

THE ZERO DAY

NEWSLETTER

VOL. 2
SEPT. 26



- > INIT SYSTEM
- > SCAN NETWORK
- > FIND VULNERABILITIES
- > PATCH. PROTECT. REPEAT.
- > _

**SYSTEM
BREACHED!**

NOT ALL
SUPERHEROES
WEAR CAPES.
SOME SECURE
YOUR SYSTEMS.

ZERO
TRUST

**SECURING
TRUST.
EMPOWERING
INNOVATION.**



- > DEFEND
- > DETECT
- > RESPOND
- > RESILIENCE

TABLE OF CONTENTS

Our Team

Convocation Glimpses

Message to our Graduates

Announcement

Research & Innovation

Cyber News

Cyber Security Insights

Vulnerability Spotlight

Tools of the Month

Emerging Technologies

Career & Internship Corner

- Opportunities

- Internships

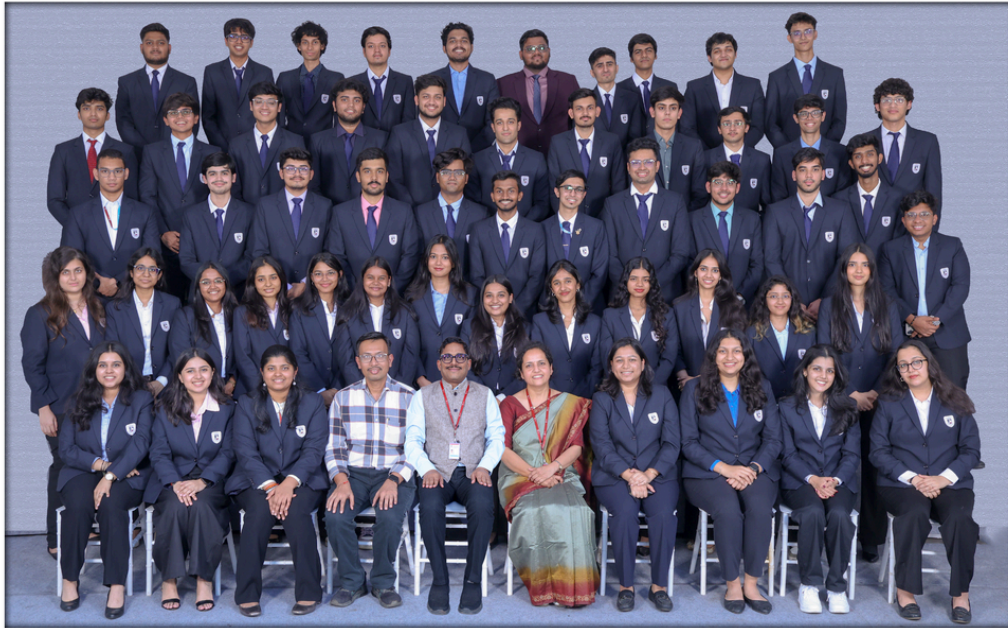
- Current Placement Positions Offered

Puzzle Corner

CONVOCAATION GLIMPSES



Mukesh Patel School of Technology Management & Engineering



B Tech Computer Science and Engineering (Cybersecurity) 2025

Studio Kiran

AVANI BHAT



“Honoured to share that I secured 2nd rank in B.Tech. CSE Cybersecurity at NMIMS Mukesh Patel School of Technology Management and Engineering! My sincere thanks to Ashwini Bhide ma'am and Sougata Ray sir for bestowing me with my medal and certificate, as well as my mentors Dr. Ashwini Rao ma'am, Dr. Pintu Shah sir, Dhanashree Kulkarni ma'am, and the faculty for their continuous guidance and support.

I am deeply grateful to my family and friends for keeping me motivated through every late-night project and study session. This milestone is truly unforgettable, and I will always be thankful to everyone who supported me along the way.

”

[Linkedin Post](#)

CONVOCATION GLIMPSES



MANAVI NANDIMATH

“

I'm incredibly proud and grateful to share that I have officially graduated with a B.Tech in Computer Science & Engineering – Cyber Security from SVKM's NMIMS Mukesh Patel School of Technology Management & Engineering (MPSTME).

