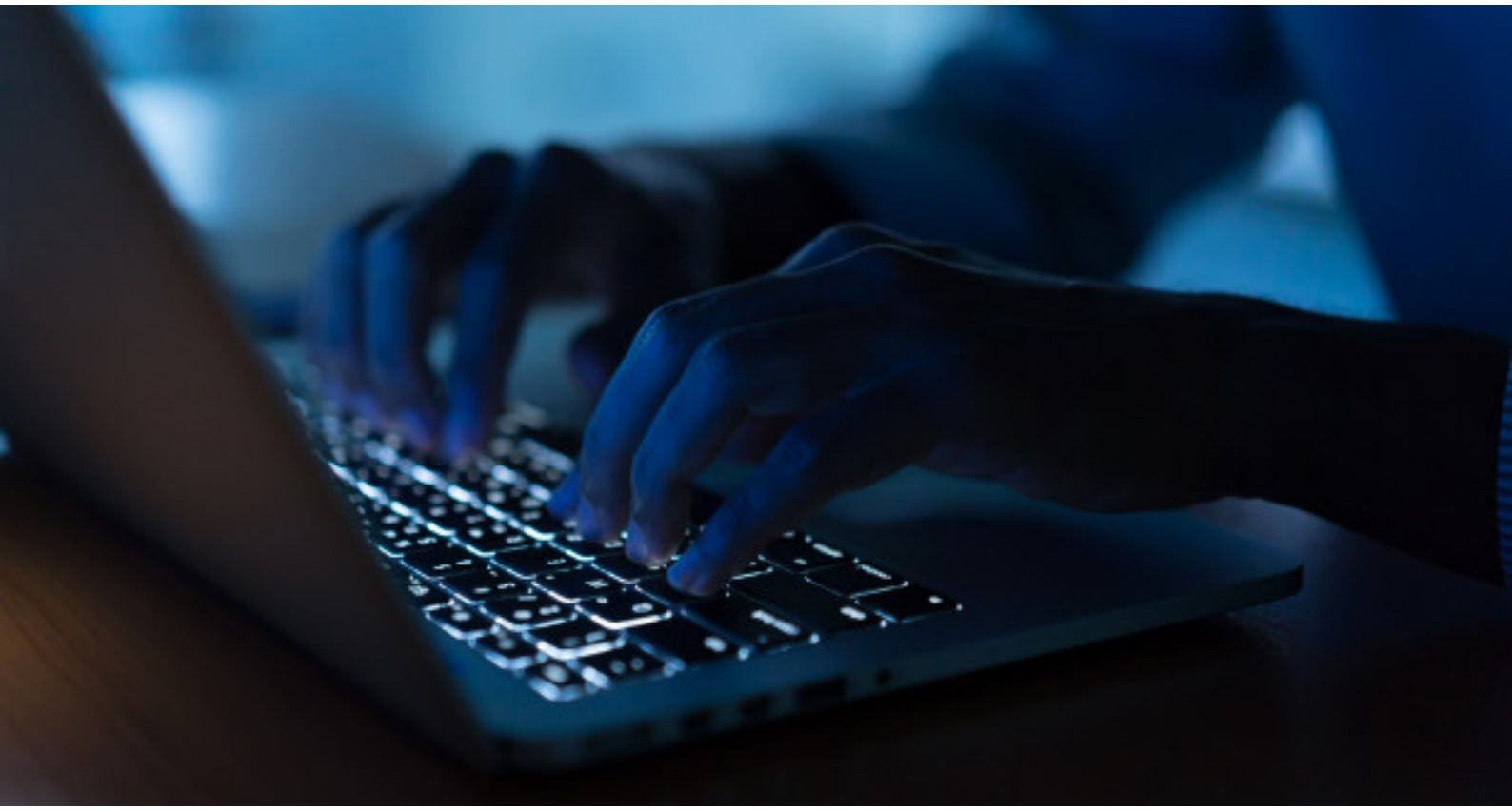
REDTEAM®
HACKER ACADEMY

CYBERSECURITY IS THE NEED OF THE HOUR AND A PROMISING CAREER



Technology in your laptops and phones are much more advanced than it took America to reach the moon. But everyone knows somone who has been hacked or who has had their identities stolen or lost control over their Facebook account. Experts have now recognized that the problem will never go away unless we have enough capable cyber security expertise who are able to secure our cyberspace.

Your password is never enough. There are always efficient hackers for every efficient encryption. Every other day a new technology comes up that is connected to networks. The more we are connected the more our personal data, business, property and information security are under threat and Cybersecurity is our only solution

REDTEAM®
HACKER ACADEMY

Impact of Cyber Attacks

Over half a billion people in India are using internet today.

This number is further increasing due to digitalization of private as well as Government sectors.

According to APAC Cyber Resiliency and Risk Report **cyber security is fast becoming an integral part of digital transformation,** with 49% of companies being 'extremely' involved and 41% 'very involved' in the digital transformation process.

