CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #139

NEWS:

1. Autonomous, GenAI-Driven Attacker Platform Enters the Chat

Original Source: Dark Reading by Elizabeth Montalbano

The introduction of an autonomous, GenAI-driven attacker platform marks a significant evolution in cyber threat capabilities, introducing a new era of automated cyber attacks.

This sophisticated platform, powered by generative AI, autonomously crafts and executes cyber strategies with unprecedented efficiency and scale, drastically enhancing the threat landscape.

As these AI-driven technologies become more prevalent, they pose complex challenges for cybersecurity defences, necessitating not only faster responses but also a fundamental rethink in how cyber defences are structured and implemented.

This shift demands an accelerated advancement in defensive technologies to match the pace of AI-driven offensive capabilities, reshaping the future of cybersecurity.

CyberSecurity Advisors Network

NEWS:

2. EncryptHub's dual life: Cybercriminal vs Windows bug-bounty researcher

Original Source: BleepingComputer by Bill Toulas

In a striking revelation of the dual nature within the cybersecurity industry, EncryptHub emerges as a figure who navigates between heroism and villainy.

By day, this individual exploits their expertise as a Windows bug-bounty researcher, identifying and patching critical vulnerabilities to bolster system security. By night, however, EncryptHub transforms into a cybercriminal, leveraging the same vulnerabilities for personal gain in various illegal activities.

This dual existence not only underscores the ethical complexities faced by those within the cybersecurity realm but also highlights the precarious balance between contributing to cybersecurity and undermining it through criminal conduct.

This duality sparks a broader discussion about the moral responsibilities and potential for conflict inherent in roles that straddle legal and illegal cyber activities.

CyberSecurity Advisors Network

NEWS:

3. Voluntary ‘Pall Mall Process’ seeks to curb spyware abuses

Original Source: Cyberscoop by Tim Starks

The 'Pall Mall Process', a newly introduced voluntary initiative, is spearheaded by an international coalition aiming to impose ethical boundaries on the use of spyware.

This process advocates for transparency, accountability, and strict governance to mitigate the misuse of surveillance tools that often infringe on privacy and human rights.

By establishing clear guidelines and oversight mechanisms, the initiative seeks to restore trust in technology used for lawful interception and to ensure that such tools do not become instruments of oppression or exploitation.

The effectiveness of this voluntary approach, however, remains a topic of debate among experts, who are concerned about its enforceability and the willingness of key stakeholders to comply.

CyberSecurity Advisors Network

NEWS:

4. That massive GitHub supply chain attack? It all started with a stolen SpotBugs token

Original Source: The Register by Jessica Lyons

A recent in-depth investigation has unveiled the origins of a massive supply chain attack on GitHub, tracing back to a compromised SpotBugs token.

This token, essential for code analysis and bug identification, became the hackers' gateway to infiltrate and manipulate software dependencies widely used across the platform.

The breach highlights the growing risks and complexities in software supply chain security, emphasising the necessity for robust verification processes and tighter security protocols around third-party tools.

As companies and developers grapple with these challenges, this incident serves as a crucial reminder of the vulnerabilities inherent in open-source ecosystems and the ongoing need for heightened vigilance and improved security practices to protect against such sophisticated attacks.

CyberSecurity Advisors Network

NEWS:

5. EU wants to give encryption backdoors a try, despite pushback

Original Source: The Stack by Noah Bovenizer

The EU's new ProtectEU security strategy proposes giving law enforcement access to encrypted data, aiming to enhance internal security across member states.

This approach, aligned with policies in the UK, India, China, and Australia, faces strong opposition over concerns that it could undermine digital trust and user privacy.

Critics emphasise the risks of weakening encryption, which could potentially expose users to cyber threats.

Additionally, the strategy addresses reducing dependencies on non-EU tech suppliers and advancing quantum-safe encryption, reflecting an effort to boost the EU's technological sovereignty and overall security framework.