Adding an even more special milestone to this journey, I'm honoured to have been recognized on the Dean's List as a Meritorious Student of my batch.

This achievement is not just a certificate to me; it is a reflection of the years of hard work, learning, challenges, projects, assignments, examinations, and all the moments that shaped me throughout college.

”

NMIMS | CLASS OF
2026

COMPUTER SCIENCE & ENGINEERING –
CYBER SECURITY | MPSTME, NMIMS



RISHAB TIWARI

“

The biggest lesson these four years gave me was simple: It's not just about learning concepts. It's about understanding how they work, why they matter, and where they fit in the real world.

”

NMIMS | CLASS
OF 2026

B.TECH | MPSTME,
NMIMS



SWARAJ TANDEL

“

Looking back, college was about much more than earning a degree. It was about discovering my interests, stepping outside my comfort zone, learning from failures, celebrating small wins, and meeting people who made the journey memorable.

”

NMIMS | CLASS
OF 2026

B.TECH | MPSTME,
NMIMS

A MESSAGE TO OUR GRADUATES

Dear Graduates,

As you turn the page on your university journey, you take with you more than a degree. You carry the lessons learned in classrooms and labs, the challenges that shaped you, the friendships that became memories, and the experiences that helped you discover who you are becoming.

The world of cybersecurity is constantly changing. New technologies will emerge, new threats will challenge you, and the answers will not always be found in a textbook. Stay curious enough to keep learning, brave enough to explore the unknown, and grounded enough to use your knowledge responsibly. Let ethics guide your decisions and let innovation drive your work.

Your journey ahead may take you into cybersecurity, research, technology, entrepreneurship, or somewhere you have not yet imagined. Wherever you go, remember that growth rarely happens by staying comfortable. Ask questions. Take risks. Learn from failure. Build things. Protect what matters. And never underestimate the impact that one determined individual can make.

As you step beyond the university, we hope you carry forward not only the skills you have gained, but also the integrity, resilience and confidence to make a difference.

The next chapter is yours to write.

May it be filled with meaningful challenges, bold ideas, remarkable achievements, and endless opportunities to grow.

Go forward. Stay curious. Keep learning. Keep securing the future.

With warm wishes for your journey ahead,
Department of Cybersecurity,
MPSTME

CYBERSECURITY ARTICLE WRITING COMPETITION 2026

“
**WRITE INSPIRE
SECURE
TOMORROW**
”



AWARDS & RECOGNITION



Top 2 articles will
be awarded at the
Department Level.



All eligible articles will
be featured in the
ZeroDay Department
Newsletter.

ARTICLE DOMAINS

1. Threats & Frauds – Ransomware, phishing, malware, cyber frauds
2. Data & Emerging Tech Security – Data breaches, cloud, IoT, blockchain, quantum
3. AI, Hacking & Forensics – AI, ethical hacking, digital forensics
4. Response & Security Management – Incident response, security policies
5. Laws, Privacy & Compliance – Cyber laws, privacy, compliance

DEPARTMENT OF CYBERSECURITY

Invites all Cybersecurity students to participate in the Article Writing Competition 2026 and showcase your insights on contemporary cybersecurity issues and innovations.

**SUBMISSION DEADLINE
11 SEPTEMBER 2026**



ELIGIBILITY & GUIDELINES

Open to all years of the Department of Cybersecurity. Participation can be individual or in a group (maximum 3 members). Word limit: 250 to 300 words. Plagiarism and AI-generated content must be less than 10%. Articles must be original and relevant to the chosen domain.

POINT OF CONTACT

Dr. Rejo Mathew
Prof. Rohit Suryawanshi

STUDENT VOICES
FOR A SAFER DIGITAL WORLD

RESEARCH AND INNOVATION

THE ATTACK YOU NEVER SEE COMING: ZERO-CLICK EXPLOITS

Most cyberattacks require you to make a mistake, you click on the wrong link, open the wrong attachment, or download something that you shouldn't have. Zero-click attacks eliminate the need for such a mistake. A zero-click exploit works by taking advantage of software that automatically processes incoming content. A victim may only need to receive a message, image, or other piece of data for the vulnerable application to handle it and trigger the attack. There is no warning telling the user to "click here." Sometimes there is no visible sign that anything happened at all.