58% of Indian companies is said to have high impact on business by cyber security attacks according to APAC Cyber Resiliency and Risk Report

The report also predicts top three threats faced by enterprises globally to be **Data Breach (62%), Data Tampering (49%) and fraud (43%),**

India has a higher rate of cyber attack than global average according to a survey by security firm Sophos

Cyber security is the need of the hour. The cybercriminal attacks have fought their way through too far, even penetrating into major elections in many parts of the world. There are expert hackers that can cripple elections overnight

78 % of Indian organisations are attacked by cyber-attack as compared to 68% which is the global average

Report by Indian Computer Emergency Response Team (CERT-In) reveals that 91% respondents believe that cyber stacks will increase by 2022

REDTEAM
HACKER ACADEMY

> That we live in a world where people, organizations, and occasionally countries could have people that would like to wipe out a large percentage of the American people, or maybe other countries, as well,"
>
> And that you now have capabilities — which I always thought, until recently, might classify it as nuclear, chemical, and biological — but I think you have to add cyber now."
>
> **WARREN BUFFET**

While organisations can put a cost on cyber security damages related to a data breach, reputational damage, impact on sales and other areas are difficult to measure, implying that the level of belief that a cost can be placed is higher than expected,"

Said Sanjay Manohar,
managing director of McAfee India

Future of Cyber security

India is world's second largest hub for IT service providers and tech innovators. But this has turned India into a plot for major cyber attacks. Therefore organisations in India have to face huge loss if not protected by sufficient security measures.

One such initiation by the government is the National Cyber Security Strategy 2020 to ensure safe secure, trusted, resilient and vibrant cyber space for our Nation

In response to the alarming cyber attacks in the country the government is also pushing companies and organisations to adopt more cyber security measures by bringing up minimum security baseline policies.

Banking sectors have already reconciled by taking appropriate cyber security measures into their system.

Energy, healthcare and manufacturing sectors are emerging with their own unique cyber security challenges. More Cyber security professionals and products will have a vast market and roles to play in these sectors in the future.

Dynamic technological development without adequate information security measures have made internet very insecure. Some of these include cloud computing, 5G internet, Artificial Intelligence and Internet of things over the internet.

While digitalization is seen as the strategy for development for the future, digitalization's impact can go downhill if not accompanied by producing capable cyber security professionals.

"A report by a Cybersecurity venture estimates that there will be 3.5 MILLION unfilled jobs by 2021"

Through various survey reports experts now predict a huge demand for adequate cyber security infrastructure and professionals.

- According to Indian Computer Emergency Response Team (CERT –IN) Report cyber security market in the government sector is estimated to grow from USD 395 million in 2019 to USD 581 million by 2022
- The report further predicts that the cyber security market in India will grow at 1.5 times the global growth rate.
- PwC predicts that the digital payments' transaction value is estimated to grow at a CAGR of 20.2% from approximately USD 64.8 billion in 2019 to USD 135.2 billion in 2023.
- The number of social network users in the country is expected to grow from 326 million in 2018 to 422 million in 2022, second only to China.

Cyber security is important

Experts conclude that it is nearly impossible to for see a future without investing and building in cyber security. Every Industry shall be affected if we are not able to find enough cyber security professionals that could meet the future demand. Such a high demand is a challenge but a boon to those who are willing to build their career in cyber securitytt

Career in Cybersecurity

As cybercriminals relentlessly keep attacking the system, **organisations struggle with understaffed security teams.** The National Association of Software and Services Companies (NASSCOM) expresses that the demand for security professionals shall increase irrespective of sectors.

NASCOM estimates that India shall demand for 1 million cyber security professionals by 2020

The EY Survey highlights that even though 56% of organisations consider cyber security as an indispensable part of their operations however skill shortage acts as a major issue

All these reasons add up for making cyber security the most demanded workforce of the year and years that follow.

With the increasingly technologically driven society, the rise in attacks and demand for security in cyberspace is more than ever before. This has led to **350%** growth in cybersecurity positions from 2013 to 2021 globally.

While a career in cyber security can be stressful, it's also extremely rewarding. You can either get certifications or work your way up the ladder or graduate in bachelors relating to cybersecurity and aim for more rewarding jobs. Cybersecurity is a fascinating and gripping field for tech enthusiasts who are interested in hacking.

The demand for ethical hackers is rising. This is an exciting field of career for those who are interested in hacking and has inbuilt skills for it. Through an ethical hacking certified training program, ethical hackers can learn to find vulnerabilities and find how insecure the system stands from unauthorised or criminal penetrations in a system or network in a lawful manner.

An average salary of cybersecurity professional in India is around 7 lakhs

REDTEAM HACKER ACADEMY

Roles in Cybersecurity

A career in cybersecurity can be stressful but it's extremely rewarding and there is always a job vacancy as well. The opportunities are endless. Cyberspace and technology are always changing and there is space for you to up skill and learn more.

The variety of roles that you can fill in this field is wide. Some of them are as follows.
Incident Responder - Prevent and protect against threats
Security Administrator - Keep security systems function in shape every day
Vulnerability Assessor - Find system vulnerabilities and provide solutions
Cryptographer - Write strong codes that by hackers can't break easily.
Security Manager - Keeps the system protected with an expert team
Security Architect - Outsmart online criminals by designing tough-to-crack security systems
Chief Information Security Officer - establishes and supervises vision, strategy and plan to ensure information security and technologies are well protected
Security Analyst - Plan and implement high-quality security measures
Security Auditor - Find the vulnerabilities in the security system before criminals do.
Security Director - makes rules and solves complex problems
Forensic Expert - manage legal compliance and protect the cyber world
Penetration Tester - Break into computers to find its vulnerabilities
Security Consultant - Advisory and implementing role in security solutions
Security Engineer - Engineers dedicated in building secure systems
Source code Auditor - Tests the quality and security of code before executing it in the program

You can always mix and match your skills and find the right role you want to specialize in.

As computers become faster and faster we have to develop new ways to make encryption too hard for computers to break. For this we need more professionals to secure the cyberspace. You can contribute to it too and grab the opportunity of this rewarding employment.