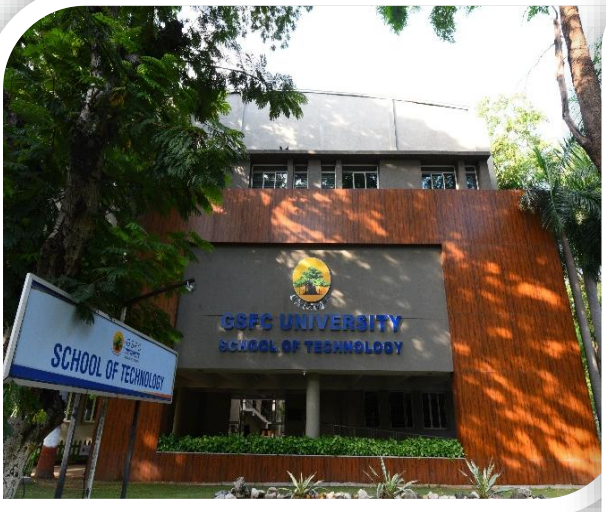
GSFC UNIVERSITY
EDUCATION RE-ENVISIONED

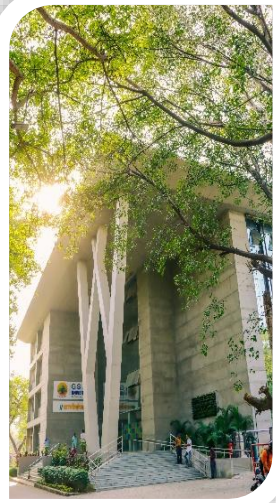
ISSUE 1 VOL. 1 JAN - FEB 2025

GYANPLEX

BIMONTHLY E-NEWSLETTER

Guarding Digital Footprint: Navigating Digital Security, Arrest and Awareness





EDUCATION RE-ENVISIONED

www.gsfcuniversity.ac.in

Follow us on:

Table of Contents

GSFC University Newsletter Editorial Board – Faculty Editors

Dr. Sneha Bajaj
Chief Editor

Mr. Bimal Bhayani
CEO,
GUIITAR

Mr. Kiran Kumar
Sr. Manager,
GUIITAR

Dr. Sanjukta Goswami
Coordinating Editor
SoT

Dr. Sindhura Gudipati
Coordinating Editor
SoS

Ms. Anshu Tiwari
Coordinating Editor
SoM&LA

Ms. Priyanka Pandya
Editor,
SoT

Dr. Jahanvi Bansal
Editor
SoM&LA

Mr. Tanmay Naik
Editor
SoM&LA

Dr. Priya Goel
Editor
SoS

Mr. Mukund Jha
Editor
Sports Cell & NCC

GSFC University Newsletter Editorial Board – Student Editors

Harsh Vaidya
Chief Editor

Adityanath R Mahto
Coordinating Editor

Akshat Pandey
Coordinating Editor

Chandraveer Solanki
Editor
GUIITAR

Harsh Shetty
Coordinating Editor

Sharline Job
Editor
SportCell

Sree Lakshmi
Editor
SOM&LA

From Editor's Desk

Dr. Sneha Bajaj
Chief Editor - 'GyanPlex'
GSFC University

Dear Readers,

As we sail through the ever-evolving digital landscape, one thing becomes increasingly clear: our online lives are as real as our offline ones. The stories we share, the connections we forge and even the risks we encounter—they all shape our digital existence. This edition of GyanPlex *is dedicated to a theme that touches each one of us: "**Guarding Digital Footprint: Navigating Digital Security, Arrests and Awareness**"*

In today's hyper-connected world, our digital footprints tell stories we often don't realize we're writing. This edition brings you thoughtful perspectives on navigating the complex landscape of online security. You'll discover why periodically disconnecting is as important as staying protected, how emerging technologies like AI are reshaping cyber-security, and practical ways to identify and avoid digital scams. Beyond just highlighting challenges, we've packed this issue with actionable advice - from simple daily habits that fortify your digital presence to compelling real-world examples that demonstrate both risks and solutions. The case studies we've included offer particularly valuable lessons from recent security incidents.

What we hope you'll take away is not anxiety, but empowerment. True digital safety isn't about technical expertise - it's about developing awareness and making conscious choices. Each small step you take creates meaningful protection.

My sincere appreciation goes to our contributors for sharing their expertise, and to you, our readers, for engaging with these crucial conversations. Together, we can build safer digital experiences.

Happy reading…..

Students' Corner: Digital Detox - Maintaining Mental Well-Being in an Over-Connected World

Mr. Harsh Vaidya
B.Tech CSE – 6th Sem
GSFC University

In today's hyper-connected world, digital devices have become an inseparable part of our daily lives. From smartphones and laptops to tablets and smartwatches, technology keeps us informed, entertained, and connected. However, the constant barrage of notifications, emails, and social media updates can take a significant toll on our mental health. The concept of a digital detox—taking a deliberate break from digital devices—has emerged as a powerful tool to restore balance, reduce stress, and improve overall well-being. This article explores the importance of digital detox, its benefits, and practical steps to incorporate it into your life.

The Need for a Digital Detox

The average person spends over 6 hours a day on digital devices, with many individuals checking their phones within minutes of waking up. This over-reliance on technology has led to several mental health challenges, including:

- Increased Stress and Anxiety: Constant notifications and the pressure to stay connected can lead to heightened stress levels.
- Reduced Focus and Productivity: Multitasking between devices and apps can fragment attention, making it difficult to concentrate on tasks.
- Sleep Disruption: Blue light emitted by screens interferes with the production of melatonin, the hormone responsible for sleep, leading to insomnia and poor sleep quality.
- Social Isolation: Ironically, excessive screen time can reduce face-to-face interactions, leading to feelings of loneliness and isolation.

A digital detox offers a way to break free from these negative effects, allowing individuals to reconnect with themselves and their surroundings.

Benefits of a Digital Detox

1. Improved Mental Health:

Stepping away from screens reduces stress, anxiety, and the constant need for validation through social media. It provides an opportunity to reflect, relax, and recharge.

2. Enhanced Focus and Productivity:

A break from digital distractions allows the brain to focus on tasks without interruptions, leading to improved efficiency and creativity.

3. Better Sleep Quality:

Reducing screen time, especially before bed, helps regulate sleep patterns and improves overall sleep quality.

4. Stronger Relationships:

A digital detox encourages meaningful face-to-face interactions, strengthening relationships with family and friends.

5. Increased Mindfulness:

Disconnecting from technology creates space for mindfulness practices like meditation, journaling, or simply being present in the moment.

Practical Steps for a Successful Digital Detox

1. Set Boundaries

Establish clear boundaries for when and where you use digital devices. For example:

- Tech-Free Zones: Designate areas in your home, such as the dining table or bedroom, as device-free zones.
- Tech-Free Times: Set specific times during the day, such as during meals or an hour before bed, to disconnect from screens.