A good and recent example of this is 'LANDFALL', an Android spyware framework that was uncovered by Palo Alto Networks' Unit 42. The researchers identified malicious Digital Negative (DNG) image files intended for exploiting a vulnerability in Samsung's image-processing software. Since devices are capable of automatically processing images, a malicious image could in principle be used as a means of attack even if the victim did not deliberately open it. Samsung fixed the vulnerability in April 2025.

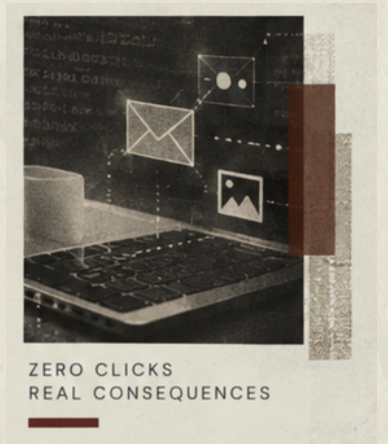
What is interesting about cases such as LANDFALL is that the image itself is not necessarily the element which the victim is tricked into trusting. Instead, the attack is directed at the software which processes the image. The main takeaway with regard to zero-click exploits is that modern devices continuously receive and process various types of content in the background, such as images, messages, documents, network traffic and are now even given AI-generated instructions. Every automatic process creates another opportunity for a vulnerability to be triggered. In the field of cybersecurity, user awareness has its limitations; although you can train people not to click on suspicious links, you can't train them to prevent an attack that in no way requires a click. The defence needs to go deeper by means of secure coding, isolation, sandboxing, quickly applying patches and monitoring for any unusual behaviour.

The most hazardous attack is the one which never asks you to take any action.

By:- Abner Rebello



“THE MOST HAZARDOUS ATTACK IS THE ONE WHICH NEVER ASKS YOU TO TAKE ANY ACTION.”



REFERENCES:

PALO ALTO NETWORKS UNIT 42 "LANDFALL: NEW COMMERCIAL-GRADE ANDROID SPYWARE DISCOVERED IN THE WILD" (2026).
RESEARCH ON LANDFALL, MALICIOUS DNG IMAGES, AND THE SAMSUNG VULNERABILITY.
SPRINGER NATURE – DISCOVER NETWORKS – "REVIEW OF ZERO-CLICK ATTACKS AND ZERO-TRUST SECURITY MODEL: CONCEPTS, ARCHITECTURE, STATE OF THE ART, AND FUTURE DIRECTIONS", 28 APRIL 2026.

RESEARCH AND INNOVATION

WHEN ROLES BECOME THE ATTACK SURFACE: LLM SECURITY

We typically view an AI prompt as being no more than a simple conversation: the system provides instructions, the user poses a question, and then the AI gives a response. However, recent research is revealing a far more unusual issue – the AI does not always have a dependable method of deciding who it should trust.

Large Language Models (LLMs) make use of labels such as system, user, and assistant in order to decide which instructions should be given priority. The system message is intended to be the most trustworthy layer, but the issue is that these labels do not correspond to a conventional security boundary; to the model they are still part of the text it is processing. This was shown by the researchers at ICML 2026 using a method they called Chain-of-Thought Forgery. Rather than just instructing the AI to ignore its safety rules, an attacker can produce some text which mimics the style of the model's own way of reasoning and then use it to affect the model's behaviour. The attack is in effect taking advantage of the AI's understanding of the structure of its own conversations.



“THE MORE WE UNDERSTAND HOW AI CAN BE FOOLED, THE BETTER WE CAN BUILD SYSTEMS THAT TRULY REMAIN TRUSTWORTHY.”