CyberSecurity Advisors Network

NEWS:

6. Google addresses 2 actively exploited vulnerabilities in security update

Original Source: Cyberscoop by Matt Kapko

Google has recently issued a critical security update addressing two vulnerabilities that were actively being exploited by cybercriminals.

These flaws, found within Google's software, posed significant threats allowing attackers to execute malicious code and gain unauthorised access to user data.

The swift response by Google underscores the relentless pace of cyber threats and the continuous need for proactive security measures.

This update is part of a broader effort to fortify defences and assure users of their data's safety amidst an escalating landscape of digital vulnerabilities. By closing these security gaps, Google aims to not only protect individual users but also maintain trust in its software ecosystems, crucial for both personal and corporate users.

CyberSecurity Advisors Network

NEWS:

7. Scattered Spider's 'King Bob' Pleads Guilty to Cyber Charges

Original Source: Dark Reading by Kristina Beek

In a landmark legal development within the cybersecurity community, the notorious hacker known as 'King Bob', affiliated with the cybercrime group Scattered Spider, has pleaded guilty to multiple cyber charges.

This case marks a significant victory for law enforcement agencies in their ongoing battle against cybercriminal networks. 'King Bob's' activities included orchestrating various high-profile attacks that compromised sensitive data across multiple industries.

The guilty plea not only brings a measure of justice but also serves as a deterrent, highlighting the increasing effectiveness of international cooperation in tracking and prosecuting cybercriminals.

This event reinforces the message that the cyber realm is no longer a lawless frontier, and that significant consequences await those who engage in malicious online activities.

CyberSecurity Advisors Network

NEWS:

8. Malicious VSCode extensions infect Windows with cryptominers

Original Source: BleepingComputer by Bill Toulas

The discovery of several malicious extensions for Visual Studio Code (VSCode) has raised alarms about the security of popular developer tools.

These extensions, once installed, secretly deploy cryptominers on Windows systems, exploiting the computational resources of unsuspecting users to mine cryptocurrency.

This incident highlights a growing trend where seemingly benign software tools are weaponized to serve cybercriminal agendas. It underscores the importance of vigilant security practices such as scrutinising software sources and updates.

The infiltration via trusted applications like VSCode not only jeopardises user systems but also calls into question the security measures of software repositories and the need for enhanced scrutiny and verification processes to prevent similar breaches in the future.

CyberSecurity Advisors Network

NEWS:

9. NSW Electoral Commission asks for cyber security top-up

Original Source: itNews by Ry Crozier

In a proactive step towards securing electoral integrity, the NSW Electoral Commission has requested additional funding to bolster its cyber security measures.

This request comes in response to increasing threats to digital electoral systems, highlighting the need for robust protections against potential cyber intrusions that could compromise election results.

The commission aims to enhance its defensive capabilities to ensure that voter information and election processes remain secure and trustworthy. As cyber threats continue to evolve, such actions signify a growing recognition of the critical importance of cybersecurity in safeguarding democratic institutions.

This move also reflects a broader trend of electoral bodies worldwide enhancing their security postures in anticipation of future electoral events.

CyberSecurity Advisors Network

NEWS:

10. Chrome to patch decades-old flaw that let sites peek at your history

Original Source: The Register by Thomas Claburn

In a significant security update, Chrome is set to patch a long-standing flaw that has allowed websites to covertly inspect users' browsing histories.

This vulnerability, which has persisted for decades, could enable websites to gather personal information without user consent, posing serious privacy concerns.

The fix, part of Chrome's ongoing efforts to enhance user security and privacy, aims to prevent any site from exploiting this flaw to track user activities across the web.

This move is a crucial step towards safeguarding user data and maintaining the integrity of personal browsing information, reinforcing Chrome's commitment to user privacy in an increasingly invasive digital landscape.

CyberSecurity Advisors Network

NEWS:

11. UK's attempt to keep details of Apple 'backdoor' case secret... denied

Original Source: The Register by Connor Jones

The UK government's effort to maintain secrecy over a legal case involving Apple and alleged backdoor access to its devices has been thwarted by a court decision, mandating transparency.

