ABES INSTITUTE OF TECHNOLOGY

College Code: 290

Department of Information Technology

e-Newsletter

An official Bi-Annual e-Newsletter for internal circulation

July 2020

Volume :V

Estd.2007

Academic Session
2019-20 (Even Semester)

VISION

- To become a front runner in transforming the individuals into competent IT professionals, to meet the needs of evolving technology and serve the humanity.

MISSION

- To impart quality education with innovative teaching learning process to develop culture of research and innovation.
- Collaborate and interact with industry professionals, academicians to provide suitable forums to exhibit the creative talent of students.
- Provide leadership and planning for effective and strategic use of information technology.

NBA NATIONAL BOARD OF ACCREDITATION

AICTE | MIC Ministry of HRD | ABESIT College of Engineering | DFS Department of Financial Services | SMART INDIA HACKATHON 2020

ABESIT team received 1st prize of ₹ 1 Lac

Big Congratulations to **Pranjal Sharma** of Team Hex#Clan, student of IT department 3rd Year, as Team Hex#clan has secured **1st Position in Smart India Hackathon 2020** for developing "Instant Communication and solution provider".

LINK TO OUR TECHNICAL MAGAZINE:-

https://abesit.in/wp-content/uploads/2020/07/IT-Magazine-2019-2020.pdf

CENTER OF EXCELLENCE

Inaugural Ceremony of Center of Excellence

A MoU was Signed Between ABESIT & EduGrad in Inaugural Ceremony of the **Center Of Excellence of Data Science, AI-ML** on 29th January, 2020. The Ribbon Cutting Ceremony of the CoE was done in the presence of **Prof. (Dr.) Vipin Garg,** Advisor ABESIT, **Prof. (Dr.) M.K. Jha**, Director ABESIT, **Dr. Bipin Kumar Rai**, HOD IT Department along with the Industry Experts **Mr. Kishore Reddy**, Co-Founder of EduGrad and **Mr. Balaji Harsh**, Associate V.P EduGrad.

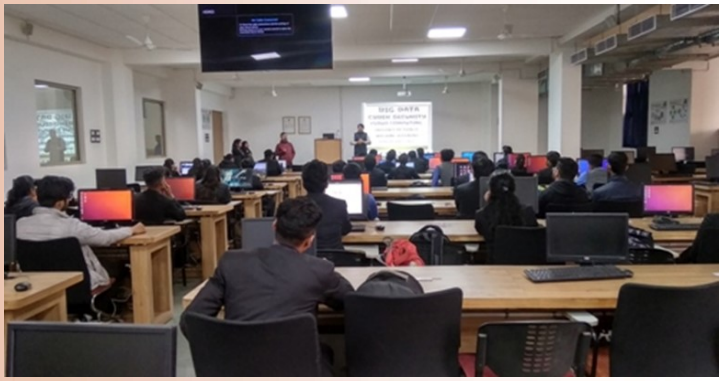
FACULTY DEVELOPMENT PROGRAM

S.NO.	Faculty Name	FDP Attended	Date	No. of Days/ Weeks	Venue
1	Ms. Shivani Sharma	Examination Reforms	29th April- 2nd May 2020	Four Days	AICTE
2	Dr. Bipin Kumar Rai	Google Cloud Platform Fundamentals: Core Infrastructure	24th May 2020	One Week	Coursera
3	Dr. Kaushal Kishor	Google Cloud Platform Fundamentals: Core Infra-structure	28th May 2020	One Week	Coursera
4	Ms. Sonika Bhatnagar	Cyber Security and Digital Safety during COVID-19 Pandemic	2nd June 2020	One Day	Poornima College of Engineering
5	Dr. Bipin Kumar Rai	How Entrepreneurs in Emerging Markets can Master the Blockchain Technology	3rd June 2020	Four Weeks	Coursera
6	Dr. Kaushal Kishor	Global Pandemic Outbreak: Role of Technology and Automation (GPORTA)	1st-5th June 2020	Five Days	JSSATE, Noida
7	Dr. Kaushal Kishor	Python and Emerging Trends in Machine Learning	2nd-6th June 2020	Five Days	Forsk Coding School
8	Ms. Sonika Bhatnagar	Applications of Machine Learning and Deep Learning	24th-28th June 2020	Five Days	RKGIT, Ghaziabad
9	Dr. Bipin	Smart Contracts	27th June 2020	Four Weeks	Coursera

Just because something doesn't do what you planned it to do doesn't mean it's useless.

