NOVEMBER 2024

inside zhero

Friend Or Foe

AI and Cybersecurity

Dive Into Deepfake

Photoshopping for the 21st Century

Danger Under Our Noses

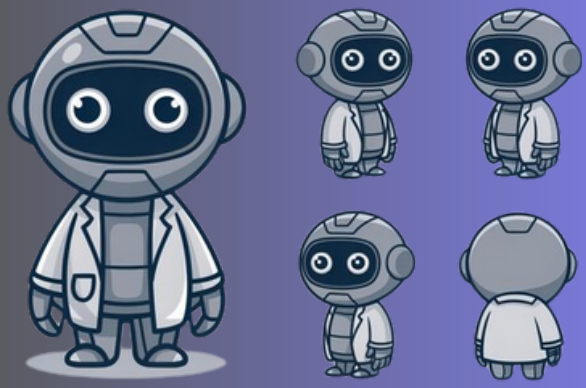
Online Safety for Kids

Message from Izak

I hope you are all well and welcome to this bumper edition of Inside Zhero.

This month, we showcase AI and cybersecurity – the good, the bad and the ugly. Our amazing Compliance Consultant and Cyber London Community Manager, Lucindi, also offers expert advice on online safety for kids.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author



In this issue

Our feature “Friend Or Foe” delves deep into the world of AI and cybersecurity, exploring security positives and cyber threats.

The market for AI-driven cybersecurity will be £46.3 billion by 2027.

"I make security a priority in every area - from data protection to AI model security, and especially identity protection. If identity is compromised, other defences won't hold up. I embrace automation in our security operations and keep adding new layers of defence to stay a step ahead of cyber attackers, building resilience against ever-evolving threats."

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consulation

90% discount **cyberzhero542**

FRIEND OR **FOE**

AI is shaking up cybersecurity, and it's a double-edged sword. On the bright side, AI is becoming a super-tool for cyber defenders, having a transformative effect on threat detection, demonstrating its capabilities in real-time threat identification, behavioural analytics, machine learning for endpoint security, adaptive defence mechanisms, and predictive analytics. But cybercriminals have also invited AI to their party. They're using it enhance attacks, automate malware creation, enable impersonation, poison data sets, and facilitate unauthorised access to sensitive information. AI and cybersecurity is a high-stakes game of cat and mouse. According to recent research from BlackBerry, 82% of IT decision-makers are gearing up to invest in AI-based defences in the next two years, as the AI-powered threat landscape keeps growing. The market for AI-driven cybersecurity is on track to hit a whopping £46.3 billion by 2027. So, what does this mean for businesses, especially smaller ones? How can they get ready for this new AI-driven world? And with the EU AI Act and other global rules coming in, how can SMEs make sure they're on the right side of these regulations?

Cybersecurity benefits

Here's how AI is transforming cybersecurity today:

- **Real-time detection:** Unlike traditional methods that rely on fixed rules, AI can detect potential threats as they happen, continuously analysing huge volumes of data to spot anomalies. This real-time edge means cybercriminals are detected and stopped faster than ever.
- **Behavioural analytics:** AI establishes a "normal" baseline of activity for users and systems, flagging any unusual behaviour—such as unexpected logins or data spikes—that might signal a threat. This adaptability makes AI-driven systems more effective at catching subtle, suspicious changes.
- **Enhanced endpoint security:** AI's machine learning models strengthen device security by recognising malware patterns and catching unknown threats, including zero-day attacks. This is essential as cybercriminals frequently target endpoints as an easy entry point into networks.
- **Adaptive defences:** AI-based systems don't just rely on static rules; they learn from new data and adapt to evolving threats. This flexibility allows AI to adjust its defences dynamically as new vulnerabilities and tactics emerge.
- **Predictive analysis:** By examining historical data and trends, AI can anticipate and predict future threats, allowing organisations to proactively bolster defences before incidents occur.
- **Reducing false alarms:** AI reduces false positives by learning from its environment, helping security teams focus on genuine threats and work more efficiently.

AI is proving itself a game-changer in cybersecurity, offering defences that are faster, smarter, and more adaptive.