2. Engage in Offline Activities

Rediscover the joy of offline activities that don't involve screens. Some ideas include:

- Pursue Hobbies: Engage in activities like painting, gardening, cooking, or playing a musical instrument.
- Exercise: Physical activities like yoga, jogging, or cycling not only improve physical health but also boost mental well-being.
- Spend Time with Loved Ones: Plan quality time with family and friends, free from digital distractions.

3. Practice Mindfulness

Mindfulness practices can help you stay present and reduce stress. Consider:

- Meditation: Spend a few minutes each day meditating to calm your mind and improve focus.
- Journaling: Write down your thoughts, feelings, and goals to gain clarity and perspective.
- Nature Walks: Spend time in nature to relax and reconnect with the world around you.

4. Limit Social Media Use

Social media can be a major source of stress and distraction. To reduce its impact:

- Set Time Limits: Use apps or built-in features to limit your daily social media usage.
- Unfollow Negative Influences: Curate your social media feed to include only positive and inspiring content.

- Take Breaks: Consider taking a day or weekend off from social media to reset your mindset.

5. Create a Digital Detox Plan

A structured plan can help you stay committed to your digital detox. Steps include:

- Set Goals: Define what you want to achieve, such as reducing screen time by 50% or improving sleep quality.
- Start Small: Begin with short detox periods, like an hour a day, and gradually increase the duration.
- Track Progress: Keep a journal to record your experiences and reflect on the benefits of your detox.

The Role of Organizations in Promoting Digital Detox

While individuals can take steps to reduce their screen time, organizations also have a role to play in promoting digital well-being. Employers can:

- Encourage Breaks: Promote regular breaks from screens during the workday to reduce burnout.
- Offer Wellness Programs: Provide resources like mindfulness workshops or fitness classes to support employee well-being.
- Set Boundaries: Establish policies that discourage after-hours emails and encourage work-life balance.

Conclusion

In a world where technology dominates our lives, a digital detox is not just a luxury—it's a necessity. By taking intentional breaks from screens, we can reduce stress, improve mental health, and reconnect with the world around us. Whether it's setting boundaries, engaging in offline activities, or practicing mindfulness, small changes can have a profound impact on our well-being.

Remember, a digital detox doesn't mean completely abandoning technology. Instead, it's about finding a healthy balance that allows you to enjoy the benefits of technology without letting it control your life. Start small, stay consistent, and experience the transformative power of disconnecting to reconnect.

Students' corner: Role of AI in Cybersecurity: How Artificial Intelligence is Transforming Online Safety Measures

Ms. Sharline Job
B.Tech CSE – 4th Sem
GSFC University

Introduction

Cybersecurity has become more of a requirement than a need in this present era where cyber threats are accelerating at an alarming rate. As time passes, cybercrooks have shaped their strategies such that the previously thought security mechanism cannot be applicable in the traditional way. However, artificial intelligence is transforming this by providing cyber threats with intelligent detection, prevention, and timely response. It discusses the increasing threats of cybercrime, which portrays the role of AI in securing personal digital footprints and the legal and ethical aspects of digital arrests.

Rising Threats of Cybercrime and Digital Arrests

Cybercrime does not appear only in phishing scams and malware attacks. Today, a cybercrime involves advanced techniques like deepfake technology, ransomware, and identity theft. "Digital arrests" is one of the most alarming trends as law enforcement implements digital proof to track and prosecute cyber offenders. This helps curb cybercrime but raises concerns about privacy, misuse of data, and wrongful accusations.
AI-Powered Cybersecurity: Strengthening Digital Defenses

AI has changed the game in cyber threat defense. Here's how AI is the game changer.

1. Threat Detection and Prevention

- AI-based systems track huge amounts of data; they are able to identify suspicious activities. Machine learning algorithms help identify a pattern related to malware, phishing and insider threats, therefore preventing breaches before the breach occurs.

2. Automated Incident Response

- Artificial intelligence-based security systems respond to threats in real time which allows them to minimize the damage. Automated security protocols help organizations neutralize cyber threats without human intervention without making any delay.

3. Behavioral Analysis

- For example, AI may track the user's behavior to detect anomalies in the access. If an employee suddenly accesses the restricted data at an unusual time, the AI system flags it as a probable security breach

4. Improving Password Security and Authentication

- Traditional passwords are susceptible to brute-force attacks. AI-based authentication provides improved security through reduced use of easily compromised passwords, including the use of biometric verification and behavioral biometrics.

5. Protecting Personal Digital Life

While AI keeps playing a crucial role in security, individuals must also practice the best policies on how to maintain personal digital footprints as well. Some of them are the following:

- Implement Multi-Factor Authentication for all applications and accounts
- Keep software and their security patches updated to avoid vulnerabilities.
- Be cautious of phishing emails and links from unknown sources.
- Regularly monitor online accounts for unauthorized activities.
- Personal information should be limited on the social media platforms.
- Legal and Ethical Dimensions of Digital Arrests

Though AI-powered cybersecurity enhances digital security, it has also thrown shadows on ethical and legal matters. Digital arrests through AI-powered surveillance and data tracking raise pertinent questions about privacy rights:

Ethics: The implementation of AI systems might raise incorrect accusations against people who are not culprits.

Legal Issues: Digital arrest is country-specific, and thus, it is tough to ensure justice is served, as it differs in all the countries.

Surveillance and Privacy: Governments and businesses that use AI for surveillance should be transparent, so there is no perversion of such development.

Conclusion

AI is very crucial in cybersecurity because it keeps on evolving with new emerging threats. Although AI boosts digital security and minimizes cyber risks, there is an urgent need to address ethical concerns and ensure the privacy of individuals. The online world can be explored safely with AI-driven security measures and knowledge of digital threats, which also help individuals and organizations maintain their digital integrity.

Students' corner: The Rise of Digital Scams: Recognizing and Preventing Common Online Frauds

Ms. Vedika Joshii
BBA – 4th Sem
GSFC University

As digital transactions and online interactions become more prevalent, cybercriminals are developing increasingly sophisticated methods to exploit unsuspecting individuals. The rapid expansion of digital platforms has revolutionized how people communicate, shop and manage finances, but it has also created new opportunities for fraud. This paper examines the growing threat of online scams, highlights common fraudulent tactics, and provides strategies to help individuals and organizations protect themselves. Strengthening awareness and implementing proactive security measures are the key to reducing the risks posed by digital fraud.

The surge in cybercrimes has made it essential to recognize the deceptive techniques used by fraudsters. Whether through phishing attacks, fake online stores, fraudulent investments, or identity theft, scammers manipulate users into providing sensitive information. To counteract these threats, adopting cyber-security best practices—such as multi-factor authentication, secure browsing habits, and software updates—can significantly enhance digital safety. By fostering a culture of vigilance and cyber-security awareness, individuals and organizations can work together to mitigate the risks associated with digital fraud.