UNDERSTANDING
VULNERABILITIES
BUILDS STRONGER AI

The situation becomes even more interesting if AI is able to perceive more than just text. Malicious instructions can be embedded within images when using multimodal AI. An image, such as a screenshot, a document, a webpage or an advertisement, may appear entirely harmless to a person even though it includes instructions intended to affect the AI system handling it. This is referred to as multimodal prompt injection. The fact that an AI can be tricked into giving an unwanted response is worrying on its own. However, many current AI systems are linked to browsers, email systems, files, coding environments and enterprise tools. In that case, the question changes from simply being “Can the AI be fooled?” to “What can it do after being fooled?”. That is why securing LLMs increasingly means more than writing better prompts. Separation between trusted instructions and external content, sandboxing, limited permissions and continuous adversarial testing are becoming essential.

By:- Abner Rebello

REFERENCES:

THE REGISTER – SECURITY RESEARCHERS TRICKED LLMS..., 30 JUNE 2026.

CLOUD SECURITY ALLIANCE AI SAFETY INITIATIVE – IMAGE-BASED PROMPT INJECTION: HIJACKING MULTIMODAL LLMS THROUGH VISUALLY EMBEDDED ADVERSARIAL INSTRUCTIONS, 8 MARCH 2026.

ACM DIGITAL LIBRARY – ANALYSIS OF LLMS AGAINST PROMPT INJECTION AND JAILBREAK ATTACKS, LM-SHIELD '26, 1 JUNE 2026.



CYBER NEWS

ELECTRONICS AND THE SILENT SUPPLY-CHAIN LEAK

A cyberattack does not always need to shut down a factory to cause serious damage. In June 2026, Tata Electronics confirmed a cyber incident after the data-extortion group World Leaks claimed to have stolen around 630.4 GB of data across more than 204,000 files. Reported material included internal communications, employee documents, manufacturing records and confidential files connected to major technology companies.

The incident drew particular attention because Tata Electronics plays an important role in Apple's India-based iPhone manufacturing ecosystem and works with other major technology companies. The exact method used to gain initial access has not been publicly confirmed, so claims about phishing, stolen credentials or a specific vulnerability should be treated cautiously.

What makes the incident particularly important is that it appears to centre on data theft and extortion rather than widespread ransomware encryption. There were no reports of large-scale factory shutdowns caused by encrypted systems. The case highlights a critical supply-chain lesson: an organisation's security does not end at its own network perimeter.

By:- Srinidi Subramaniam

THE TAKEAWAY

Vendors must be treated as part of the security boundary, with strong access controls, continuous monitoring and effective detection of unusual data movement.

Puzzle Corner

RANK THE PASSWORD

Put these five passwords in order from weakest to strongest.

1. Password123
2. P@sswOrd!
3. Tr0ub4dor&3
4. Lemonpie
5. Xzy@127

CIPHER CRACKER

Atbash Cipher

The alphabet is mirrored:

A↔Z, B↔Y, C↔X...

GIFHG YFG EVIRUB

CIPHER CRACKER

Binary

Each 8-digit block is one letter's ASCII code. A space between words is its own block.

```
01001101 01000110
01000001 00100000
01010011 01010100 01001111
01010000 01010011
00100000 01000010
01010010 01000101
01000001 01000011
01001000 01000101
01010011
```


CYBER NEWS

AURORA: HACKERS MANIPULATE AN AI CODING AGENT TO BREAK INTO COMPANIES

AI coding assistants are designed to make developers faster. But what happens when attackers turn those same capabilities against organisations?

In August 2026, Russian-speaking cybercriminals reportedly abused Cursor, an AI-powered coding assistant, during attacks against at least seven companies. The campaign, known as AurOra, highlights a growing concern in cybersecurity:- AI tools can become part of the attack chain when their legitimate capabilities are manipulated by threat actors. Instead of simply using AI to generate code, attackers reportedly used the coding environment to assist with malicious activities, including attack planning and execution.

CloudSEK's investigation provides a deeper look into the campaign, including its ransomware-related activity and supporting infrastructure. The incident is significant because the AI itself was not necessarily the vulnerability. Rather, attackers found ways to make a legitimate development tool work in their favour. For security teams, this creates a new challenge.

AI coding environments need the same scrutiny as other privileged development tools, particularly when they can access source code, terminals, files or organisational systems itself.