Cybersecurity threats

On the flip side, while AI is advancing cyber threat detection and defence, it's also giving cybercriminals powerful new tools for malicious purposes, ramping up security threats in alarming ways:

- **Optimising cyberattacks:** Cybercriminals are using AI to supercharge their attacks, analysing vast datasets to pinpoint system vulnerabilities. With automated penetration testing, AI can probe networks to identify the easiest entry points for exploitation.
- **Automating malware:** AI accelerates malware creation, generating variants that can dodge traditional detection. Machine learning tailors malware to specific environments, pushing defenders to constantly update their security systems.
- **Enhancing impersonation:** Cybercriminals exploit AI's ability to mimic human behaviour, creating phishing emails and social engineering attacks that are eerily convincing by analysing and replicating real communication styles.
- **Poisoning data sets:** Attackers can corrupt the datasets used to train AI models, weakening defences or creating exploitable biases. This "poisoned" data leads to detection models that miss specific threats or become easier to manipulate.
- **Targeting sensitive data:** Using AI to study user patterns and security protocols, cybercriminals can exploit weaknesses with precision, executing attacks like credential stuffing or password guessing with higher accuracy.

As AI becomes more sophisticated, so too do the tactics of cybercriminals—posing a constant challenge for security teams to stay ahead of these evolving threats.

Investment in AI

We cannot ignore the role AI has to play in cybersecurity and investment therein. While board members and CISOs may toss and turn at night contemplating the optimal investment level in AI, the fact remains that against the backdrop of rapid technological advancements and ever-evolving threats, investments need to be made.

Professor Raj Rajarajan, a cybersecurity leader, Zhero Head of R&D, and a director at Cyber London says:

"For companies, the core technology focus areas for investment should be around defensive AI, identity management and automation of threat intelligence."

Raj's words are accentuated by the findings of a 2024 report by CNBC. 60% of companies regard generative AI as critical to their business operations, making it the largest technology spending priority for 44% of organisations in the coming year. This underscores the growing significance of AI, particularly within cybersecurity budgets, and highlights the need for strategic investment in areas with the potential for the greatest impact. It also emphasises the importance of tracking the returns on these investments.

