ALU AISD SofTact

Editor-in-Chief
Dr. G. Ilankumaran
Director i/c,
AISD

Managing Editor
Dr. C. Balakrishnan
Asst.Prof., AISD

Associate Editors
Dr.B.Sugumar
Dr.P.Subhasri
Ms.K.Nithya Kalyani
Mr.C.Manikandan
Mr. S. Phabhakaran
Ms. K. Maheswari
Teaching Asst.
AISD

Technical Editors

M.Voc. Students
AJAYTHA K
PANDIYARAJA S
RAVEENA B
B.Voc. Students
ARAVINTH V
DURGA DEVI M
DHANUSH K
ESWARI S
GAYATHRI R

INSIDE THIS ISSUE:

BLUE EYES TECHNOLOGY

Imagine a world where machines can identify us, feel our presence, and interact with us the way we interact with each other. All these things will soon be a part of the world we are living in and will be achieved with the help of Blue Eyes technology. Blue eyes technology has been conducted by the research team of IBM at Almaden Research Center (ARC) in San Jose, California since 1997. It is an amalgamation of both hardware and software technologies with the help of which we can build machines having human-like sensory and perceptual abilities. In Blue eyes technology, Blue stands for Bluetooth which depicts a wireless and reliable mode of communication and helps in creating a PAN (Personal Area Network) for linking various components of the Blue Eyes devices, and Eyes that help us perceive the world and obtain interesting information. Blue eyes technology works on Artificial Intelligence. It aims to give human abilities to a computer. A research team of IBM has come up with this technology to make a computer understand and sense human feelings and behavior. The aim of the blue eyes technology is to give human power or abilities to a computer so that the machine can naturally interact with human beings.

AJAYTHA K
II- M.Voc (SD)

From the Editor-in-Chief's Desk

Editor-in-Chief
Dr. G. Ilankumaran
Director i/c,
AISD

The SofTact , annual magazine of AISD, focuses to provide insights into departmental operations and creative content from B.Voc. and M.Voc. Software Development students in order to enlighten, engage, and inspire a varied readership that includes academia, students, industry professionals, and other stakeholders. It aims in helping our students discover their latent creative abilities and to instill in them the skill of authorship. I encourage more students to take part in activities like ALUTES, which is our university's interdepartmental cultural event, and I wish the students who are keen to participate the best of luck. I encourage the students to work even harder and perform even better in the upcoming assessments in relation to their performance on the internal exam. This SofTact magazine (Volume 2) allows us to share our B.Voc. and M.Voc (Software Development) students proved their talents and it shows their strength towards their holistic learning and nurturing the development of the department.
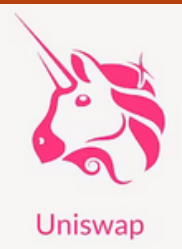
CRYPTO CURRENCY

Cryptocurrency is basically a decentralised digital and virtual currency which is not regulated, monitored or controlled by any supervising authority. The only thing that upholds our integrity is cryptography and blockchain technology. And this is exactly where crypto currency and technology comes together, through blockchain. Blockchain and cryptocurrency, being two very different technologies, are very deeply intertwined and the digital money is able to function because of blockchain. Blockchain also developed further with the popularity of crypto even though it is used in many other areas. Blockchain is a collection of blocks, i.e., digital information that is stored across various computers to form a database. When transactions through crypto take place, they are added to these blocks which later on form a chain. These chains are protected and are difficult to manipulate. Many experts claim that blockchain technology has the power to change our lives in significant and multi-dimensional ways. It has potential for much more than just crypto and it is an innovative and miraculous way of storing data. It ensures then authenticity and protection of data and one of the most impactful uses we could attain out of it is as simple as storing sensitive yet personal data. here are hardly a couple of things which attracted as much attention as the   coronavirus and Cryptocurrency

was surely one of them. With the first Cryptocurrency being introduced in 2009, the very famous Bitcoin, very few people knew or as much as cared about them. Then one day suddenly, the world was after these decentralised digital currencies and we could literally look at 800% surge in even satiric and 'joke' coins.