The case revolves around government requests for access mechanisms in Apple's devices, which critics argue could undermine user privacy and security.

The court's decision to deny secrecy highlights the ongoing tension between national security needs and individual privacy rights.

This ruling is seen as a victory for advocates of digital privacy, asserting the public's right to be informed about government actions that could potentially compromise personal security and privacy standards in technology products.

CyberSecurity Advisors Network

NEWS:

12. EDR-as-a-Service Makes the Headlines in the Cybercrime Landscape

Original Source: Security Affairs by Pierluigi Paganini

The cybercrime landscape is witnessing the rise of Endpoint Detection and Response (EDR) as a Service, offering organizations advanced tools to detect and respond to threats in real-time.

This service model enhances cybersecurity postures by providing continuous monitoring and analysis of endpoint activities, crucial for identifying and mitigating potential threats quickly.

With cyber threats becoming more sophisticated, EDR services are becoming essential for businesses of all sizes, particularly those with limited in-house security capabilities.

By outsourcing critical security functions, companies can focus on core operations while ensuring that their networks remain protected against evolving cyber threats. The adoption of EDR-as-a-Service also highlights a shift towards more dynamic and responsive cybersecurity strategies in an era of unpredictable cyber risks.

CyberSecurity Advisors Network

NEWS:

13. European Commission pushes for encryption ‘backdoors

Original Source: Brussels Signal by Paddy Belton

In a controversial move, the European Commission is advocating for the implementation of 'backdoors' in encryption technologies, a proposal that has sparked intense debate across the tech and privacy sectors.

These backdoors, intended for law enforcement access, raise significant concerns about the potential for abuse and the undermining of digital security.

Critics argue that creating systematic weaknesses in encryption could be exploited by malicious actors, compromising the safety of all users.

This push by the European Commission reflects the ongoing struggle to balance security needs with the protection of individual privacy rights in an increasingly digital world, highlighting the complex interplay between technology, law, and ethics.

CyberSecurity Advisors Network

NEWS:

14. EU set to fine Elon Musk's X up to $1 billion for breaking disinformation law

Original Source: Irish Star by Jeremiah Hassel

The European Union is poised to levy a significant fine, potentially up to $1 billion, against Elon Musk's social media platform X for failing to comply with its disinformation regulations.

This action highlights the EU's stringent stance on controlling the spread of false information online.

The potential fine underscores the challenges tech companies face when operating in jurisdictions with strict regulations on online content.

This case serves as a critical reminder of the financial and reputational risks associated with non-compliance in an era where digital platforms are increasingly held accountable for the content they host.

CyberSecurity Advisors Network

NEWS:

15. E-ZPass toll payment texts return in massive phishing wave

Original Source: BleepingComputer by Bill Toulas

A massive phishing campaign is targeting E-ZPass users, sending fraudulent texts that mimic toll payment notifications.

These deceptive messages aim to trick recipients into divulging personal information by clicking on malicious links purportedly for paying tolls.

This surge in phishing attacks underscores the continuing vulnerability of consumers to identity theft and financial fraud through seemingly legitimate communications. It highlights the importance of vigilance and the need for continuous public education on recognising and avoiding phishing schemes to protect personal and financial information.

CyberSecurity Advisors Network

CyAN Members Only

Are You In the #CyANQuiz?

Hey CyAN Champions,

Round One of the Quarterly #CyANQuiz Challenge is officially in the books—congrats to those who took the plunge! Missed it? Oof. You're going to have to wait for Round Two to redeem yourself... but don't worry, it's coming soon.

🔹 **30 Questions. Timed. No second chances.**
🔹 **Based on Recent Cybersecurity News & Events**
💡 **Why Play? Bragging rights. Community glory. Actual prizes. And the satisfaction of knowing you're sharper than your peers (well, most of them).**

This isn't just a quiz—it's a year-long leaderboard battle to find CyAN's sharpest minds.

So start reading, start prepping... and next time, don't miss your shot at the cyber crown!