— Thomas Edison

WORKSHOPS & EXPERT TALKS



IT Department Organized a Workshop on Big Data Analytics on 6th February 2020. Total 52 students from CSE , ECE & IT attended the workshop.
The Resource person gave hands-on experience by helping the students in installing and working

CoE-Data Science, AI-ML owned by IT Department organized a workshop on "Designing facial filter using Python". Total 41 students from IT, EC and CSE attended the workshop. Mr. Harpreet Singh Sachdeva from EduGrad started the session by introducing python language. He also discussed the basics of computer vision and

Department of IT Organized a Workshop on "Introduction to DevOp". The Workshop was organized on Wednesday, 26th February 2020. Total 42 students of 3rd year IT attended the Workshop. The Resource Person gave hands-on Experience by helping the students in installing and working on Web Development Operations. For example, Docker & Kubernetes. The

On the 27th of Feb, ABESIT conducted a workshop named "Launch your careers" which was led by Ms Vineela from Linkedin.
The 2nd and 3rd year students of CS, IT, Civil, and ME branches took part in it actively. While Ms. Vineela was an excellent speaker, students also turned out to be effective listeners who were frequently asking questions and were

Alumni Meet (Reminiscence-2020)

The Department of IT Organised Alumni Meet (Reminiscence-2020). The Program started with lighting of the lamp followed by the welcome speech by presentation by **Prof. (Dr.) Bipin Rai** with few memories of the alumnus present in the hall, progress of the Institute was shared by our Honorable Director **Prof. (Dr.) M. K. Jha**. Prominent 20 alumni from different batches (2007-11 to 2015-19) graced the occasion with their presence and shared their memories of the past with the faculty and juniors. Also, they have shared their experiences in their respective job profiles and guided their juniors about the latest developments taking place in the different industries.

Students Achievements

Smart India Hackathon-2020

Shortlisted Teams for Grand Finale in the SIH-2020

S. No.	Team Name	Members Name
1	Intelleneur	Kumar Satyarth
		Sumrah Fatima
2	!ncognito	Dhishwari Singh
3	Shinobi_Coders	Gaurav Kumar
		Sparsh Srivastava
		Satyam Pal
		Juli Singh
		Sarthak Chahal
		Shreyshi Maheshwari
4	Hex Clan	Rohit Sharma
		Pranjal Sharma

Shortlisted Teams for Round-2 Evaluation in the SIH-2020

S. No.	Team Name	Members Name
1	Angry_Nerds	Deepali Rao
		Pallavi Ghosal
		Digvijay Dheer
		Sagar Singhal
		Saurabh Bhardwaj
		Kajal Gupta

Students Achievements

Internal Hackathon Conducted By ABESIT For SIH-2020

Big Congratulations to **Sumrah Fatima** (IT 2nd year) and **Satyarth** (IT 2nd Year), as their Team Intelleneur has secured Winning Position in Internal Hackathon (Software Edition) conducted by ABESIT for Smart India Hackathon

IIC–National Innovation Contest-2020

Prototype shortlisted in the contest Conducted By IIC

S. No.	Name of Team Member	Year	Title Of Idea	Theme Assigned
1	Vaibhav Kumar	2nd	Queue Management System on Airports ("Pravega Divigaman")	IOT Based Technologies (e.g. Security and Surveillance Systems etc.)
	Pranjal Sharma	2nd		
	Ritik	2nd		
	Shubham Dhawan	2nd		
	Satyam Gupta	2nd		
2	Sumrah Fatima	2nd	Setu—Its Here For your Help	Agriculture and Rural Development
	Kumar Satyarth	2nd		