Common Types of Digital Scams

1. **Phishing Attacks**
   These scams involve deceptive emails, messages, or websites designed to trick users into disclosing personal information, such as login credentials or banking details. Fraudsters often impersonate trusted entities like banks or service providers to gain access to sensitive data.
2. **Online Shopping Scams**
   Fake e-commerce websites attract buyers with seemingly great deals but fail to deliver products. In some cases, these fraudulent platforms steal financial details during transactions.
3. **Investment and Cryptocurrency Fraud**
   Scammers entice victims with fraudulent investment opportunities, often promising high returns with minimal risk. Many fall prey to fake cryptocurrency platforms that vanish after collecting funds.
4. **Tech Support Fraud**
   Posing as representatives of well-known tech companies, scammers convince users that their devices are infected and persuade them to grant remote access or pay for unnecessary services.
5. **Identity Theft and Social Media Scams**
   Cybercriminals exploit personal data obtained from compromised accounts to impersonate individuals, gain access to financial resources, or engage in fraudulent activities.

Preventive Measures

1. **Raising Awareness and Educating Users**
   Understanding common online scams and learning to recognize suspicious messages, websites, and emails is crucial for prevention.
2. **Using Multi-Factor Authentication (MFA)**
   Adding an extra layer of security, such as authentication codes, reduces the risk of unauthorized access to accounts.
3. **Practicing Safe Browsing**
   Avoiding unverified links, refraining from downloading suspicious attachments, and steering clear of unsecured public Wi-Fi networks can minimize risks.
4. **Updating Software Regularly**
   Keeping operating systems, browsers, and security programs up to date helps protect devices from vulnerabilities that cybercriminals exploit.
5. **Verifying Websites and Transactions**
   Before sharing financial details or making payments, users should confirm the legitimacy of websites, emails, and businesses.

Conclusion

With the constant evolution of digital scams, it is essential for individuals and businesses to remain vigilant and adopt strong security measures. Recognizing fraudulent patterns, educating users, and implementing advanced cyber-security strategies can significantly reduce exposure to online fraud. Promoting cyber-security awareness and responsible online behavior will contribute to a safer digital environment for everyone.

Students' Corner: Cognitive overload in the Age of Constant Connectivity

Ms. Netra Gajjar
B.Tech CSE – 6th Sem
GSFC University

Abstract

In our hyperconnected world we find ourselves swimming in a sea of information. This overwhelming influx leads to what we call cognitive overload, where our mental capacity feels stretched to its limits. In this rapid pace of connectivity, its no wonder we feel like we are running on empty by the end of the day. Finding a way to navigate this information overload has become essential for maintaining our natural creativity and reclaiming our ability to think deeply and creatively.

Introduction

Like everything has its limits, our human brain also has limits where it can stretch itself. We try to balance and jiggle too many tasks at once- such as reading emails, scrolling through media, texting and what not! We push our cognitive abilities to its breaking point. This frantic multitasking can lead to challenges such as---

- unstable focus,
- decline in ability of concentration,
- sense of mental exhaustion,
- Forgetfulness

In the world which demands our attention from every angle, its crucial to recognize the toll it takes our minds to take back our focus and creativity.

The Impact of Constant Connectivity

The time when you were settled to do a task only to be distracted by a notification and entering a wormhole of social media, checking messages, distracted by Instagram reels completely interfered by the sight of what you

intended to do. This is a perfect example of the effect of so much cognitive overload. The constant multitasking doesn't scale our productivity but it just declines our performance.

Strategies to Mitigate Cognitive Overload

Consider adopting the following strategies to overcome the problem of constant connectivity:

- Prioritize Your Tasks: Concentrate on completing one task at a time. Techniques like the Pomodoro Technique, mind mapping, or the Feynman Technique can enhance your study sessions and boost productivity.
- Schedule Regular Digital Detoxes: Carve out an hour each day to catch up on social media and dedicate the rest of your time to work, personal growth, and nurturing relationships.
- Incorporate Mindfulness and Meditation: Practicing meditation can significantly improve your attention span, reduce stress, and enhance your ability to concentrate.
- Establish Device Boundaries: Designate specific times for checking emails and social media. Silence non-essential notifications to minimize distractions and create a more focused environment.
- Create an Optimized Environment: Minimize distractions by silencing unnecessary notifications and keeping your workspace tidy and organized. A clutter-free environment can lead to clearer thinking and greater productivity.

Conclusion

In this world of digital haze, always multitasking can toll on our well-being. However, by setting boundries and being mindful of how we use technology, we can ease our minds by removing unnecessary mental strain and help ourselves being better at focusing, productivity and clarity. Your mind would be thankful for the break!

Cyber Hygiene Practices: Tips to Protect Your Data Online

Ms. Kalyani Joshi
Senior Academic Associate - Mathematics
GSFC University

In today's digital-first world, where technology permeates every aspect of our lives, practicing good cyber hygiene has become as essential as maintaining personal hygiene. Cyber hygiene refers to the proactive steps individuals and organizations take to maintain the health and security of their digital systems and data. With cyber threats becoming increasingly sophisticated, adopting robust cyber hygiene practices is no longer optional—it's a necessity. This article delves into actionable tips to help you safeguard your personal and professional data online, ensuring a secure digital footprint.

The Importance of Cyber Hygiene

Cyber hygiene is the foundation of digital security. Just as neglecting personal hygiene can lead to health issues, poor cyber hygiene can result in data breaches, identity theft, financial losses, and reputational damage. The rise in remote work, online transactions, and digital communication has made individuals and organizations more vulnerable to cyberattacks. According to a report by Cybersecurity Ventures, cybercrime is expected to cost the world $10.5 trillion annually by 2025. This staggering figure underscores the urgent need for individuals and businesses to prioritize cyber hygiene.

Actionable Tips for Effective Cyber Hygiene

1. Use Strong Passwords

Passwords are the first line of defense against unauthorized access to your accounts. However, many people still use weak or easily guessable passwords, such as "123456" or "password." To enhance your security:

- Create Complex Passwords: Use a combination of uppercase and lowercase letters, numbers, and special characters.
- Avoid Common Words: Refrain from using easily guessable words like your name, birthdate, or "admin."
- Use a Password Manager: Password managers generate and store strong, unique passwords for each of your accounts, eliminating the need to remember them all.

2. Enable Two-Factor Authentication (2FA)

Two-factor authentication adds an extra layer of security by requiring a second form of verification in addition to your password. This could be a one-time code sent to your phone or a biometric scan like

a fingerprint. Even if a hacker obtains your password, they won't be able to access your account without the second factor.

3. Update Software Regularly

Software updates often include patches for security vulnerabilities that hackers can exploit. To stay protected:

- Enable Automatic Updates: Ensure your operating system, apps, and antivirus software are set to update automatically.
- Don't Ignore Notifications: Promptly install updates when prompted, even if they seem inconvenient.