NEWS:

16. Expert Used ChatGPT-4O to Create a Replica of His Passport in Just 5 Minutes Bypassing KYC

Original Source: Security Affairs by Pierluigi Paganini

A cybersecurity expert demonstrated the potential misuse of AI by using ChatGPT-4O to create a fake passport in just five minutes, successfully bypassing Know Your Customer (KYC) protocols.

This experiment highlights the emerging risks associated with AI technologies in identity verification processes.

The ease with which the passport was replicated raises significant concerns about the effectiveness of current KYC measures and the potential for AI to facilitate identity fraud.

This case stresses the urgent need for robust safeguards and updates in verification systems to counteract the sophisticated capabilities of modern AI.

CyberSecurity Advisors Network

NEWS:

17. Microsoft Credits EncryptHub, Hacker Behind 618+ Breaches, for Disclosing Windows Flaws

Original Source: The Hacker News by Ravie Lakshmanan

In an intriguing twist, Microsoft has publicly acknowledged EncryptHub, a hacker linked to over 618 breaches, for responsibly disclosing critical vulnerabilities in Windows.

This acknowledgment highlights the complex relationship between tech giants and the hacking community.

While EncryptHub's past is marred by cybercriminal activities, this act of disclosure underscores the potential for rehabilitation and the role that ethical hacking can play in enhancing system security.

Microsoft's recognition of EncryptHub also sparks a broader discussion on the balance between condemning past actions and encouraging constructive contributions to cybersecurity.

CyberSecurity Advisors Network

NEWS:

18. WinRAR flaw bypasses Windows Mark of the Web security alerts

Original Source: BleepingComputer by Ionut Ilascu

A critical flaw in WinRAR has been identified, allowing malicious files to bypass the Windows "Mark of the Web" security warning, which typically alerts users to the risks of files downloaded from the internet.

This vulnerability exposes users to potential malware infections without the usual security prompts, highlighting a significant risk in commonly used file compression software.

The discovery prompts an urgent call for updates and heightened awareness among users to verify the authenticity of downloaded files, reinforcing the need for vigilant security practices in the face of evolving cyber threats.

CyberSecurity Advisors Network

NEWS:

19. Malicious Python Packages on PyPI Downloaded 39,000+ Times, Steal Sensitive Data

Original Source: The Hacker News by Ravie Lakshmanan

The Python Package Index (PyPI) has become the target of cyber attackers who have uploaded malicious packages that were downloaded over 39,000 times.

These packages are designed to steal sensitive data from unsuspecting developers who incorporate these tainted modules into their applications.

The incident underscores the vulnerabilities in software supply chains and highlights the need for increased vigilance and security measures in the management of open-source repositories.

Developers are urged to verify the integrity and source of the packages they use to prevent such security breaches.

CyberSecurity Advisors Network

NEWS:

20. Senators re-up bill to expand Secret Service's financial cybercrime authorities

Original Source: Cyberscoop by Matt Bracken

A renewed legislative effort seeks to enhance the U.S. Secret Service's authority in tackling financial cybercrimes.

This bill, reintroduced by senators, aims to provide the agency with expanded capabilities to pursue cybercriminals involved in financial fraud and other related activities.

By broadening the scope of the Secret Service's investigative powers, the bill addresses the growing complexity and frequency of financial cybercrimes that threaten both individual and national economic security.

The move reflects an ongoing commitment to adapting legal and enforcement frameworks to the evolving landscape of digital threats.

CyberSecurity Advisors Network

NEWS:

21. PoisonSeed phishing campaign behind emails with wallet seed phrases

Original Source: BleepingComputer by Bill Toulas

The PoisonSeed phishing campaign is at the forefront of recent cyber threats, targeting individuals with emails containing fake wallet seed phrases.

These phishing attempts are designed to steal cryptocurrency by deceiving users into revealing their wallet's private keys.

The campaign's sophistication and targeting of digital wallet users underscore the evolving nature of phishing tactics and the critical need for heightened awareness and security measures among cryptocurrency holders.

This incident serves as a stark reminder of the ongoing risks in the digital finance space.