Technovation Hackathon 2 at Sharda University

Big Congratulations to **Keshav Sharma** (Team Leader-IT 2nd Year) and **Sparsh Chaudhary** (IT 2nd Year), as their Team has secured 1st Runner Up in Technovation Hackathon 2 at Sharda University and won a prize money of Rs. 20000. Total 810 teams

Students Achievements

Research Papers

Research Papers 2019-2020 published in the Journal

S. No.	Name of Members	Title Of Research Paper	Published in:
1	Prof. Faraj Chishti Nimisha Pal Nandini Garg Prachi	Dual Axis Solar Tracker with Irrigation System	Nimisha Pal et al., International Journal of Research in Engineering, IT and Social Sciences, ISSN 2250-0588, Impact Factor: 6.565, Volume 10 Issue 6, June 2020, Page 11-16
2	Dr. Kaushal Kishor Divyanshu Tyagi Drishti Sharma Rishabh Singh	Real Time 'Driver Drowsiness' & Monitoring & Detec-tion Techniques	International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-8, June 2020
3	Prof. Sonika Bhatnagar Akash Garg Nakul Tyagi Manish Kumar	E Healthcare (Online Consultancy and Pharmacy) Android Application	International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) ISSN: 2278-6856, Volume 9, Issue 2, March - April 2020
4	Dr. Bipin Kumar Rai Anisha Singh Akarshita Jain	Image based Bird Species Identification	Anisha Singh et al., International Journal of Research in Engineering, IT and Social Sciences, ISSN 2250-0588, Impact Factor: 6.565, Volume 10 Issue 04, April 2020, Page 17-24
5	Nitish Kumar Mandal Suheil Khan	RFID BASED ATTENDANCE MONITORING SYSTEM	International Journal of Research and Analytical Reviews (IJRAR) E-ISSN: 2348-, P-ISSN 2349-5138, Volume 7 Issue 2, April 2020

Students Achievements

Research Papers

Research Papers 2019-2020 published in the Journal

S. No.	Name of Members	Title Of Research Paper	Published in:
6	Prajjwal Singh Priyanshi Lavania	E-Mandi	International Journal of Research and Analytical Reviews (IJRAR) E-ISSN: 2348-1269, P-ISSN: 2349-5138, Volume-7 Issue-2, April 2020
7	Prof. Shivani Sharma Prashant Tyagi Shivam Chahal Vishakha Sharma	College Information Chatbot	Prashant Tyagi et al., International Journal of Research in Engineering, IT and Social Sciences, ISSN 2250- 0588, Impact Factor: 6.565, Volume 10 Issue 04, April 2020, Page 43-47
8	Dr. Kaushal Kishor Shagun Saxena Shivam Yadav Sarvesh Yadav	Study and development of Air Monitoring and purification System	Vivechan International Journal of Research, ISSN No: 0976- 8211, Vol. 10 Issue 2, 2019
9	Prof. Rishabh Kamal Sidhant Khanna Shivam Yadav Shivam Chaudhary	Plant Disease Detection	Sidhant Khanna et al., International Journal of Research in Engineering, IT and Social Sciences, ISSN 2250- 0588, Impact Factor: 6.565, Volume 10 Issue 05, May 2020, Page 1-5
10	Prof. Sumit Kumar Sumakshi Chauhan Shreya Pathak	Two Layer Image Encryption using Symmetric Key Algorithms	International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075,Volume-9 Issue-7, May 2020