4. Avoid Public Wi-Fi

Public Wi-Fi networks are often unsecured, making them a prime target for cybercriminals. If you must use public Wi-Fi:

- Use a VPN: A Virtual Private Network (VPN) encrypts your internet connection, making it difficult for hackers to intercept your data.
- Avoid Sensitive Transactions: Refrain from accessing bank accounts or entering passwords on public networks.

5. Be Cautious with Emails

Phishing emails are a common tactic used by cybercriminals to steal sensitive information. To avoid falling victim:

- Verify the Sender: Check the email address for authenticity, especially if the message requests personal information.
- Avoid Clicking Links: Hover over links to see their destination before clicking.
- Don't Download Attachments: Be wary of unexpected attachments, even from known contacts.

Additional Cyber Hygiene Practices

6. Regularly Back Up Your Data

Data loss can occur due to cyberattacks, hardware failures, or accidental deletion. Regularly backing up your data ensures you can recover it in case of an incident. Use both cloud-based and physical backups for added security.

7. Educate Yourself and Others

Cyber threats are constantly evolving, making it essential to stay informed about the latest risks and best practices. Share this knowledge with family, friends, and colleagues to create a culture of cybersecurity awareness.

8. Monitor Your Accounts

Regularly review your bank statements, credit reports, and online accounts for any suspicious activity. Early detection of unauthorized access can prevent further damage.

9. Secure Your Devices

Ensure all your devices, including smartphones, tablets, and laptops, are protected with strong passwords, encryption, and antivirus software. Enable remote wipe features in case your device is lost or stolen.

10. Limit Data Sharing

Be mindful of the information you share online, especially on social media. Cybercriminals can use seemingly harmless details like your pet's name or hometown to guess passwords or answer security questions.

The Role of Organizations in Promoting Cyber Hygiene

While individuals must take responsibility for their digital security, organizations also play a critical role in promoting cyber hygiene. Businesses should:

- Conduct Regular Training: Educate employees about cybersecurity best practices and the latest threats.
- Implement Strong Policies: Enforce password policies, data encryption, and access controls.
- Invest in Security Tools: Use firewalls, intrusion detection systems, and endpoint protection to safeguard networks and devices.

Conclusion

In an era where cyber threats are omnipresent, practicing good cyber hygiene is not just a recommendation—it's a responsibility. By adopting the tips outlined in this article, you can significantly reduce the risk of cyberattacks and protect your personal and professional data. Remember, cybersecurity is a continuous process, not a one-time effort. Stay vigilant, stay informed, and make cyber hygiene an integral part of your digital life.

By taking these steps, you not only safeguard your own digital footprint but also contribute to a safer and more secure online environment for everyone.

Guarding Digital Footprint: Navigating Digital Security, Arrests and Awareness

Mr. G R Purohit
Visiting Faculty - Fire & EHS
GSFC University

Introduction

In today's digital world, online activities have become an integral part of our lives, making digital security a crucial concern. From social media interactions to financial transactions, every action leaves behind a digital footprint. While technology offers convenience, it also exposes users to cyber threats, identity theft, and privacy risks. Understanding digital footprints, their impact, and ways to safeguard personal data is essential in ensuring online safety.

Understanding Digital Footprint

A digital footprint refers to the trail of data left by individuals through online activities, including:

- **Active footprint:** Data intentionally shared, such as social media posts, online purchases, and subscriptions.
- **Passive footprint:** Data collected without the user's knowledge, such as website tracking through cookies and location tracking.

Employers and universities often review digital footprints before making hiring or admission decisions. Additionally, cybercriminals can exploit digital footprints for identity theft, phishing, and fraud.

Cyber Threats and Digital Crimes

The growing reliance on digital platforms has led to an increase in cybercrimes. Common threats include:

- **Phishing attacks:** Fraudulent emails or messages tricking users into revealing personal information.
- **Ransomware:** Malicious software encrypting user data, demanding payment for decryption.
- **Identity theft:** Unauthorized use of personal information for financial fraud.
- **DDoS attacks:** Overloading servers to disrupt services.
- **Cryptojacking:** Unauthorized use of a device for cryptocurrency mining.

Law enforcement agencies are employing digital arrest techniques to track and apprehend cybercriminals through IP tracing, online surveillance, and data analysis.

Safeguarding Your Digital Footprint

Protecting personal data requires proactive measures. Key strategies include:

- **Use strong passwords**: Create unique, complex passwords for different accounts and enable two-factor authentication (2FA).
- **Adjust privacy settings**: Restrict access to personal information on social media.
- **Avoid public Wi-Fi**: Use Virtual Private Networks (VPNs) for secure browsing.
- **Think before posting**: Be mindful of sharing sensitive information online.
- **Regularly update software**: Ensure devices and applications are equipped with the latest security updates.
- **Monitor online presence**: Regularly search your name and review online accounts for potential data leaks.

Ethical Hacking and AI in Cybersecurity

Ethical hacking plays a crucial role in identifying vulnerabilities and strengthening cybersecurity defenses. Additionally, artificial intelligence (AI) enhances online safety by detecting cyber threats, analyzing behavioral patterns, and improving security measures.

Legal Framework and Future Trends

Governments worldwide are implementing cybersecurity laws to address digital threats. Key regulations include:

- **General Data Protection Regulation (GDPR)** (EU) – Protects user privacy.
- **Digital Personal Data Protection Act (India)** – Aims to safeguard personal data.
- **Cybercrime Prevention Act (Philippines)** – Focuses on combating online crimes.

The future of cybersecurity is shaped by advancements in AI, quantum computing, and global regulatory measures to strengthen digital security.

Conclusion

Managing digital footprints is vital for personal security and protecting sensitive information. While technology continues to evolve, individuals must stay informed and adopt responsible online habits. By implementing cybersecurity best practices, users can safeguard their data and contribute to a safer digital environment.

The Premature Development of AI and Under Developed Cyber Security Frameworks a Challenge for India's Digital Infrastructure

Mr. Vishal Harith
Assistant Professor - CSE
GSFC University

In the era post Covid-19 pandemic, the world has seen a surge in the internet users and the technological disruptions caused by the evolution of Generative Pre-trained Transformer otherwise known as GPT has put the world in a different pedestal.

Talking about India and its cyber space, the expect growth of Internet users by 2025 is to touch 900 million with India being the 2nd largest online market behind China. India is faced by sophisticated and persistent cyber threats from state-sponsored and non-state actors, who target India's economic and strategic interests.

Most equipment, hardware and software technology for setting up digital infrastructure in India are currently procured from global sources. These systems are vulnerable to cyber threats just like any other connected system.