By:- Srinidi Subramaniam

THE TAKEAWAY

As AI becomes more deeply integrated into software development, securing the AI-assisted development environment is becoming just as important as securing the code.

Puzzle Corner

PORT MATRIX

Match the pairs:

- | | |
|--------------|----------|
| 1. Port 22 | A. HTTPS |
| 2. Port 80 | B. SSH |
| 3. Port 443 | C. RDP |
| 4. Port 3389 | D. HTTP |
| 5. Port 21 | E. DNS |
| 6. Port 3389 | F. FTP |

TWO TRUTHS AND A BREACH

Yahoo (2013–2014 breaches)

- A. The breach first disclosed in 2016 ultimately turned out to affect all 3 billion Yahoo accounts.
- B. Yahoo discovered and publicly disclosed the breach within 24 hours of it happening in 2013.
- C. The stolen data included security questions and answers, not just passwords.

CYBERSECURITY INSIGHTS

Chain Reconnaissance: Breaking Air-Gapped Networks from the Outside

An air-gapped network sounds like the ultimate cybersecurity fortress. No direct internet connection, limited external access and layers of isolation. But attackers do not always need to break through the front door. Supply chain reconnaissance focuses on finding the organisations, contractors, software dependencies and cloud services that sit around a high-value target.

Instead of attacking a heavily monitored corporate network directly, an adversary can look for a weaker partner that already has some level of trusted access. MITRE ATT&CK classifies this under Supply Chain Compromise (T1195), covering attacks involving software, hardware and third-party services. The wider lesson is that trust relationships can become attack paths.

From an attacker's perspective, the strategy is simple:- Why spend months trying to bypass a heavily protected perimeter when a less-secure contractor may provide a much easier route? For defenders, this changes the definition of the security perimeter. Vendor accounts, software packages, cloud platforms and outsourced services all need to be monitored as potential entry points.

By:- Srinidi Subramaniam

THE TAKEAWAY

An organisation may be completely secure from the outside and still be exposed through the people and systems it trusts.

Puzzle Corner

CYBER SCRAMBLE

Unscramble these 4 essential cybersecurity terms:

- O A R W A M N S E
- H P I S I N G N
- F I R A L E W L
- I Z O R T O E R D A

TWO TRUTHS AND A BREACH

Target (2013)

- A. Attackers got their initial foothold using network credentials stolen from a third-party HVAC vendor.
- B. The breach exposed around 40 million customers' credit and debit card numbers.
- C. Target's security tools caught the intrusion within hours and shut it down before any data left the network.





VULNERABILITY SPOTLIGHT

CVE-2026-42271 – BerriAI LiteLLM Command Injection

LiteLLM, BerriAI's lightweight open-source proxy framework that has been widely employed to proxy language model APIs, faces a critical security threat at the moment because of the vulnerability CVE-2026-42271, which has been recently discovered. The problem is that a vulnerability occurs when the parameters parsing mechanism does not allow attackers to bypass security and inject arbitrary shell commands, which turns out to be a critical problem. This security flaw has been added to the list of critical vulnerabilities that require urgent attention.

According to the national vulnerability database, this security flaw has been classified as critical, meaning that it receives the maximum possible score according to the CVSS v3/v4 scoring system. As for the nature of the attack, executing the remote code enables the attacker to get complete access to the AI servers. However, it should be said that the attack surface of this security problem is broader than that because of the fact that it enables 100% control over the host server.

The threat is not hypothetical since on June 8th, CISA included the exploit CVE-2026-42271 in its list of "Known Exploited Vulnerabilities". Hence, the fact that the vulnerabilities were indeed exploited in the cyber-attack chain in order to gain an entry into the targeted network became known. With such a directive by CISA, there was a mandatory requirement for the mitigation of these security risks. By ensuring that the organization patched up the vulnerability, CISA was able to reduce the surface area exposed due to the zero-day vulnerability.