CyberSecurity Advisors Network

NEWS:

22. Call Records of Millions Exposed by Verizon App Vulnerability

Original Source: SecurityWeek by Eduard Kovacs

A critical vulnerability in a Verizon app has led to the exposure of call records for millions of users.

This significant security lapse not only revealed sensitive personal information but also highlighted the ongoing challenges in protecting user data within large telecommunications networks.

The breach prompts urgent calls for enhanced data protection measures and regulatory oversight to prevent such incidents in the future, emphasising the need for robust security protocols in mobile and digital services to safeguard user privacy.

CyberSecurity Advisors Network

NEWS:

23. Trump fires Gen. Timothy Haugh from leadership of Cyber Command and NSA

Original Source: Cyberscoop by Mark Pomerleau

In a dramatic move, President Trump has removed General Timothy Haugh from his leadership roles at Cyber Command and the National Security Agency (NSA), sparking significant concern and debate over the impact on national security.

This unexpected decision raises questions about the continuity and effectiveness of U.S. cyber defence strategies at a critical time when cyber threats are intensifying globally.

The dismissal is part of a series of controversial personnel changes affecting key positions within the nation's security apparatus, which could potentially alter the trajectory of U.S. cybersecurity policy and its operational readiness.

CyberSecurity Advisors Network

NEWS:

24. Europcar GitLab breach exposes data of up to 200,000 customers

Original Source: BleepingComputer by Ionut Ilascu

Europcar has reported a significant data breach within their GitLab repositories, impacting up to 200,000 customers.

This breach has exposed sensitive customer data, highlighting vulnerabilities in data management practices and the challenges companies face in securing user information.

The incident has prompted a thorough review of Europcar's cybersecurity measures, emphasising the need for enhanced security protocols and continuous monitoring to protect against sophisticated cyber threats.

This breach serves as a critical reminder for the automotive rental industry to bolster their cyber defences.

CyberSecurity Advisors Network

NEWS:

25. Rafts of Security Bugs Could Rain Out Solar Grids

Original Source: Dark Reading by Kristina Beek

A new report from Dark Reading by Kristina Beek uncovers multiple security vulnerabilities within solar grid systems, which could potentially lead to widespread disruptions.

The investigation reveals that these security flaws, if exploited, could allow hackers to manipulate energy production and distribution, posing serious risks to the stability and reliability of power networks.

This discovery emphasises the critical need for the energy sector to implement stronger cybersecurity measures and conduct regular system audits to prevent potential cyberattacks that could cripple solar infrastructure.

CyberSecurity Advisors Network

NEWS:

26. SpotBugs Access Token Theft Identified as Root Cause of GitHub Supply Chain Attack

Original Source: The Hacker News by Ravie Lakshmanan

An investigative report has identified the theft of a SpotBugs access token as the root cause behind a significant GitHub supply chain attack.

This token, crucial for code scanning and vulnerability identification, was exploited by hackers to insert malicious code into numerous projects.

This incident not only disrupted operations but also sparked a reevaluation of security practices surrounding third-party integrations in software development environments.

The breach has prompted calls for tighter access controls and more rigorous security protocols to protect against similar vulnerabilities in the future.

CyberSecurity Advisors Network

NEWS:

27. State Bar of Texas Says Personal Information Stolen in Ransomware Attack

Original Source: Security Week by Ionut Arghire

The State Bar of Texas has confirmed that it suffered a ransomware attack in which personal data was stolen, affecting attorneys, employees, and possibly clients.

The compromised information may include names, contact details, and potentially sensitive legal records.

This breach underscores the growing threat posed by ransomware actors targeting professional and regulatory bodies, which often hold extensive confidential data.

In response, the organisation has begun coordinating with law enforcement and cybersecurity experts to investigate the incident, contain the damage, and implement stronger safeguards.

The attack highlights the urgent need for legal institutions to prioritise cyber resilience in their risk management strategies.