Students Achievements

Research Papers

Research Papers 2019-2020 published in the Journal

S. No.	Name of Members	Title Of Research Paper	Published in:
11	Prof. Faraj Chishti Piyush Rawal Priyansh Gupta Shubham Gaur	Comparison Website for Online Shopping	Piyush Rawal et al., International Journal of Research in Engineering, IT and Social Sciences, ISSN 2250-0588, Impact Factor: 6.565, Volume 10 Issue 05, May 2020, Page 19-21
12	Prof. Rishabh Kamal Shivam Singh Sarthak Verma Yash Kulshreshtha	Online Travel Planner using Sentiment Analysis	Shivam Singh et al., International Journal of Research in Engineering, IT and Social Sciences, ISSN 2250-0588, Impact Factor: 6.565, Volume 10 Issue 04, April 2020, Page 25-29
13	Prof Shivani Sharma Jhalak Mittal Arushi Garg	Online Chatting Application	Jhalak Mittal et al., International Journal of Research in Engineering, IT and Social Sciences, ISSN 2250-0588, Impact Factor: 6.565, Volume 10 Issue 04, April 2020, Page 10-16
14	Prof. Shivani Sharma Ankit Kumar Atras Harsh Chaudhary	An 'Iot' based Smart Helmet	Ankit Kumar Atras et al., International Journal of Research in Engineering, IT and Social Sciences, ISSN 2250- 0588, Impact Factor: 6.565, Volume 10 Issue 06, June 2020, Page 1 -7
15	Dr. Bipin Kumar Rai Ravi Verma Shiva Tiwari Janvi	Open Source Intelligence Initiating Efficient Investigation and Reliable Web Searching	Bipin Kumar Rai et. al., in Advances in Computing and Data Sciences, 4th International Conference, ICACDS 2020, Valletta, Malta,24-25 April 2020, Proceeding ISBN: 978-981-15-6633-2 Springer Nature Singapore Pte, Ltd, Communications in Computer and Information Science, CCIS 1244 (Scopus Indexed), ISSN:1865-0929

PLACEMENTS

Department Congratulate And Wish All The Success

STARS OF OUR IT DEPARTMENT!! THE ONES WHO SHONE!!

S.No.	Name of Student(s)	Company
1	Shiva Tiwari	TO THE NEW
2	Arushi Garg	Cavisson Systems
3	Janvi Jaiswal	Cavisson Systems
		INFOSYS
4	Sumakshi Chauhan	Cavisson Systems
5	Sarthak Verma	Nucleus Software
6	Shivam Yadav	Nucleus Software
7	Shailesh Singh	Nucleus Software
8	Apoorva Singh	TCS
9	Anisha Singh	Fluper
		Tech Mahindra
		HestaBit Technologies
10	Drishti Sharma	Fluper
11	Nikhil Sharma	Fluper
12	Prachi	Fluper
13	Prachi Chauhan	Fluper
		NTT Data
14	Ravi Verma	Fluper
		IT By Design
		INFOSYS
15	Rohan Rai Gupta	Fluper
16	Shagun Saxena	Fluper

PLACEMENTS

Department Congratulate And Wish All The Success

S.No.	Name of Student(s)	Company
17	Shivam Singh	Fluper
		Appinventiv
18	Shreya Pathak	Fluper
		NTT Data
19	Shubham Gaur	Fluper
		HestaBit Technologies
20	Siddharth Sharma	Fluper
		SYMB Technologies
21	Sidhant Khanna	Fluper
22	Aayushi Singh	QA InfoTech
23	Akarshita Jain	QA InfoTech
24	Ankita Saxena	NIIT Technologies
25	Nikita Kataria	NIIT Technologies
		Certybox
26	Deepak Sharma	Webkul Software
27	Divyanshu Tyagi	Quantum IT Innovation
28	Aditya Tyagi	Tech Mahindra
29	Nandini Garg	Amazon
30	Nimisha Pal	WFX
31	Sarvesh Yadav	INFOSYS
32	Harshita Mathur	Capgemini

ARTICLE

SOURCE: **http://www.bing.com/images/**

Cybersecurity And Management

By Sagar Singhal (2rd year IT)

In the world of risk management, risk is commonly defined as threat, vulnerability, consequence. The objective of risk management is to mitigate vulnerabilities to threats and the potential consequences, thereby reducing risk to an acceptable level. When applied to cybersecurity, this equation provides a great deal of insight on steps organizations can take to minimize the risk.

In this article, we'll propose a definition of cybersecurity risk as carried out by the risk formula, and best practices any organization can take to implement a cybersecurity risk management program that protects their critical data and systems.