A person who had invested in these as a part of some truth or dare game was now a millionaire and every newspaper had the same headline. A new trend was here and it was not some dance or meme, but a Laxmi chit fund-sure shot- in a whip way of becoming rich, only difference being, this was actually legit. Does this not seem too good to be true? Why don't people buy 20$ worth of these coins, get rich and end poverty? Because these supposedly new age replacement for real, normal, everyday money were not really so. In Jan 2021, all these crypto currencies crashed leading to $134B losses. How did this happen? The distrust of governments and unstable market were the main culprits to blame. However, this opened investor's eyes and the bitter truth of investment was realised yet again, that loss and gain are the two sides of the same coin.

ARAVINTH V
II B.Voc (SD)

CRYPTO CURRENCY

Bitcoin

Uniswap

Ripple

GUESS THE RIDDLE

The Bitcoin was introduced in this world by?

Check your answer at page no.5

CYBER SECURITY AND ITS SHORTCOMINGS IN PANDEMIC

According to Forbes, 2022 will present us with a pack of diverse and terrifying cyber security challenges, everything from supply chain disruption to increased smart device risks to a continued cyber security talent drought. According to Cybercrime Magazine, cybercrime will cost the world $10.5 trillion annually by 2025. With advances in technology, cybersecurity is not an option it has become a necessity. Cyber security is a discipline that covers how to defend devices and services from electronic attacks by nefarious actors such as hackers, spammers, and cybercriminals. A strong cybersecurity strategy can provide a good security posture against malicious attacks designed to access, alter, delete, destroy or extort an organization's or user's systems and sensitive data. Cybersecurity is also instrumental in preventing attacks that aim to disable or disrupt a system's or device's operations. Maintaining cybersecurity in a constantly evolving threat landscape is a challenge for all organizations. Traditional reactive approaches, in which resources were put toward protecting systems against the biggest known threats, while lesser-known threats were undefended, are no longer a sufficient

tactic. To keep up with changing security risks, a more proactive and adaptive approach is necessary. Several key cybersecurity advisory organizations offer guidance. For example, the National Institute of Standards and Technology (NIST) recommends adopting continuous monitoring and real-time assessments as part of a risk assessment framework to defend against known and un-

known threats. Cyberthreats take many forms, some of which are: Malware is a form of malicious software

in which any file or program can be used to harm a computer user. This includes worms, viruses, Trojans, and spyware. Ransomware is another type of malware. It involves an attacker locking the victim's computer system files -- typically through encryption – and demanding a payment to decrypt and unlock them. Social engineering is an attack that relies on human interaction to trick users into breaking security procedures to gain sensitive information that is typically protected. Spear phishing is a type of phishing attack that has an intended target user, organization, or business. Insider threats are security breaches or losses caused by humans -- for example, employees, contractors, or customers. Insider threats can be malicious or negligent in nature Man-in-the-middle (MitM) attacks are eavesdropping attacks that involve an attacker intercepting and relaying messages between two parties who believe they are communicating with each other.

Healthcare organizations and banks became the major target of cyber-attacks. This is particularly problematic due to the significant functions performed by both institutions, and the amount of personal data stored in both institutions. Leakage or heft of such confidential information could end in a tragedy for the victims.

The business sector too experienced a significantly increased number of attacks with a shift to online mode. Not only that, cybercriminals have been trying to exploit people's heightened levels of reasonable concern

Gmail is an email service provided by Google. As of 2019, it had 1.5 billion active users worldwide, making it the largest email service in the world. [1] It also provides a webmail interface, accessible through a web browser, and is also accessible through the official mobile application.