By:- Deetya Shivathaya

Puzzle Corner

CIPHER CRACKER

Caesar Shift (key: 3)

SDVVZRUG PDQDJHUV VDYH
OLYHV

TWO TRUTHS AND A BREACH

WannaCry (2017)

A. WannaCry spread using EternalBlue, an exploit targeting a Windows SMB vulnerability.

B. A researcher slowed the outbreak by registering a domain that acted as an accidental "kill switch."

C. WannaCry only hit computers running the newest, fully patched version of Windows 10.





TOOLS OF THE MONTH



Velociraptor - Hunting Threats Across Endpoints

Velociraptor is an open source, digital forensics and incident response (DFIR) platform. Designed to collect evidence at the endpoint, it helps investigate suspicious activity and perform threat hunting. In their version 0.77, Velociraptor introduced interactive shell sessions where each command appends to the same flow, replacing the previous approach where each interaction ran as a separate flow.

Apart from this, Velociraptor contains extensive memory analysis and effective detection capabilities.

This tool is currently on the rise and gives students an exposure to the world of professional DFIR, or threat hunting workflow, instead of the traditional scanning tools.

By:- Deetya Shivathaya

Volatility 3 Forensic Memory Framework Official Documentation

Volatility 3 is an open-source, cross platform digital forensic framework that has been designed to perform volatile memory (RAM) analysis. It checks system memory dumps from endpoints to rebuild execution state without having to depend upon the target operating system.

Incident response teams, Tier 2/3 analysts and forensic investigators use the tool during live threat hunting and post-breach investigations.

Volatility allows investigators to analyse non-volatile evidence stored in RAM, without having to worry about the problem of the malicious binaries being written on physical hard drives.

From beginners to advanced users, Volatility serves as a daily tool for hunting malware persistence and extracting injected binaries.

By:- Deetya Shivathaya





EMERGING TECHNOLOGIES

The AI Analyst That Never Sleeps - AI SOC

A Security Operations Centre (SOC) has a familiar problem: too many alerts and not enough people to investigate them. Every suspicious login, unusual connection, malware detection or endpoint event can create another alert for an analyst to examine. AI SOC agents are emerging as a way to change that workflow. Instead of simply displaying alerts, these systems can investigate them, collect context from security tools, decide how serious they are and, in some cases, take response actions. The interesting part is the autonomy. A conventional security automation tool operates according to a set playbook, if X occurs, then carry out Y. An AI agent, on the other hand, is able to carry out a less predictable kind of investigation. It could link an endpoint alert with identity activity, check the cloud logs, refer to threat intelligence and then give a conclusion to the analyst.

Recent industry deployments indicate that multi-agent systems are being used across endpoint, identity, Software-as-a-Service (SaaS), cloud and network data, with investigations being reduced from hours to minutes. However, when an AI is given access to the SOC a brand new kind of problem arises because the security data itself can then become an attack surface. Logs, filenames, HTTP headers, command lines and other telemetry can contain attacker-controlled text. Researchers and security practitioners have warned that an attacker could plant instructions inside this data and potentially influence an AI agent investigating an alert.

The next generation of SOC's might therefore involve more than just replacing analysts with AI. It could involve finding a suitable balance between speed and trust.

An AI that investigates 1,000 alerts instantly is impressive. An AI that investigates 1,000 alerts instantly and knows when not to trust what it is reading is far more impressive.

By:- Abner Rebello

Puzzle Corner

INCIDENT RESPONSE RELAY

Correct the order:

- 1.Eradication
- 2.Preparation
- 3.Recovery
- 4.Detection & Analysis
- 5.Post-Incident Activity (Lessons Learned)
- 6.Containment

TWO TRUTHS AND A BREACH

Human Factor Facts

- A. Simple, guessable passwords like "123456" have topped leaked-password lists for years running.
- B. Industry breach reports consistently find that most breaches involve a human element phishing, error, or stolen credentials.
- C. Multi-factor authentication blocks 100% of account-takeover attempts with zero known exceptions.

CAREER AND INTERNSHIP

INTERNSHIP OPPORTUNITY

SECURITY CONSULTANT INTERN

CloudSEK | Bengaluru

Gain hands-on experience in VAPT, threat intelligence, OSINT, dark-web monitoring and attack-surface security.