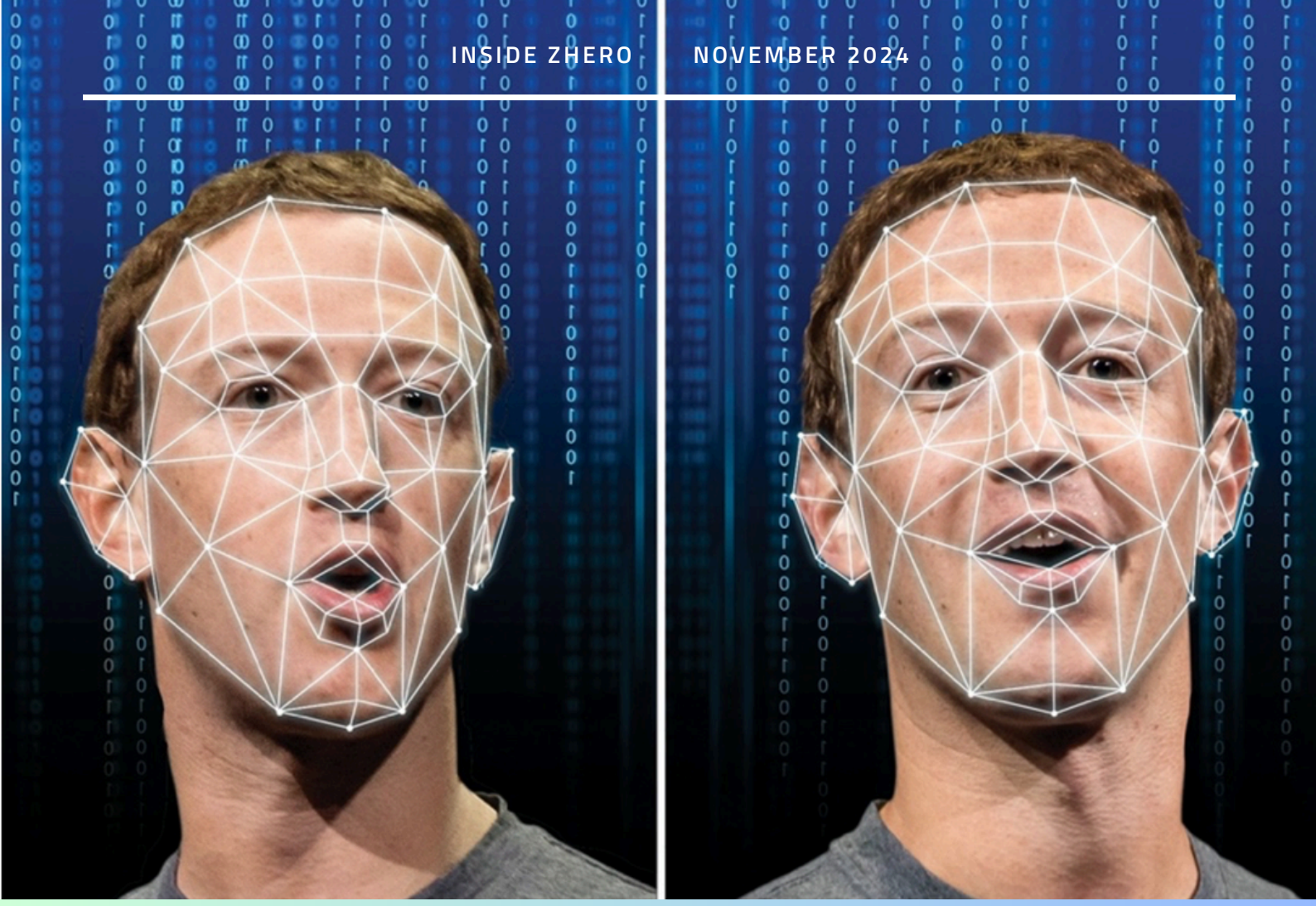
AI bubble

According to Statista, the global AI market is predicted to exceed $800 billion by 2030. To put this in context, AI could easily be worth more than the GDP of Sweden, Ireland or Singapore, and three times the GDP of smaller economies such as Greece and New Zealand. But will AI become another underwhelming hype like the Dotcom businesses, RSS feeds and 3D Printing of years gone by?

John Naughton, a Professor at the Open University, outlined the five stages of financial bubbles, suggesting that AI currently sits between stages three and four: euphoria and profit-taking. Despite tech giants like Microsoft and Google continuing to invest heavily to sustain the hype, wise investors are recognising the signs and preparing to exit to avoid significant losses. American chip giant Nvidia lost 10% on the Nasdaq, wiping $300 billion off its stock market valuation. The reason? Investors are no longer enamoured by the boom in AI. Back to Naughton's fifth stage – panic. Is that where we are headed? The big sellout?