Google also supports the use of third-party email clients via the POP and IMAP protocols

around COVID-19, trying to promote misinformation and scam people out of their money or personal data.
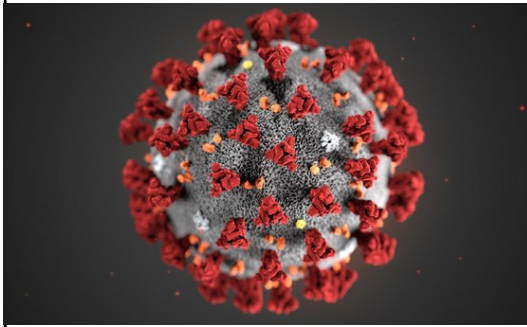
Nevertheless, cyber-attacks have been prevalent regardless of the situation in the world. Hence, cybersecurity is a must. Some steps that can be taken towards a safe cyberspace include:

♦ Installing antivirus software on all devices connected to the internet

♦ Choosing strong and different passwords for your email and social media accounts

♦ Reviewing the privacy settings of your social media accounts

♦ Not opening links and attachments in unsolicited emails and text messages

♦ Not replying to suspicious messages or calls

♦ Not sharing your bank card details or personal financial information.

CYBERBULLYING

Cyberbullying is a form of online bullying or harassment that occurs over digital devices and platforms. With the widespread use of technology and the anonymity that comes with it, cyberbullying has become more frequent and prevalent. Hidden behind their computer or mobile screens, peo-

ple don't hesitate in harassing others. This can be clearly seen in the increase in suicide cases due to online bullying. From time to time we even see celebrities facing online trolls and bullies. A recent study by CRY (Child Rights and You), a non-governmental organisation, shows that around 9.2 per cent of 630 adolescents surveyed in the Delhi-National Capital Region had experienced cyberbullying and half of them had not reported it to teachers, guardians or the social media companies concerned. Nationwide, according to research conducted by Symantec, nearly 8 out of 10 individuals are subject to the different types of cyberbullying in India. Out of these, around 63 per cent faced online abuses and insults while 59 per cent were subject to false rumors and gossip which became responsible for degrading their image. The same study ranks India as the country facing the highest cyberbullying in the Asian Pacific region. Cyberbullying can occur in several forms such as sending, posting, or sharing negative, harmful, false or mean content about someone else. It can include sharing personal or private information causing embarrassment or humiliation.

**RAVEENA B**
II M.Voc. (SD

Computer Beeps
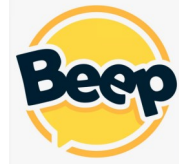
- **A very short beep** is indicative of a problem with your motherboard. It can also mean that you have a problem with your system memory (BIOS AWARD).
- **A long beep followed by three sequential short beeps** signals an issue linked to your graphics card configurations.
- **A short beep followed by three sequential long beeps** means that you have a problem with your system memory. If you are hearing **beep, pause, beep, pause, followed by two sequential beeps**, the error is linked to your CPU (central processing unit).
- **Three beeps, pause, three beeps, pause, followed by four beeps** indicates an issue with video memory.
- **One long beep and nine short beeps** means there is a problem with the ROM (BIOS AWARD).
- **Three beeps, pause, four beeps, pause, followed by a beep** signals an error with your graphics card.
- **Four beeps, pause, three beeps, pause, and then one beep** indicates a system memory problem.
- **Five short beeps** is another indication of issues with your CPU.
- **Long, constant beeps** alert system memory problems. PHOENIX BEEP CODES

PANDIYARAJA S
II M.Voc. (SD)

Windows 10's Action Center keeps everything together in a well-organized panel with notifications in the top and quick settings in the bottom.
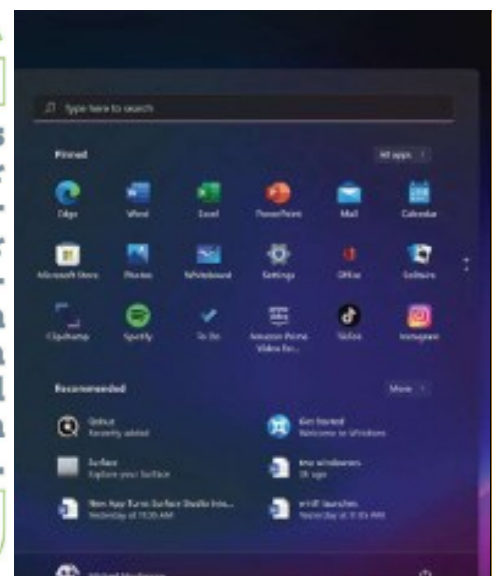
Answer for riddle asked in page no. 2