India has a "pro-innovation" stance to AI regulation. It is striving to unlock the full potential of AI while taking into account the anticipated risks. This was reflected in the G20 Ministerial Declaration made during India's presidency, as well as a statement in Parliament in April 2023. This has opened the flood gates to unlocking the raw power of advanced deep learning algorithms that although has positive aspects in Research & Development yet the same can be used for Advanced Persistent Threats (APTs)which are prolonged and complex cyber-attacks, usually carried out by skilled groups who are well-resourced with the power of AI. These attacks are designed to infiltrate and remain hidden in the target's network for a long time, allowing them to steal, manipulate data, or cause damage.

In India, post pandemic era there has been many prominent cyber-attacks on our digital public infrastructure some of the prominent ones are National Disaster Management Authority (NDMA)faced a data breach that compromised the personal data of 93,000 volunteers, the hacker group Transparent Tribe targeted critical sectors within India's government and defence industries, using phishing emails to gain access to sensitive systems, Tamil Nadu's police Facial Recognition Software portal was breached using compromised credentials, exposing data of over 6 million records, the Telangana police's Hawk Eye app experienced a data breach, exposing sensitive information of approximately 200,000 citizens, Sun Pharmaceutical Industries, a major player in the Indian pharmaceutical sector, faced a cyberattack that marked the third significant attack on an Indian drugmaker, raising concerns about the security of critical healthcare infrastructure and the potential impact on patient safety and data integrity, RailYatri, e-booking service for Indian Railways, faced a data breach in December 2022 that resulted in over 30 million user records being compromised, Motilal Oswal Financial Services experienced a cyber incident linked to the LockBit group, known for extortion tactics, In December 2022, the All India Institute of Medical Sciences (AIIMS) suffered a significant cyberattack, leading to the encryption of about 1.3 terabytes of data across five servers, in

September 2022, the Swachh City platform, associated with the Swachh Bharat Mission, was hacked, compromising the data of approximately 16 million users, in August 2022, BharatPay, a digital financial services provider, experienced a serious data breach exposing the personal data of around 37,000 users.

As the famous words of Hayreddin Barbarossa, admiral of the Ottoman Navy was quoted telling emperor Suleiman "He who rules on the sea will shortly rule on the land also", this led to explorers and navigators to find a new sea route to India. Present day the quote fits the "cyber explorers" and "cyber navigators" who are constantly "discovering" the cyber infrastructure vulnerabilities in the Indian cyber space.

Now in this Information Age, the sophisticated cyber criminals aspire to harness the potential of Artificial Intelligence (AI) to automate and enhance their attacks. In order to make it a real threat they need two ingredients, a huge chunk of digitally vulnerable assets and the access to the unbridled power of AI. Presently India is serving both these, for the modern day "cyber explorers" to get "deeper learning" into the vulnerability of the digital systems.

The dire need of the hour for India is for researchers in cyber security and AI, policy makers, technocrats to come to a single forum and chart out an effective action plan to have a balanced view of AI and strengthen India's cyber space.

A Flight, a Dream and a Digital Trap

Dr. Jahanvi Bansal
Associate Dean-R&D Cell
GSFC University

It was a crisp December evening as I sat near Gate 6 at Vadodara airport, waiting for the boarding announcement for my flight, 6E5164, to New Delhi. Excitement brewed within me as I anticipated reuniting with my family after six long months. As someone who likes to arrive at least 1.5 hours early for flights, I had secured a comfortable spot near the gate, my mind already wandering to the warmth of home and the festivities awaiting the New Year.

Just then, my phone buzzed with a call from an unknown number, starting with +97-17556. Ordinarily, I would have ignored such calls, but an inexplicable instinct urged me to pick up.

"Hello," a calm, composed female voice said, "I'm calling from FedEx. We have received a suspicious parcel in your name containing drugs and arms." My heart skipped a beat as she continued, "You are under digital arrest. A car is waiting outside to take you home. From this moment, you will be under virtual surveillance through a video call."

Shock rendered me mute. The noise of the bustling airport seemed to grow louder as the weight of her words sank in. I noticed people around me forming a crowd, their presence closing in as though to usher me out of the terminal. My legs moved involuntarily as I followed the stream of people toward the exit.

The car awaited, just as she had said. I stepped in, my mind a whirlwind of confusion and fear. Suddenly, the sound of banging filled the air. I turned sharply, expecting an officer or a dramatic revelation, but instead, I woke up.

It had been a dream. My window, left ajar, was swinging against the wind, producing the banging noise that had jolted me awake. My heart raced as I pieced together the surreal fragments of my nightmare. Yet, as relief washed over me, a thought struck hard: what if this dream wasn't entirely a figment of my imagination?

In recent months, I had read about cases eerily similar to what I had just experienced in my dream. Victims falling prey to scams under the guise of "digital arrest" orchestrated by cyber predators. A Bengaluru woman reportedly paid ₹1.2 crores to scammers, believing their meticulously crafted deception. These scams felt laughable when viewed from a distance, but my dream had given me a terrifying glimpse into how real they could feel when experienced firsthand.

Such scammers leave no detail unchecked. Their phishing emails and cloned websites are as polished as a Sanjay Leela Bhansali movie set. They use uniformed backdrops, authentic-sounding jargon, and precise personal details to ensnare victims. Their legitimacy is so convincing that panic becomes inevitable. Victims are coerced into transferring money, fearing the consequences of "going legal."

Even Prime Minister Narendra Modi, in his October *Mann Ki Baat* series, warned citizens against these cyber threats. As of now, over 92,323 cases of digital arrest scams have been reported in India, with more than ₹20,000 crores lost to these predators.

My dream, though fictional, felt like a cautionary tale. It reminded me of the importance of cybersecurity: using trusted Wi-Fi networks, creating strong passwords, enabling two-factor authentication, and being vigilant about phishing attempts.

As I reflected on this surreal experience, I decided to do my part. I urge you, the reader, to spread awareness about such scams. Share this message with ten people—not for luck, but to save someone else from falling into the trap. Awareness and caution are our strongest weapons against these digital predators.

While my New Year's journey may have been uneventful in reality, my dream reminded me of the vulnerability that lurks in the digital age. Let's stay informed and vigilant. After all, someone's nightmare could very well be someone else's reality.

The Psychology of Digital Overload: Why We Need a Break?: Digital Detox

Dr. Archana Magare
Assistant Professor - CSE
GSFC University

Digital overload is a condition that indicates excessive use of digital devices particularly smart phones, laptops, computers and social media platforms which causes severe psychological implications. It results in mental fatigue and reduced cognitive functions [1]. Digital overload impacts on mind, body and mood.

Understanding Digital Overload:

Digital overload refers to the constant bombardment of digital stimuli, including notifications, emails, social media updates, and multimedia content, leading to mental exhaustion. A study showed that individuals who spend more than four hours daily on digital devices report significantly higher stress levels and symptoms of anxiety and depression compared to those with moderate usage [2][3].