CyberSecurity Advisors Network

NEWS:

28. OPSEC Failure Exposes Coquettte's Malware Campaigns on Bulletproof Hosting Servers

Original Source: The Hacker News by Ravie Lakshmanan

A major operational security (OPSEC) lapse has exposed the infrastructure behind Coquettte, a cybercriminal group running widespread malware campaigns via bulletproof hosting services.

Researchers uncovered detailed information on the group's tools, techniques, and monetisation strategies, revealing how they weaponised cracked software and fake installers to distribute infostealers and remote access trojans.

The exposure has given cybersecurity professionals rare insight into the inner workings of these campaigns, potentially enabling more effective detection and takedown efforts. It also reinforces the risks associated with pirated software and the importance of securing hosting environments to prevent abuse by threat actors.

CyberSecurity Advisors Network

NEWS:

29. Australian super funds compromised after data breach as hackers use stolen passwords

Original Source: The Guardian by Josh Taylor

Several Australian superannuation funds have been compromised in a data breach linked to credential-stuffing attacks using stolen passwords.

The breach impacted multiple accounts and exposed sensitive personal and financial information. Although the exact scale is still being assessed, the attack has prompted urgent investigations and raised concerns about security across the superannuation sector.

Industry bodies and regulators are now emphasising the importance of multi-factor authentication and proactive monitoring to prevent unauthorised access.

This incident is part of a broader pattern of financially motivated attacks targeting institutions that manage large volumes of identity and payment data, further highlighting the risks posed by password reuse.

CyberSecurity Advisors Network

NEWS:

30. “Nudify” deepfakes stored unprotected online

Original Source: Malware Bytes by Pieter Arntz

Tens of thousands of explicit deepfake images generated using so-called "nudify" AI tools were found stored online without any protection, exposing not just the manipulated content but also user-uploaded photos and metadata.

Many of the targets appear to be women who never consented to having their images altered, raising serious ethical and legal concerns.

The unprotected storage highlights not only the predatory nature of these platforms but also their disregard for basic data security.

As deepfake tools become more accessible and sophisticated, this incident underscores the urgent need for stronger regulation, enforcement, and platform accountability to prevent image-based abuse and digital gender-based violence.

CyberSecurity Advisors Network

ANALYSIS:

31. PCI DSS 4.0.1: A Cybersecurity Blueprint by the Industry, for the Industry

Original Source: Security Week by Kevin Townsend

The latest update to the Payment Card Industry Data Security Standard (PCI DSS 4.0.1) reflects a more flexible and proactive approach to safeguarding payment data.

Developed in collaboration with industry stakeholders, the new version introduces tailored implementation options and continuous compliance expectations rather than periodic assessments.

Emphasising shared responsibility, it encourages organisations to build security into daily operations and move beyond checkbox compliance.

While some view the changes as overdue, they represent a cultural shift that prioritises risk-based thinking, adaptability, and accountability in an evolving threat landscape where financial data remains a high-value target.

CyberSecurity Advisors Network

ANALYSIS:

32. Intergenerational Mentoring: Key to Cybersecurity's AI Future

Original Source: Dark Reading by Han Cho

As AI transforms cybersecurity, intergenerational mentoring is emerging as a strategic advantage.

Pairing seasoned professionals with younger, tech-fluent practitioners bridges experience gaps and fosters innovation in rapidly evolving environments.

The piece argues that younger professionals bring fresh perspectives and native fluency in emerging tools, while older mentors provide context, risk awareness, and institutional memory. This mutual exchange strengthens workforce resilience, accelerates skill development, and enhances adaptability.

With AI redefining threat detection, response, and decision-making, cultivating intergenerational collaboration is framed not just as a workforce strategy but as a long-term security imperative.

CyberSecurity Advisors Network

ANALYSIS:

33. State-Sponsored AI Attacks: How Nations Are Using AI to Wage Digital War

The Weaponisation of AI in Cyber Warfare – Part 2

Original Source: PrivID (Substack)

State actors are rapidly integrating AI into their cyber arsenals, using it to automate reconnaissance, generate phishing content, and overwhelm defences at machine speed.