What is cybersecurity risk? Threat x vulnerability x consequence

SOURCE: **http://www.bing.com/images/**

Threat: There are many threat actors working out there, including nation states, criminal syndicates and enterprises, hacktivists, insiders, and loner actors. These threat actors play on a variety of motivations, including financial gain, political statements, corporate or government espionage, and military advantage.

Vulnerability: Threat actors are able to launch cyber attacks through the exploitation of vulnerabilities. In cybersecurity, these vulnerabilities follow a process, procedure, or technology. For example, an employee may choose to exploit their identity with internal processes, procedures, or technology such as their knowledge let us assume Everyone in their company uses the password "98765."User names consist of an employee's first and last name. Their organization is very conscious about additional security they uses controls like multifactor authentication. This failure in both process and technology could then be exploited by said insider. And, of course, there are a large number of vulnerabilities in both hardware and software that can be exploited from the outside sources, such as unpatched software, unsecured access points, misconfigured systems, and many more.

Consequence: The consequence is the harm caused to an exploited organization by a cyberattack, they are mostly in the form of loss of sensitive data, to a disruption in a corporate network. Consequences from a cybersecurity incident not only affect the machine or data that was breached — they also affect the company's customer base, reputation, financial standing, and regulatory good-standing. These can be considered both as a direct and an indirect costs. For instance, if your company handles a great deal of sensitive information and that information is breached for malicious purposes, you may lose a great deal of customers as their data will be at risk. This is a direct consequence. But once word spreads of this violation of your customer's privacy, other potential customers may be wary and choose not to use your services. This is an indirect consequence. Both direct and indirect consequences can be very costly to an organization. They also bring a huge loss to the

ARTICLE

SOURCE: **http://www.bing.com/images/**

Cybersecurity Risk Management: 4 Things to focus on

Understanding the definition of cybersecurity risk as carried out by the risk formula is helpful, but ensuring that you can properly manage this risk is another concern.

Threat actors are increasingly rapidly and vulnerabilities are constantly emerging. Consequently, it's more a case of whether your organization is attacked or not. Given this fact, in addition to straightens security controls on your endpoints, we recommend that your cybersecurity management risk program also focuses on mitigating the potential consequences of a cyber attack.

Here are four best practices you can begin working on (or continue working on) today to develop a robust cybersecurity risk management program.

1. Involvement of the Senior Executives and Board Members

Security has become a market differentiator in recent time. Companies will win and lose contracts because of cybersecurity alone. However, it's difficult to get departmental buy-in without ensuring that the top individuals in your organization are supporting a push for reducing cyber risk. Therefore, it's mandatory that senior executives and Board members look out for the cybersecurity and risk management conversations and take care of it.

2. Identification of your material data

Material data is the data you need to care about the most. This can vary by industry or line of business to include sensitive customer, constituent, or patient information; intellectual property data; consumer data; or even the data that ensures the reliable operations of your IT systems or manufacturing

3. Limiting the number users who will be accessing the data

When individuals in your organization, or even across your partner or third-party network, are given privilege to access the information or vital data, there are several steps that should be taken to monitor and observe their behavior towards the use of that particular data. Firstly, identify the data that each employee can access. Next, determine whether it is necessary for each of those individuals to have that level of access. If access is unnecessary, put the required restrictions or say a limited access to sensitive data. lastly, it is important to closely monitor those who have access to highly sensitive data and information, including your vendors, to ensure that the information is only used for necessary purposes and not misused. Always keep in mind the Do's and don't while sharing the sensitive data with the vendors or users.

4. Looking for Tight Technology

Choosing the right cybersecurity risk management tool makes all the difference. An ideal system enables you to monitor both the performance of your own security program as well as your third parties in real time (or at least daily). With real-time monitoring, it becomes more easier to keep up with today's cyberthreats. For instance, BitSight allows you to monitor your organization's and your vendors' Security Ratings, which gives you a good signal of overall security measures. If that number changes to better or to worse you will have a good sense of whether or not your organization may have been negatively impacted by a cybersecurity attack or if your third parties are putting adequate controls in place to protect your data and improve their security.