Doomscrolling, a phenomenon that emerged during the COVID pandemic across all age groups has resulted in various mental health issues, such as anxiety and depression. A Harvard Health Publishing article highlights the effect of doomscrolling on mental health that further results in physical consequences [4]. Doomscrolling stems from the amygdala-driven fight-or-flight response. In this, the brain is wired to scan for threats, reinforcing compulsive news consumption.

Psychological Impacts

Constant influx of notification leads to anxiety, depression, and sleep disruption.

Neuroscientific studies indicate that overdependence on digital devices can lead to cognitive atrophy, diminishing critical thinking and problem-solving abilities.

A brain rot is the reduced cognitive ability due to too much doomscrolling on social media.

Digital Detox:

Various studies in recent years focused on analysing ways to handle the digital overload. It aims to mitigate the effects of digital overload by reducing screen time, which can improve overall well-being and social relationships. The solution to handle digital overload is digital detox. The need for digital detox arises from the concerns about the detrimental effects of prolonged digital engagement on mental and physical health. Digital detox is the practice of taking breaks from digital technology, especially smartphones and social media, to enhance well-being and minimize adverse effects related to overuse.

Benefits of Digital Detox

Digital detox activities involve refraining from using various digital devices and platforms for a certain amount of time. This results into several mental health benefits:

- ✓ Reduction in Anxiety and Depression

- ✓ Improved Sleep Quality
- ✓ Enhanced Productivity and focus

Ways to Implement a Digital Detox

- ✓ Partial Reduction Over Total Abstinence: Reducing screen time on social media, rather than complete abstinence, results in a stronger positive impact on well-being. This approach allows individuals to maintain necessary digital interactions while minimizing negative impacts [5][6].
- ✓ Creating Tech-free Zones and Times: Creating designated digital-free zones and time slots empowers individuals to reclaim their focus and prioritize well-being [7].
- ✓ Mindfulness and Offline Activities: Replace screen time with activities such as reading, exercising, meditating, or socializing [7].
- ✓ Digital Literacy and Self-Regulation: Teaching digital literacy and self-regulation techniques provide individuals with the tools to navigate the digital world responsibly and reduce excessive device usage [7]

Lesson to Learn: Case Study - The MOVEit Data Breach of 2023

Dr. Sneha Bajaj
Chief Editor – GyanPlex,
GSFC University

Case Summary:

The MOVEit data breach of 2023, which continued to have significant repercussions into 2024, is one of the most impactful cybersecurity incidents in recent years. This case study examines the causes, consequences, and lessons learned from the breach, emphasizing the importance of robust cybersecurity practices, timely vulnerability management, and proactive risk mitigation in an increasingly digital world.

Background

MOVEit, a widely used file transfer software developed by Progress Software, is utilized by organizations globally to securely share sensitive data. In May 2023, a critical vulnerability in MOVEit was exploited by the Clop ransomware group, leading to a massive data breach that affected hundreds of organizations, including government agencies, financial institutions, and healthcare providers. The breach exposed sensitive data such as Social Security numbers, financial records, and medical information, impacting millions of individuals worldwide.

The Breach: What Happened?

The breach stemmed from a zero-day vulnerability in MOVEit's file transfer protocol, which allowed attackers to gain unauthorized access to sensitive data stored on the platform. Despite Progress Software releasing a patch shortly after the vulnerability was discovered, many organizations failed to apply the update promptly, leaving their systems exposed.

Key factors contributing to the breach included:

1. **Zero-Day Exploit:** The attackers exploited a previously unknown vulnerability, highlighting the challenges of defending against advanced threats.

2. **Delayed Patching:** Many organizations using MOVEit were slow to apply the security patch, leaving their systems vulnerable for weeks.

3. **Lack of Encryption:** In some cases, sensitive data stored on MOVEit was not encrypted, making it easier for attackers to access and exfiltrate information.

4. **Third-Party Risks:** The breach affected not only direct users of MOVEit but also their clients and partners, underscoring the risks of third-party dependencies.

Consequences of the Breach

The MOVEit breach had far-reaching consequences that continued to unfold into 2024:

1. Massive Data Exposure: The breach exposed sensitive data of millions of individuals, including employees, customers, and patients.

2. Financial Losses: Affected organizations faced significant costs, including legal settlements, regulatory fines, and remediation efforts. For example, the breach cost some companies tens of millions of dollars in damages.

3. Reputational Damage: Organizations impacted by the breach suffered reputational harm, eroding customer trust and confidence.

4. Regulatory Scrutiny: The incident prompted investigations by regulatory bodies, including the U.S. Securities and Exchange Commission (SEC) and the European Data Protection Board (EDPB), leading to calls for stricter data protection regulations.

5. Operational Disruptions: Many organizations had to temporarily halt their file transfer operations, disrupting business processes and causing delays.

Lessons Learned

The MOVEit breach serves as a critical reminder of the importance of cybersecurity in an era of increasing digital threats. Key lessons include:

1. Timely Vulnerability Management: Organizations must prioritize the timely identification and patching of vulnerabilities to reduce the risk of exploitation.

2. Proactive Threat Monitoring: Implementing advanced threat detection and monitoring systems can help identify and mitigate attacks before they cause significant damage.

3. Data Encryption: Encrypting sensitive data, both in transit and at rest, can minimize the impact of a breach by making it harder for attackers to access usable information.

4. Third-Party Risk Management: Organizations must assess and manage the cybersecurity risks posed by third-party vendors and partners.

5. Incident Response Planning: A well-defined and tested incident response plan is essential for minimizing damage and restoring operations quickly.

Conclusion

The MOVEit data breach of 2023, with its lingering effects into 2024, highlights the evolving nature of cybersecurity threats and the need for organizations to remain vigilant. By learning from this incident, businesses can take proactive steps to strengthen their cybersecurity posture, protect sensitive data, and build resilience against future attacks.

In an increasingly interconnected world, the MOVEit breach serves as a stark reminder that cybersecurity is not just a technical issue but a critical business imperative. Organizations must prioritize cybersecurity at all levels, from leadership to operations, to safeguard their assets, reputation, and customer trust.