This piece explores how AI enables more precise, persistent, and adaptive attacks, reducing the need for human operators while amplifying the reach and impact of digital campaigns.

From deepfake propaganda to AI-generated zero-day exploitation, the weaponisation of AI is reframing cyber warfare as faster, stealthier, and harder to attribute.

As democracies lag in defining norms for military AI use, the article warns of a strategic imbalance where authoritarian regimes may act with fewer constraints, forcing urgent global conversations on policy and defence.

CyberSecurity Advisors Network

ANALYSIS:

34. Australia’s social media ban is attracting global praise – but we’re no closer to knowing how it would work

Original Source: The Guardian by Josh Taylor

Australia’s proposed power to ban social media platforms in times of crisis has received international attention, but key questions about enforcement and feasibility remain unanswered.

While the move is framed as a way to curb the spread of harmful content during emergencies, critics argue the law is vague, potentially unworkable, and risks overreach without strong oversight.

Concerns include how platforms would be technically blocked, the role of internet service providers, and whether such actions would meaningfully address disinformation.

The proposal reflects growing global anxiety over social media’s influence, but as it stands, it raises more questions than it answers about balancing public safety, free expression, and digital governance.

CyberSecurity Advisors Network

ANALYSIS:

35. Secure Communications Evolve Beyond End-to-End Encryption

Original Source: Dark Reading by Robert Lemos

While end-to-end encryption remains a cornerstone of secure communication, experts warn it is no longer enough on its own.

This article explores how threat actors are increasingly targeting metadata, endpoints, and peripheral systems—areas not protected by encryption alone.

Emerging strategies focus on decentralised identity, zero-trust architecture, and secure enclaves to protect data before, during, and after transmission.

As communications grow more complex, especially in hybrid and mobile work environments, security must extend beyond message content to encompass context, device integrity, and authentication layers.

The future of private communication lies in layering protections, not relying solely on encryption protocols.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

CyAN CyAN Members
Op Eds, Articles, etc

36. Protecting the Power of AI: Strategies Against Emerging Security Risks

By CyAN Member Shantanu Bhattacharya

In his RSA Conference contribution, Shantanu Bhattacharya explores the dual-edged nature of AI—its transformative potential and its susceptibility to misuse.

He outlines key strategies for safeguarding AI systems, from building resilient architectures to implementing continuous monitoring and adversarial testing.

With threat actors using AI for malicious purposes such as automated exploits and misinformation, Shantanu argues that security must be integrated at every layer of the AI lifecycle.

He also stresses the importance of transparency, ethics, and governance frameworks to ensure trust and accountability. His insights offer a practical roadmap for organisations aiming to harness AI responsibly without compromising security or public confidence.

CyAN Cybersecurity Advisors Network

CyAN CyAN Members Op Eds, Articles, etc

37. Antivirus, Firewalls, and VPNs: What Do They Actually Do?

Original Source: CyAN General Secretary Fel Gayanilo

Fel Gayanilo offers a clear, jargon-free guide to three foundational cybersecurity tools—antivirus software, firewalls, and VPNs—explaining how each functions and where their protections begin and end.

He breaks down common misconceptions, such as assuming a VPN guarantees anonymity or that antivirus alone can stop modern threats.

