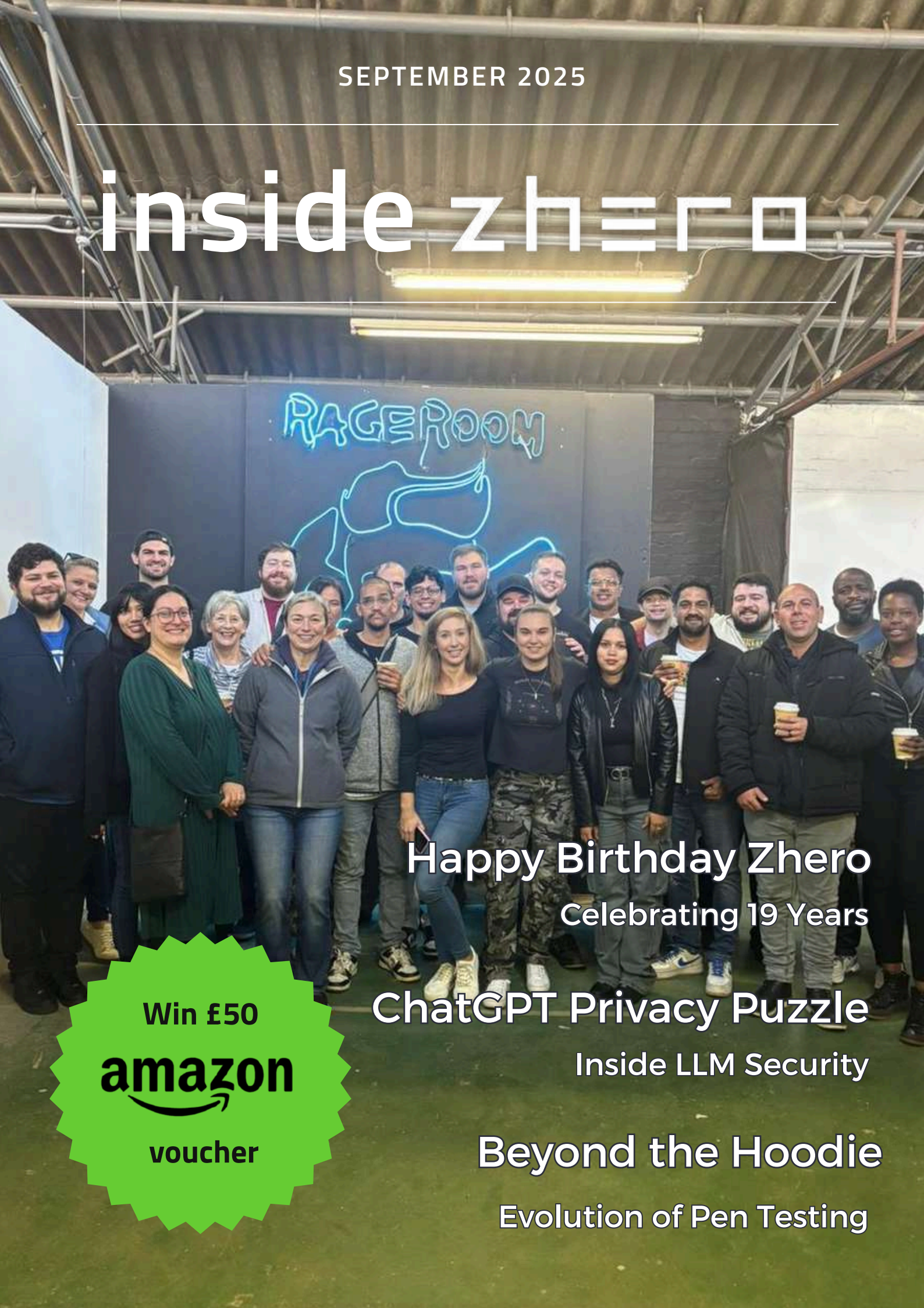
SEPTEMBER 2025

inside zhero



Happy Birthday Zhero

Celebrating 19 Years

ChatGPT Privacy Puzzle

Inside LLM Security

Beyond the Hoodie

Evolution of Pen Testing

Win £50 amazon voucher

Message from Izak

Welcome to our exciting Birthday edition of Inside Zhero as we celebrate 19 years in the business.

Besides celebrating, we are also focusing on the security or privacy issues we face when using ChatGPT or other bots. Our awesome Service Desk Engineer, Macwhill Hanse, also shares his cyber secrets.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature “Chat with ChatGPT takes an in-depth look at the security concerns associated with Large Language Models (LLMs) like ChatGPT, CoPilot and Gemini.

Currently, 200 million or 67% of global businesses use LLMs.