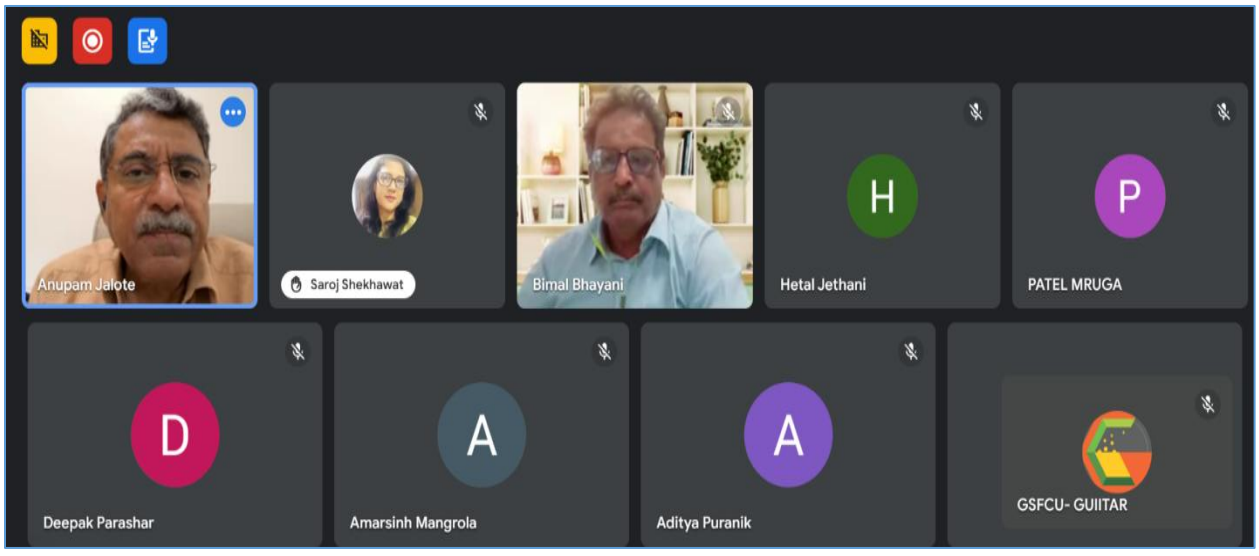
GUIITAR Council: Report 1

Mr. Kirankumar Parmar
Sr. Manager - GUIITAR
GSFC University

One Faculty One Innovation -2

The One Faculty One Innovation 2.0 event was organized to catalyze the innovation ecosystem at GSFC University by leveraging interdisciplinary faculty expertise and industry insights. The session conducted by esteemed speaker Shri Anupam Jalote, CEO, iCEM, Ahmedabad with active participation from faculty members across engineering, science, and management departments. Key learning Points:

- **Formation of Domain-Specific Teams:** Four clusters—CSE, Biotechnology, Chemical Engineering, and Fire & Safety—were proposed with interdisciplinary faculty and management representation for holistic mentorship.
- **Ideation and Idea Selection:** Each team will generate 10 startup ideas, to be shortlisted using an evaluation matrix based on feasibility, relevance, and market potential.
- **Outreach and Mentorship:** Emphasis was placed on leveraging social media, student groups, and faculty industry networks for idea validation and mentorship.
- **Funding and Support:** Participants were briefed on SSIP funding up to Rs. 2.5 lakhs for student-led projects, focusing on technical and market viability.
- **Industry Engagement:** Early collaboration with industry and studying global trends was encouraged to align projects with real-world needs.



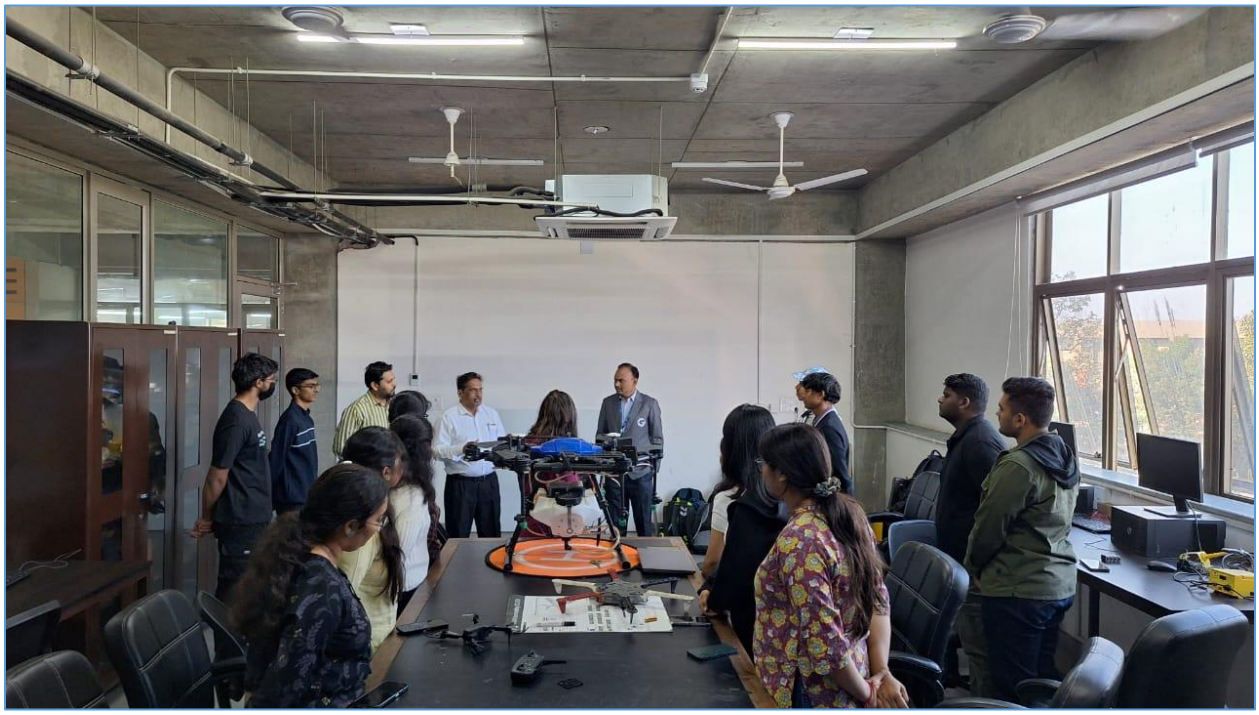
GUIITAR Council: Report 2

Mr. Bimal Bhayani
CEO – GUIITAR
GSFC University

Drone Technician Program in Association with Garuda Aerospace Pvt. Ltd., Chennai

From 6th to 8th February 2025, the GUIITAR Council and GSFC University, in collaboration with Garuda Aerospace Pvt. Ltd., Chennai, organized a three-day offline training session on Drone Technology, led by Dr. K. Ramesh Kumar, Head - RPTO Establishments, Garuda.

The session engaged 15 participants in an in-depth exploration of drone components, operations, and practical applications. Day 1 covered theoretical aspects including drone types like Vajra, Agridrone, and videography drones, historical developments, regulatory frameworks (ICAO & DGCA), and technical components like flight controllers, BLDC motors, and ESCs. On Day 2, students practiced drone piloting through Phoenix Software, simulating square and circular flight patterns, followed by a theory quiz. Day 3 featured a hands-on outdoor flying session where students assembled, armed, and flew drones under expert guidance. The program provided a strong foundation in drone technology, flight dynamics, safety checks, and operational regulations, effectively blending theoretical knowledge with practical exposure.