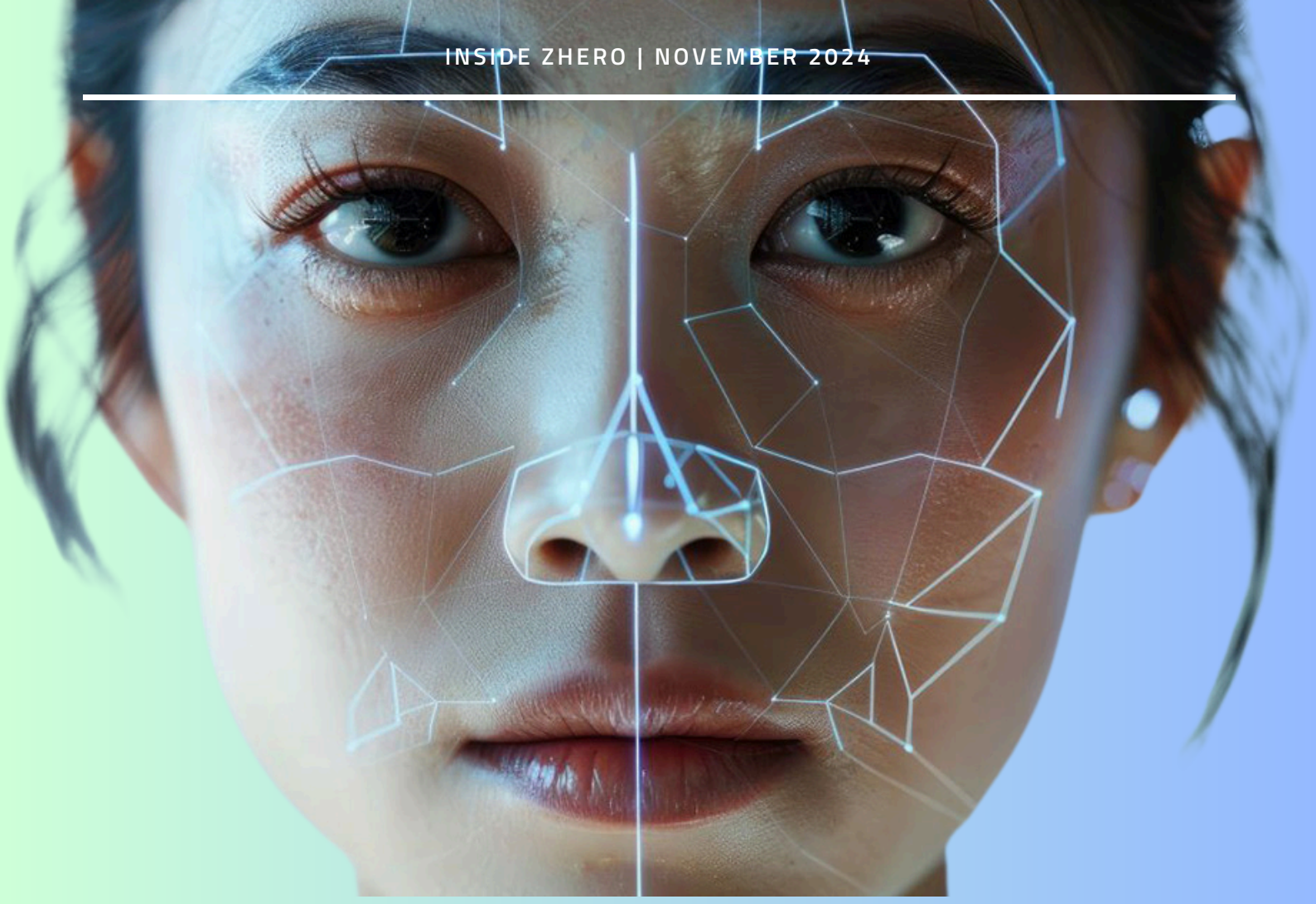
Professor Naughton says:

"It could be that governments eventually tire of having uncontrollable corporate behemoths running loose with investors' money. Or that shareholders come to the same conclusion. Nothing grows exponentially forever. So, going back to that original question: are we caught in an AI bubble? Is the Pope a Catholic?"



DIVE INTO DEEPFAKE

Have you ever seen Mark Zuckerberg boast about having “complete control over billions of people’s stolen data” or witnessed Jon Snow’s heartfelt apology for the disappointing conclusion to Game of Thrones? If so, you’ve encountered a deepfake. The 21st century’s answer to Photoshopping, deepfakes use a type of artificial intelligence known as deep learning to create images of fabricated events, hence the name "deepfake". Want to put new words in a politician’s mouth, star in your favourite film, or dance like a professional? Then it’s time to create a deepfake.

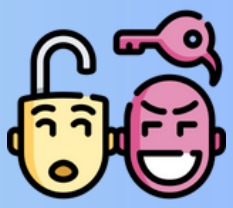


How deepfakes work

Deepfakes rely on neural networks that analyse large sets of data to learn how to imitate a person's facial expressions, mannerisms, voice, and inflexions. The process involves inputting footage of two individuals into a deep-learning algorithm to train it to swap faces. In other words, deepfakes use facial mapping technology and AI to replace one person's face in a video with that of another. Deepfakes are difficult to detect, as they use real footage, often include realistic-sounding audio, and are designed to spread rapidly on social media. Many of us think what we are watching is authentic.

Deepfakes uses

- **Impersonating public figures:** Deepfakes have been used to create fake videos of politicians, celebrities, and business leaders, fuelling misinformation and reputational harm. Kendrick Lamar's video The Heart Part 5, for example, uses a deepfake to morph his face into that of Kobe Bryant. A 2018 deepfake by BuzzFeed showed President Obama speaking in a fabricated video, quickly raising ethical alarms about disinformation risks.·
- **Business fraud:** Fraudsters manipulate deepfake audio and video to scam employees or customers, gaining unauthorised access to funds. In one case, a bank manager authorised $35 million in wire transfers due to AI voice-cloning, while in another, an AI hologram impersonated a company COO, causing a major loss.
- **Identity theft:** Cybercriminals use deepfakes to bypass identity checks, enabling them to impersonate others, access restricted data, or commit financial fraud.
- **Social engineering:** Deepfake personas are used to trick people into sharing sensitive information or making risky decisions. In 2023, a deepfake of finance influencer Martin Lewis promoted a fake investment app, while in 2021, a cybercriminal used a deepfake of Dubai Crown Prince Sheikh Hamdan to solicit money. These cases highlight the urgent need for better detection tools to fight deepfake-driven fraud.