Mitigating cyber risks

There's no doubt that cybersecurity risk management is a long and ongoing process. It is being said, that it is important not to get fatigued or think cybersecurity risk is something you can pass along to IT and forget about. Cybersecurity affects the entire organization, and in order to mitigate your cyber risk, you'll need to onboard the help of multiple departments and multiple roles. Your finance team could play just as large

SOURCE: **http://www.bing.com/images/**

ARTICLE

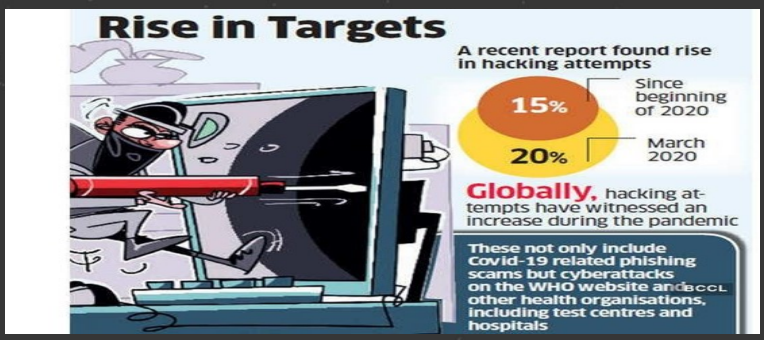
SOURCE: https://hotforsecurity.bitdefender.com/wp-content/uploads/2020/03/connection-4884862_1280-800x545.jpg

"PARADISE FOR HACKERS"

"PARADISE FOR HACKERS"

by Pranjal Sharma (2rd year IT)

Cyber attacks of all types have intensified during the Covid-19 pandemic, with hackers targeting public figures, banks, healthcare providers et al. because the rise in remote work creates new access points. An assault on the facility grid could have wide-ranging implications across sectors. While no outages have thus far been attributed to hackers, grid companies are beefing up security amid an unprecedented onslaught that, during a worst case scenario, could trigger blackouts or damage vital equipment.COVID-19, hackers are presented with opportunities on multiple fronts. They play on people's concerns about the virus by presenting phishing schemes or malware disguised in fake Centers for Disease Control and Prevention (CDC) alerts that mention the newest vaccine or treatment developments. Hackers are using the phishing attack to inject the malware into the users system. there's also pressure on healthcare companies and researchers to safeguard their vaccine and treatment data.



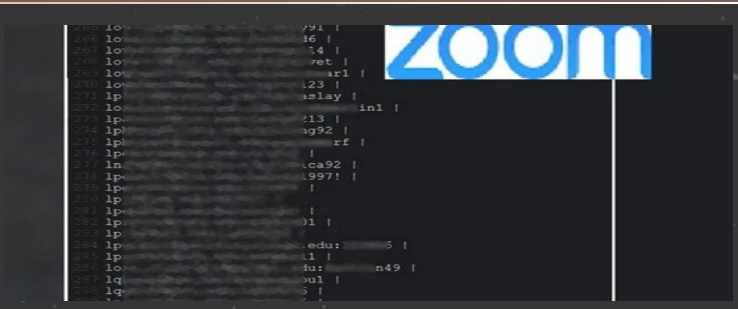
SOURCE: https://economictimes.indiatimes.com/thumb/msid-75214603,width-640,height-480,resizemode-7/1.jpg?from=mdr

Over the past few months, many workers have turned their homes into their new, remote office, including government employees, which brought host of risks through use of unsecured Wi-Fi and poor access controls. The hackers, focus and targets aimed toward the remote worker.