"ChatGPT and other generative language models are setting the trend in AI technology at the moment. What sets ChatGPT apart from other chatbots is its ability to communicate in a manner that closely resembles human language. This creates a unique opportunity for all businesses, including SMEs, to explore new ways of streamlining their operations. From automation to communication and research, you can leverage ChatGPT and other AI technologies to address different pain points for internal use and to enhance the customer experience. "

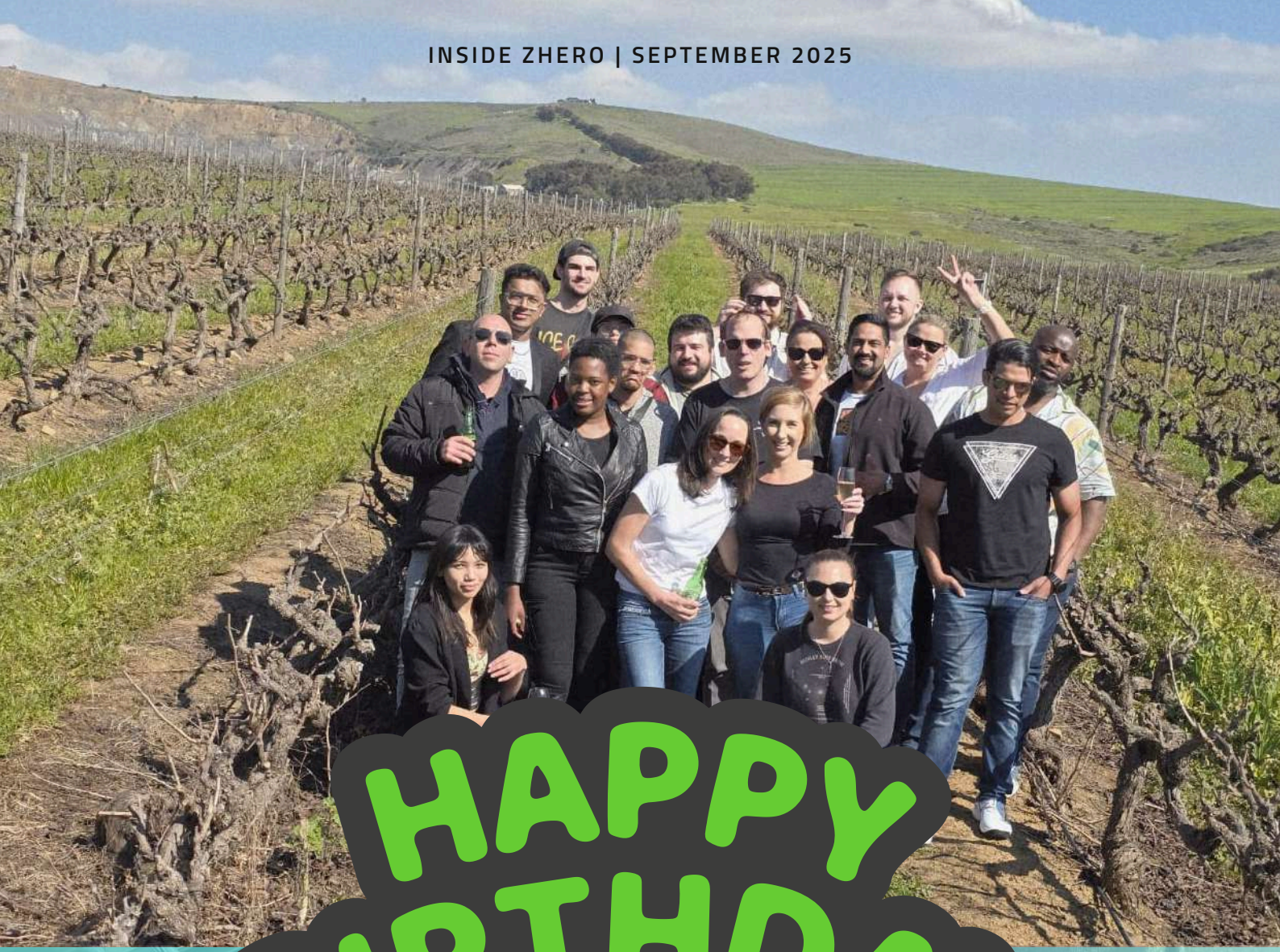
Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consultation