Elon Musk scam

In August, all Steve Beauchamp wanted was some money for his family, and he believed Elon Musk could help. Beauchamp, an 82-year-old retiree, had seen a video late last year featuring Musk endorsing a radical investment opportunity that promised quick returns. He got in touch with the company behind the scheme and opened an account with $248. Over several weeks and multiple transactions, Beauchamp drained his retirement savings, ultimately investing more than $690,000. Then, the money disappeared – lost to digital scammers operating at the cutting edge of a new wave of crime fuelled by artificial intelligence. The scammers had taken a genuine interview with Musk and manipulated it, using AI tools to replace his voice with a replica. The AI was so advanced that it could subtly adjust Musk's mouth movements to match the new script they had written for the fake video. To a casual viewer, the deception would have been almost impossible to detect.

Deepfake infamy timeline

- **August, April 2018 - Obama Deepfake Video** – video of former US President Barack Obama raises mainstream awareness.

- **April 2019 – David Beckham Deepfake Video** - Malaria survivors speaking through David Beckham to help raise awareness around the Malaria Must Die initiative spooked a lot of people.

- **December 2020 - Deepfake Queen Alternative Christmas Message** - an alternative Christmas message for a very alternative year.

- **July 2021 - This is not Morgan Freeman** - Freeman condemned the AI-generated narration using his voice.

- **Donald Trump Deepfakes** - Deepfake image shows President Trump kissing top US scientist Anthony Fauci.

Click an image to see the deepfake

Spotting a deepfake

- **Odd colouration** - Watch for inconsistent lighting or strange skin tones.
- **Strange eye movements** - Check if the eyes blink unnaturally or not at all.
- **Awkward facial expressions** - See if the face and emotions match the conversation.
- **Unnatural teeth/hair** - AI struggles with teeth details and perfect hair with no flyways.
- **Inconsistent audio** - Look for mismatched mouth movements or odd background noises.
- **Blurry alignment** - Watch for edges that are out of focus or frames that seem misaligned.

Deepfakes and cybersecurity

In the field of cybersecurity, deepfakes have been utilised in various deceptive practices, particularly as a means to advance social engineering attacks like spear-phishing. A common tactic involves creating video or audio clips that mimic corporate executives or public figures. Another approach sees voice deepfakes used to authenticate fraudulent requests over the phone, deceiving employees into divulging sensitive information or making unauthorised transfers. Instances of fraud involving deepfakes have surged by 3,000% over the past year, especially in the financial sector. In one recent case, deepfakes were employed to simultaneously impersonate a CFO and other executives from a multinational company during a conference call, tricking a finance employee into transferring over $25.6 million.

zhero

Danger under our noses

Lucindi Storme is Zhero's Compliance Consultant and also works at Cyber London as their Community Manager. Here's her advice for parents on how to keep their children safe and secure online.

Let's be honest—parenting in the digital age is a whole different game. Gone are the days when all we had to say was, "Don't talk to strangers" and hope for the best. Now, it's more like, "Don't click that link, don't trust everything an influencer says, and no, that's definitely not really Tom Holland inviting you to join his private fan club!" And don't even get me started on ride-sharing apps. When I was a kid, the rule was never to get into a car with a stranger; now, there' are apps on our phones giving us access to one, 24/7. Today's digital world is a complex jungle of new dangers that our wildest 90s imaginations could never have dreamed up—and our kids are the ones navigating it.