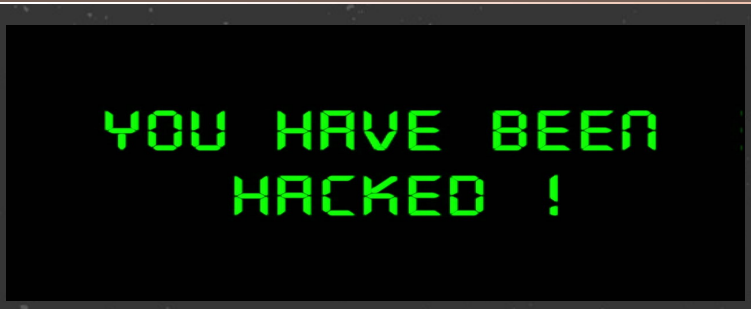
CONTACT TRACING ISSUES

Another opportunity for hacking during the pandemic comes with contact tracing. Hackers found contact tracing apps a perfect protect phishing schemes, by misrepresenting official tracing accounts via email. Legitimate apps themselves also are targets for hackers who see it as a treasure trove of knowledge with individual names and addresses also as insights

ARTICLE



SOURCE: https://i1.wp.com/fuchsiandroid.com/wp-content/uploads/2020/04/500000-Zoom-Accounts-Hacked-And-Being-Sold-On-Dark-Webs.jpeg?resize=749%2C506&ssl



SOURCE: http://i.ytimg.com/vi/0vxCFIGCqnI/maxresdefault.jpg

ZOOM

Zoom video conferencing application has seen a remarkable degree of development in the previous month or something like that. This is principally a direct result of the Covid-19 pandemic that has constrained individuals to remain inside and telecommute, leaving voice and video calls the main method of correspondence. As a result of this unexpected development, a few protection and security concerns encompassing Zoom have gone to the front. Presently, a new report guarantees that more than 500,000 Zoom accounts have been hacked and are being sold on the dull web. Zoom accounts were apparently being sold for $0.0020 (generally Rs. 0.15) per account and at times, parted with for nothing.

SOURCE: https://webdevolutions.blob.core.windows.net/blog/2020/03/Hackers-Are-Targeting-Remote-Workers-During-the-Coronavirus-Pandemic1.png

CYBER ATTACKS IN INDIA SINCE LOCKDOWN:

Digital security assaults and breaks in the country have hopped by 500% since the lockdown was first declared in March, as per security experts. Most of the assaults are beneath the radar and remember assaults for little organizations, cash lost, phishing. According to reports, in excess of 22,000 pages of plans are spilled.

New cyber security policy coming for digital India

Prime Minister Shree Narendra Modi said on 15th August that India will soon have a replacement cybersecurity policy because the country goes digital, and dependence on cyberspace increases manifold. In a short span of your time, a draft of the latest cybersecurity policy would be presented to the state. Within the coming times, we'll need to integrate everything then work within the framework of this cybersecurity. we'll formulate strategies to maneuver

TARGETING REMOTE WORKERS

The massive shift toward remote work means more networks are accessed by employees on their own devices. Companies without a remote work component were left to scramble as shutdowns started, putting in place a patchwork of security protocols that often afforded little protection. Remote workers are targeted by hackers for conducting data theft and ransomware.

BE ON THE SAFE SIDE!

On the people side, training is needed to bring at-home employees up to speed on the latest types of attacks and proper defenses that are necessary during this period of enhanced hacker activity. Education is key. They need additional information about spotting fraudulent emails, and guidance to not click on links or download attachments from unfamiliar senders. Mandates about use of VPNs to access company data and platforms. Automatic updating to remove security and patch gaps from manual updating. IT and security should work together to communicate more frequently with remote employees about the latest tech implementations, best practices, and any shift in expectations from corporate. Put in place DDoS protections which can impact the entire remote workforce which relies on accessing the company's cloud platforms. More security focused appliances are also needed in the cloud to support the infrastructure and protect against DDoS. Use multi-factor authentication (MFA) to reduce access points for hackers to intrude home-based networks. Mandate employees to stay off public Wi-Fi networks which provide easy entry points for hackers. Use monitoring tools to spot poor decisions such as clicking on suspect sites, downloading attachments from unverified senders and other detrimental choices. Use a secure search engine and communication platform.