Applications

GUIITAR Council: Report 3

Mr. Bimal Bhayani
CEO – GUIITAR
GSFC University

Empowering Women Entrepreneurs

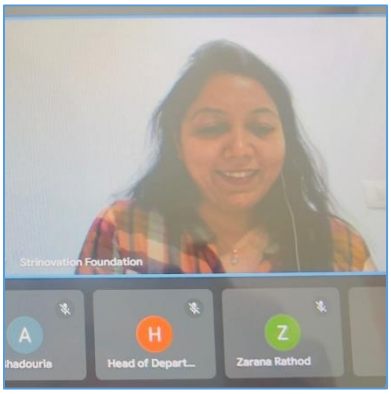
The GUIITAR Council organized a talk session on "Empowering Women Entrepreneurs" on 4th February 2025 at GSFC University to inspire and guide aspiring women entrepreneurs. The session covered key topics such as challenges faced by women in entrepreneurship, financial literacy, leadership development, and the importance of digital transformation. Speakers shared valuable insights on accessing funding through government schemes, venture capital, and angel investors, while also highlighting the role of mentorship, professional networking, and strategic planning. Real-life success stories underscored the importance of resilience, innovation, and a strong support system. The event concluded with an interactive Q&A session, leaving participants motivated and better equipped to navigate their entrepreneurial journeys. Key Takeaways:

- Navigate funding challenges with strategic planning and awareness of support schemes
- Build leadership capabilities and resilient mindsets for sustained growth
- Embrace digital transformation to enhance business reach and efficiency
- Develop strong support systems and networks for long-term success

The session successfully ignited confidence and clarity among women entrepreneurs, empowering them to lead with purpose and passion in today's evolving business landscape

Ms. Mamta Shah, CEO, Mamta Shah & Associates, Vadodara

Ms. Shweta Upadhyay, Founder Director, University Global LLP, Vadodara



Dr. Krupa Mehta, Founder, Strinovation Foundation, Ahmedabad

Sports, NCC and HealthPlex Update

Mr. Mukund Jha
Assistant Professor - Physical Education & Sports
GSFC University

Sports Achievements

The Table Tennis team secured a remarkable victory at the National-level Indus Cup in Ahmedabad (Jan 6-11), winning gold medals, certificates, and a ₹15,000 cash prize. The team included Sheli Patel (B.Tech CSE, 2nd Year), Sharline Job (B.Tech CSE, 3rd Year), and Sakshi Navani (B.Sc. Biotechnology,3rdYear).

Our *Table Tennis Team* emerged as champions at the prestigious *National-level MIT WPU Summit* in Pune (Feb 25 – Mar 1), competing against 150+ elite teams.

Sheli Patel (2nd Year, B.Tech CSE) was awarded *'Best Player of the Tournament'*. The team—Sheli Patel, Sharline Job, and Sakshi Navani—clinched gold medals, certificates, and a

₹7,500 cash prize, bringing pride to our university.

Dev Rajput (B.Tech F&EHS) won Gold Medals in Badminton (Singles & Doubles) at the Khel Mahakumbh District Championship, earning **an ₹8,000 cash** prize and State Level Championship qualification.

Bhakti Mali (BBA-BA, 1stYear) excelled at the KMK 3.0 District Level Swimming Competition, winning gold in 100m Butterfly, silver in 100m Breast stroke & 200m Individual Medley, earning **a ₹11,000 cash prize** and State Level Championship qualification.

At Khel Mahakumbh 3.0 District (Vadodara Rural) Table Tennis Competition, Sakshi Navani (B.Sc. Biotech, 3rd Year) won Gold (Singles, **₹5,000**), Sharline Job (B.Tech CSE,3rdYear) Secured Silver (Singles, **₹3,000**), and together they Clinched Gold (Doubles, **₹6,000**).

Sheli Patel (B.Tech CSE,2ndYear)won Gold in Women's Singles & Mixed Doubles at Khel Mahakumbh 3.0 (Vadodara City)Table Tennis Competition, earning an **₹8,000 cash prize** and State Level qualification.

NCC

Cadet Het Thakker (B.Sc. Biotechnology, 2nd Year) has been selected for RDC 2025, representing in the Prime Minister's Rally and Youth Exchange Program.

SUO Bhrugu Yagnik has been selected for the International Youth Exchange Program in Nepal from October 21 to October 31, 2024.

Cadet Captain Pritam Yadav (BBA, 3rd Year) has been selected for the prestigious Special Sailing Expedition- RDC 2025, among only two cadets from the Gujarat Directorate, under the motto "भारतीयनदियाँ - सस्कं ृदतय कीजननी.

40 NCC cadets from our university participated in a 10m Air Rifle & Pistol Shooting Workshop from February 1 to3.

At Verdict us 2025, a prestigious National Law Fest by Navrachna University, SUO Bhrugu Yagnik (B.Tech CSE, 6th Sem) won the Best Speaker award and the Trophy for Commendable Performance.

Our three NCC cadets participated in the Baroda District Level Rifle and Pistol Shooting Competition, securing two gold medals and one silver medal.

NCC Cadet CSM Mujeeb Leengadia (B.Tech Fire &EHS, 3rd Year) was selected for the prestigious Indian Military Academy -Army Attachment Camp in Dehradun (Dec 23 -Jan 3).

Eshan Devadhara (2nd Year, B.Tech CSE) brought glory to GSFC University by winning the Inter-University Debate Competition.

54 students, including 38 NCC cadets and 16 first- year Fire and EHS students, participated in an enriching Educational field visit to the Air Field, Air Force Station Vadodara.

Three of our NCC Air Wing Cadets have been selected for an exclusive Air Experience Sortie at Vadodara Airfield—Cadet Vrati Arya (CSE, 2nd Year), Cadet Shlok Panchal (Chemical Engg, 2nd Year), and Cadet Dev Purohit (CSE, 2nd Year).

41 students participated in an educational visit to ITM University for the Indian Air Force Induction Publicity Exhibition Vehicle (IPEV) Drive, including 27 NCC Army Wing Cadets, 10 First-Year Fire & EHS Students, and 4 Air Wing Cadets.

HEALTHPLEX

HealthPlex is a state-of-the-art gymnasium equipped with advanced cardio machines, strength training equipment, free weights, and rehabilitation tools.

The new HealthPlex was inaugurated by our esteemed President, Shri P.K. Taneja, IAS(Retd.), on the university's 10th Foundation Day, December 17, 2024.

Every function of HealthPlex is digitally integrated—from slot booking and fitness assessments to knowledge resources, equipment details, and health records—all accessible via the Prayaas application.

GSFC UNIVERSITY
EDUCATION RE-ENVISIONED

GSFC University, Vigyan Bhavan,
P. O. Fertilizer Nagar,
Vadodara-391750, Gujarat, INDIA
T: 0265 – 3093740
: For Feedback kindly mail us at:
feedback.newsletter@gsfcuniversity.ac.in

FOLLOW US ON :

gsfcuniversity gsfcuniversity
www.gsfcuni.edu.in