When it comes to digital dangers, cyberbullying is at the top of the list. Unlike traditional bullying, cyberbullying doesn't have a "pause" button. It can happen anywhere, anytime—whether through social media, group chats, or online games. The hurt from a mean comment or rumour posted online can feel relentless, especially when it's accessible 24/7. For kids, this can feel overwhelming, and often, they may be too embarrassed or afraid to reach out for help.

zhero

Support is strength

Cyberbullying comes in many forms. It might look like exclusion from a group chat, someone posting unkind memes, or even spreading false rumours online. And since it's digital, the audience can be much larger, and the impact can feel far-reaching and lasting. For some kids, it can feel like there's nowhere to hide, making them feel cornered in their own digital world.

So how can we help them? First, it's essential to create a safe space where kids know they can come to us without fear of judgment. Encourage open conversations by sharing your own school experiences—if they know you've faced challenges too, they're more likely to open up about theirs. Next, teach them to use digital defence tools. Show them how to block bullies, report harmful content, and adjust their privacy settings to control who can reach them. Many apps also offer reporting features to help deal with harmful behaviour. Explain that these tools aren't about "snitching"; they're there to protect their mental health and give them control. And remind them that a bully's actions often say more about the bully than the person being targeted.

It's important our kids understand that they should never feel they have to "just put up with" or ignore harmful behaviour. They deserve to feel safe and respected in their online spaces, just as they do anywhere else. If cyberbullying escalates or becomes overwhelming, seeking professional help is not only okay—it's essential. Sadly, there are numerous reports linking cyberbullying to serious consequences, including teen suicides.

Let's remind our kids that reaching out for support is a sign of strength, and there are people who genuinely want to help them through tough times.

On 12 November, Cyber London hosted three visitors from Virginia Beach Economic Development, Paige Fox, Amanda Jarratt and Charles Macdowell. Virginia Beach is a fast-emerging cyber cluster with numerous companies, R&D and academic assets employing over 7,000 people. The meeting was held at Zhero's HQ in London, attended by two Cyber London directors, Izak and Mark Child. The event promises to foster international collaboration in cybersecurity and business development. Afterwards, Charles posted on LinkedIn: "This could be the beginning of a beautiful friendship"

MacPartland powerup

On the heels of the Virginia Beach meetup, Izak had the immense pleasure of hosting an hour-long face-to-face with a cyber expert and former UK Minister of State for Security, The Rt Hon Stephen McPartland. The pair were engrossed in discussing the future of cybersecurity in the UK and how SMEs can better defend themselves. They also juxtaposed the different security approaches used by micro-businesses, SMEs and enterprise-scale operations. Most recently, Stephen was asked by the government to conduct an independent Review into Cyber Security as an enabler of Economic Growth. He is also a strategic consultant and non-executive specialist in risk, governance, cyber security and digital sustainability.

On 13 November, Izak was all aboard the HMS Belfast at the VerseOne Group NHS Customer Day on the Thames in London. In his keynote presentation, Izak showcased the future challenges of cybersecurity in the NHS and helped everybody understand essential tips and strategies needed to keep their organisations compliant and secure. In a nutshell, this means applying basic cybersecurity practices and adhering to them.

NHS

Three issues make the NHS vulnerable to cyberattacks and security breaches:

- Hardware and software they use are outdated or are EOL.
- Devices and applications across departments do not speak to each other, making processes inefficient and increasing vulnerability.
- Use of unvetted third-party providers/suppliers in the supply chain.

CRUSH IT CHAOS

Tune in here:

zhero | PODCAST

Meet the team

Vivekananda Govender

SERVICE DESK ENGINEER

Hi Viv! What made you realise you want to go into the IT industry?

My choice of choosing the IT industry was one of the main goals that I had hoped to be apart of. As a passion, I enjoyed learning about new technology being released and how it improves our daily lives.

What's your most-used productivity tool?

Microsoft Teams is one of my favourite and most used productivity tools because it allows me access to converse with others and produce service excellence.

How would you describe yourself?

I would describe myself as a Philomath. I enjoy new experiences and always being open to different perspectives about the nature of IT.

What do you enjoy the most about your role?

My favorite aspect about my job role is being able to make others happy by ensuring their problems are resolved and being able to learn something new every day.

Do you have any hidden talents or hobbies?

I enjoy reading and travelling to new destinations.

What is your favourite movie or TV show?

Big Bang Theory is one of my favourite series -Sheldon's role, specifically.

LONDON

162 Farringdon Road
London
EC1R 3AS

SPEAK TO US

+44 20 7183 3975

START THE PROCESS

zhero
crush the chaos