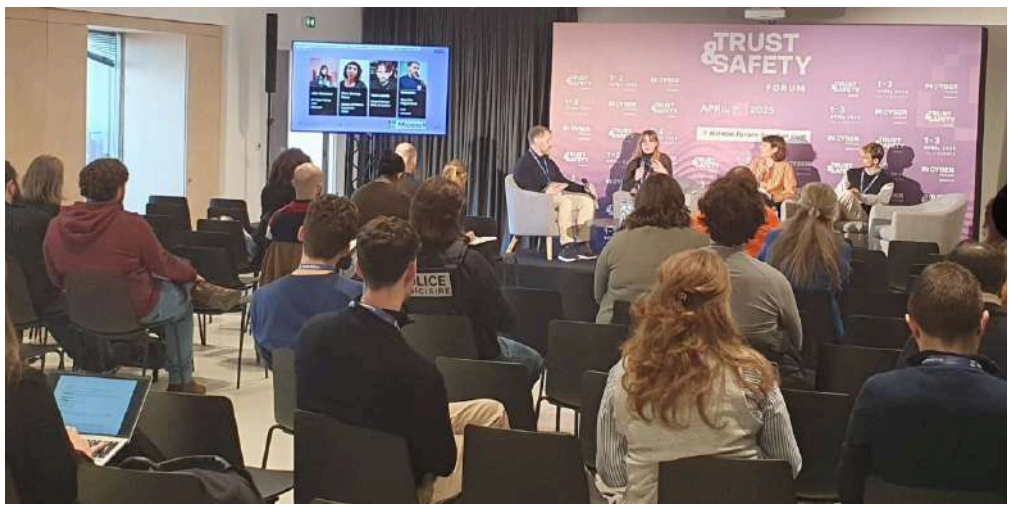
Fel emphasises the importance of layering these tools as part of a broader security strategy rather than relying on any one solution.

His approachable explanations empower individuals and small businesses alike to make informed decisions about their digital safety, while reminding readers that tools are only as strong as the habits and awareness of the people using them.

CyAN Member's News:

Trust & Safety Forum #4: A Powerful Gathering on Consent, Survivors' Voices, and Digital Resilience

The fourth edition of the Trust & Safety Forum was a resounding success, drawing over 40 speakers across 18 sessions and cementing its place as a leading event in the digital safety space.



Discussions spanned geopolitics, the defence of trusted flaggers, the importance of fact-checking to safeguard democracy, and protecting intellectual property.

Highlights included a bold, cross-sector session on consent empowerment and a powerful opening on image-based sexual violence. A standout workshop featured the voices of survivors, offering raw insight and hope while underscoring the urgency of platform accountability and policy reform. The forum continues to set the standard for collaborative, impact-driven dialogue in the trust and safety community.

We at CyAN are ALWAYS overjoyed to celebrate our members successes and their contributions to the cybersecurity community!

UPCOMING CyAN and CyAN Partner EVENTS:

- **Supply Chain Cyber Security Summit (SCCS), Lisbon Portugal: 9-11 April 2025 https://sccybersecurity.com/cyber-security-summit-europe/**
- **GITEX AFRICA, Marrakesh, Morocco: 14-16 April https://tinyurl.com/2yhuztwk**
- **GITEX ASIA, Singapore (Marina Bay Sands: 23-25 April https://gitexasia.com/**
- **GISEC Global, Dubai World Trade Centre: 6-8 May https://gisec.ae/home**
- **The Cyber Outstanding Security Performance Awards (Cyber OSPAs), London, UK: 8 May https://www.thecyberospas.com/about/**
- **CSG Awards 2025, Dubai: 7 May https://csgawards.com/**
- **World AI Technology Expo, Dubai: 14-15 May https://worldaiexpo.i**
- **CyAN 10th Anniversary Celebrations!**
- **GITEX Europe Messe, Berlin: 21-23 May https://www.gitex-europe.com/**
- **MaTeCC, Rabat, Morocco: 7-9 June https://tinyurl.com/mtecz8vw**
- **CyAN Q2 Community Call (APAC and the Gulf), June 11: 12:00 GST / 16:00 SGT / 18:00 AEST**
- **CyAN Q2 Community Call (EMEA and the Americas), June 11: 20:00 GST / 18:00 CET / 17:00 UTC / 12:00 EDT**

CyAN Cybersecurity Advisors Network

Catch up on Past Issues:

Missed an issue of (In)Securities? No worries! Scan the QR code to explore our archive of past editions—packed with insights, trends, and actionable tips to keep you ahead in the ever-evolving world of cybersecurity. Dive in and catch up today!

CyberSecurity Advisors Network

If you found this interesting, please like and share it with your friends and colleagues!

#ReallyInterestingCyberStuff!
#SharingIsCaring