Satoshi Nakamoto

5 Ways to Wellbeing

- 5 WAYS TO WELL BEING **BE ACTIVE**
- 5 WAYS TO WELL BEING **CONNECT**
- 5 WAYS TO WELL BEING **GIVE**
- 5 WAYS TO WELL BEING **TAKE NOTICE**
- 5 WAYS TO WELL BEING **TO LEARN**

Stop Using the Same Password on Multiple Sites

The number from our recent survey of 1,041 adults age 18 or older in the US say it all. A full 70% of respondents admitted they use the same password for more than one site or service – sometimes (25%) most of the time (24%) or all the time (21%). If you don't know why that's bad, read on: When someone steals your password for just one service, they have your password for everything. Since most online accounts assign your email address as a username, it doesn't take Mr. Robot to creak that code.

Do you use the same password for more than one service or site?

Yes, I use the same password for **everything** — 21%

No — 30%

Yes, I use the same password for **most things** — 24%

Yes, I sometimes use the same password for **more than one thing** — 25%
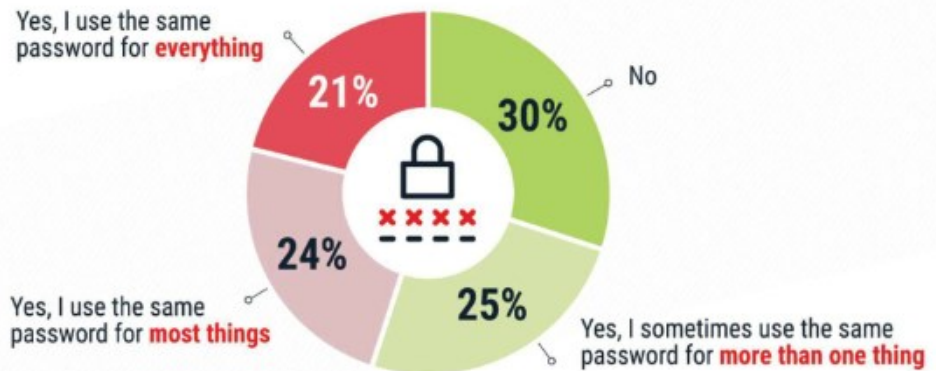
How would a cyber-crook get your passwords, you wonder? Thirty-six percent of our respondents said they physically write down passwords, and 24% keep them in notes stored electronically. Both of these methods make stealing passwords too easy—witnessed out of the corner of some criminal's eye, for the love of Snowden . Of course, you can't beat memorizing. Almost half of those surveyed said that's their preference. It's the most secure method of all, unless you're afraid of having the info tortured out of you, Bond-style. In that case, we highly recommend you use a password manager. Sadly, only one-third of respondents said they use a password manager—a software program that will store and even create strong passwords for you. But we'll continue to trumpet their use until that number goes up. Another reason to use password manager is they make it very easy to change passwords into something stronger. The major-ity of people said they change passwords every four to six months. choice. The 26% claiming they don't regularly change passwords are likely being the most honest.

> "Sadly, only one-third of respondents said they use a password manager—a software program that stores and even creates strong passwords for you."

**DURGA DEVI M
III B.Voc (SD)**

How to find the MAC address of your computer?

A MAC (Media Access Control) address is a number that identifies the network adapter(s) installed on your computer. The address is composed of up to 6 pairs of characters, separated by colons. You may need to provide your MAC address to a router in order to successfully connect to a network. To find your MAC address on any system with a network connection, use the following method on Windows Vista, 7 or 8.