Eligibility: Students or recent graduates in Computer Science, Information Security or related fields.

Preferred: VAPT knowledge, CTFs, bug bounties or security research

Work Areas: Web • API • Mobile • Cloud

Security Status: Applications

OpenApply: CloudSEK Careers SOC

CURRENT PLACEMENT POSITIONS

CYBER SECURITY ANALYST

Craw Security | New Delhi

Craw Security is hiring freshers and experienced candidates for its cybersecurity team, with openings across SOC, VAPT, cyber forensics, cloud security and security engineering.

Eligibility: Graduates in CS/IT/Cybersecurity

Location: New Delhi

Type: Full-time

Roles: SOC • VAPT • Cyber Forensics • Cloud Security

Experience: Freshers welcomed

Hiring: September 2026

OPPORTUNITY

IIT Madras Pravartak × SWAYAM Plus Cloud & Cybersecurity Programmes

IIT Madras Pravartak Technologies

Foundation and SWAYAM Plus have launched programmes focused on multi-cloud computing and cybersecurity skills, helping learners build industry-relevant knowledge in rapidly evolving technology areas.

Registrations open: 10 September 2026

Focus: Cloud Computing • Cybersecurity • Industry Skills

For: Students & learners interested in emerging technology

A useful opportunity for students looking to strengthen their technical profile beyond the classroom.

INTERNSHIP OPPORTUNITY

INTERN Irdeto | Noida

Work with Irdeto's Service Operations team to monitor security alerts, investigate application and infrastructure incidents, support AWS-hosted systems and assist with incident response.

Skills: Windows/Linux • IP Networking • AWS • Python/Bash/PowerShell

Tools: Grafana Cloud • AWS CloudWatch • Pingdom.



PUZZLE CORNER

HOW TO PLAY:-

Mark a square every time something on the bingo card has happened to you or a colleague in the past month. Keep going until you complete a row, column, or diagonal. First to complete one? Shout "SECURE BINGO!"

BINGO

Got a "package delivery failed" text you almost clicked	Reused a password you swore you'd change	Spotted a sticky note with a password on it	Ignored a software update notification (again)	Got a call from "IT Support" you didn't request
Used public Wi-Fi without a VPN	Got a "CEO" email asking for gift cards	Hit "Remind me tomorrow" on an MFA prompt	Spotted a phishing email and reported it	Locked your screen before stepping away
Found a USB drive and wondered: plug it in?	Changed a default router/admin password	Got tagged in a "you won a prize!" message	FREE SPACE	Used a password manager for the first time
Paused on "urgent: verify your account" to check the sender	Backed up important files this month	Got a sketchy "recruiter" DM	Enabled 2FA on an old, forgotten account	Spotted a "quishing" QR code attempt
Had a "wait, is this real?" moment before clicking	Reminded a colleague not to overshare online	Received a fake invoice / wire-transfer request	Noticed a look-alike domain (like arnazOn.com)	Actually read a phishing-simulation training email

OUR TEAM

EDITOR-IN-CHIEF



**Prof. Rohit
Suryawanshi**

Department of
Cyber Security

MANAGING EDITOR



**RAHUL
BEHERA**

CONTENT & RESEARCH



ABNER REBELLO

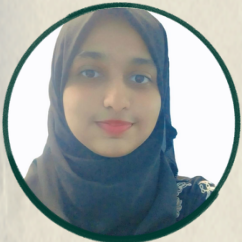


SRINIDI SUBRAMANIAM



DEETYA SHIVATHAYA

TECH & RESEARCH



AYESHA TOOFANI



ATIYA SRIVASTAVA



PIYUSH SHUKLA



SHIVANK KAKKAD



AANYA KASARAGOD

DESIGN & MEDIA



MIRARI KAPADIA



GAURI GHADAGE

QUALITY ASSURANCE



AASHVIKA DUBEY



YUVRAJ BISHNOI

JOIN OUR TEAM



Had Fun Reading?

Work with us!

Join the Zeroday Newsletter



Follow us on Linkdin:

[@zeroday-cybersecurity-newsletter](#)