Step 1:

Connect to a network. This method is only applicable if you are currently connected. Make sure to connect with the interface that you need the MAC address for (Wi-Fi if you need your wireless card's MAC address, Ethernet if you need your wired card's MAC address).
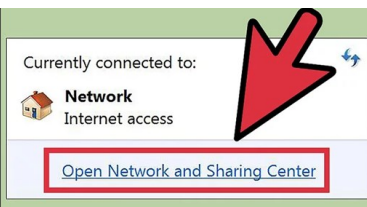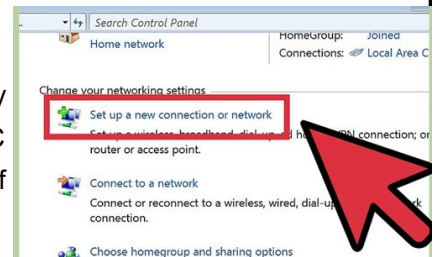
Step 2:

Click on the connection icon in the system tray. It may look like a small graphic or like a tiny computer monitor. After clicking on it, select "Open Network and Sharing Center". In Windows 8, run the Desktop application in your Start screen. Once you're in Desktop Mode, right-click on the connection icon in the system tray. Select "Network and Sharing Center".
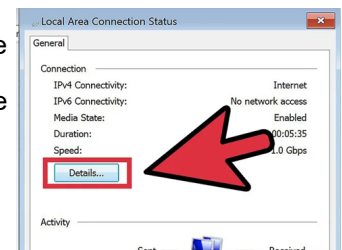
Step 3:

Find the name of your network connection and click on it. It will be located right after the word Connections. This will open a small window.
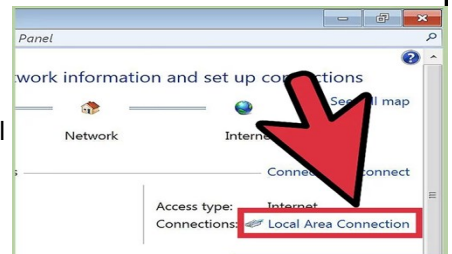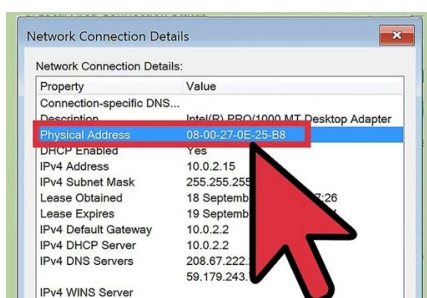
Step 4:

Click Details. This will open a list of configuration information about the connection, similar to what appears when you use the IPConfig tool in the Command Prompt.

Step 5: **Look for Physical Address.** This your MAC address.

**DHANUSH K
II B.Voc (SD)**

What you say...

WHAT INSPIRES YOU?

Bruce lee's quotes.
> --R .Viswanath
> II-B.Voc.(SD)

Speech of Sagayam IAS.
> -- S.Vigneshwaran.
> III-B.Voc.(SD)

My Father.
> --K.Sowmiya
> II B.Voc.(SD)

Motivational talk, movies, songs and my own confidence.
> -- A.Pandivel.
> III B.Voc.(SD)

Dr. APJ. Abdul Kalam.
> --Most of the students
> B.Voc. & M.Voc.(SD)

Saina Nehwal.
> -- V.Sri Surya
> I B.Voc.(SD)

My teachers are my inspiration.
> -- S.Priyanka
> I M.Voc.(SD)

Simple shortcut keys for Notepad++

Shortcut keys	Description
Ctl + N	To Create a New Document
Ctrl + Alt + S	To Open Save As . Dialog Box
Ctrl+W	To Close Current Document
Alt + F4	To Close Notepad++
F3	Find Next Searched Value
Tab	Increase Line Indent
Shift + Tab	Decrease Line Indent
Ctrl + Shift + U	To Uppercase Characters
Ctrl + U	To Lowercase Characters
Ctrl+F2	To Toggle bookmark
F2	Next Bookmark
Shift+F2	Previous Bookmark
Ctrl + Shift + Tab	To Go to Previous Document
Ctrl + Shift + Up Key	To Move Current Line Up
Ctrl + Shift + Down Key	To Move Current Line Down

ESWARI S
II B.Voc (SD)

ETHICAL HACKING

The term 'hacking' has a very negative connotation attached to it. It refers to gaining unauthorized access to data in a computer or system. It is the unlawful use of another's resources. However, hacking when done with permission is not only legal but has several advantages to organizations and companies. What kind of vulnerabilities does a hacker see? What information might be targeted by a hacker? What will the attacker do with the information and how many people notice the attempt? What can be done to fix the vulnerabilities in the system? All these questions can be answered by an ethical hacker. Ethical hacking is the act of identifying vulnerabilities in an application, system, or organization's infrastructure that can be exploited by an attacker. By lawfully hacking into networks and looking for weak places, ethical hackers (also known as the white hats) try to avoid cyberattacks and security breaches. Ethical hacking has five major phases. Reconnaissance is the preparatory phase where the hacker collects preliminary information about the target prior to the attack. Through scanning, the hacker identifies a quick way to gain access to the network by exploiting the vulnerabilities of the system. After gaining access to the network, the user privileges are escalated to control the systems connected to it. Having gained the access, the hacker tries to maintain it by securing access.

GAYATHRI R
II B.Voc. (SD)

Top 10 Online Book Reading Websites

10.24Symbols

9.Bookish

8.Wattpad

7.Scribd

6.Blurb

5.Smashwords

4.Google Books

3.Open Library

2.Internet Archive

1.Project Gutenberg

Y.Jeya Seela & R.Nandhini
III B.Voc. (SD)

TECHNOLOGY IN CINEMA

Technology and Cinema go hand in hand, as technology advances, so is the ability of filmmaking. We have advanced from Black and White to Color, from shooting on matte paintings or curtains to green screens, and the set design is setting new heights now and then. I have found myself obsessing over filmmaking or behind-the-scenes videos recently, the sheer creativity of making a movie amazes me, how every scene included has some story behind how it was shot, why those particular colors are used and how have they been achieved.

How many of you have come out of the theatre and said," the storyline was bland but the songs were amazing or the lightning or the colors", well, we all have said it, haven't we? Filmmaking is not just about the storyline but it is a collective effort of the screenplay, background score, sound quality, lighting and colors, makeup, and much more. We have found ourselves leaning toward K-dramas more and more recently, why? the reason is the same as explained above, we love the aesthetics. Why we can't stop listening to some songs even if their lyrics make no sense, the reason is their amazing sound quality. Even the academy has accolades for the best background score, best makeup, and best soundtrack, they are not just value addition but an important part of the movie itself.

Well, who doesn't like Sanjay Leela Bhansali's grand, royal, extravagant films, it will not be wrong to say that he makes all the actors look like walking portraits in his films, well some of you might think it is due to the exquisite costumes and eminent direction but you will be surprised to know that the cinematography has an upper hand here. For filming Bhansali collaborated with NY VFXWAALA, a leading Indian VFX corporation that delivered this film over eight months in terms of CGI creation and visual effects with a team of 50 to 60 artists working on it. Talking about it Prasad Sutar, Founder and Managing Director says that he and his team were involved with the film from the scripting stage. Throughout the shooting process, they would discuss and analyze whether a particular shot was possible to shoot live or with CGI or VFX, and arrangements were made accordingly. He further adds that he likes to hoot live and further adds effect to make it as realistic as possible. Talking about scenes he says," The opening war wherein the entire army was created using CGI, was shot in broad daylight and then converted into the night.

**PRISCELLIA MANCY B
II M.Voc (SD)**