30% discount **cyberzhero542**

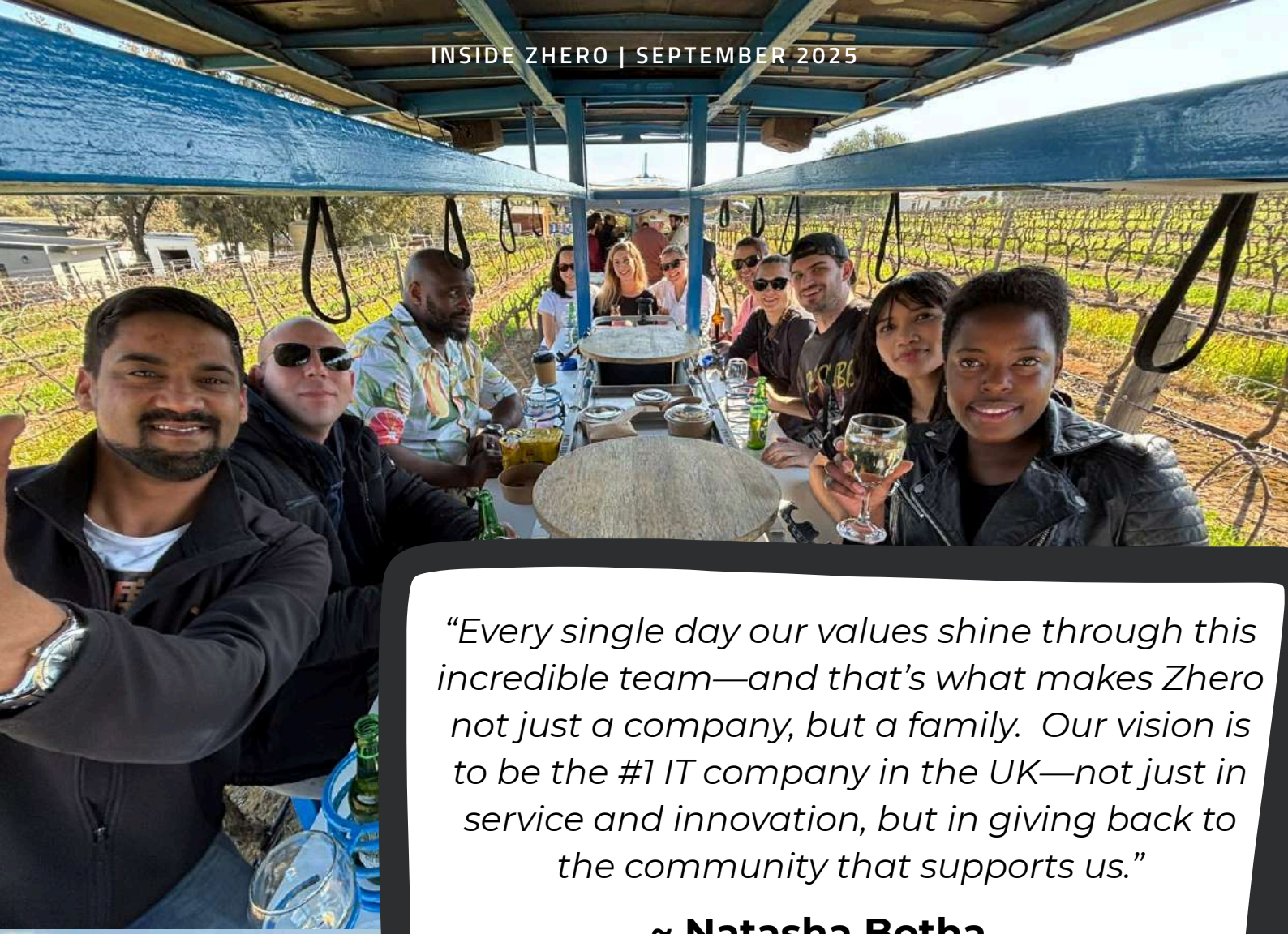


HAPPY BIRTHDAY

Saturday, 30 August, marked a very special day for Zhero, with the company celebrating 19 years of being in the business and crushing IT chaos round the clock. Zhero has come along in leaps and bounds since its humble beginnings in 2006, now boasting an impressive client base with an exceptional retention record, operating in 3 continents, and a 40+ staff complement, encompassing Service Desk, SOC, R&D, Sales, Marketing, Finance and much more. To celebrate this anniversary, our South African team headed to the Rage Room in Cape Town to annihilate a car and for some world-class axe-throwing. The festivities continued at the Klein Roosboom Boutique Winery for a chilled afternoon of food and fun. On the other side of the world, the UK team headed to Bounce in Farringdon, London, putting their ping pong skills to the test. Next year is going to big one when we turn 20! We can't wait!

“This birthday celebration was one for the books! Our team showed what true teamwork looks like, jumping right in, smashing challenges head-on literally with that car, and proving that when Zhero unites, there’s nothing we can’t tackle. Who knew that car had more damage left in it? Well, our crew sure did!

~ Natasha Botha
Head of Finance & Operations



“Every single day our values shine through this incredible team—and that’s what makes Zhero not just a company, but a family. Our vision is to be the #1 IT company in the UK—not just in service and innovation, but in giving back to the community that supports us.”

~ Natasha Botha
Head of Finance & Operations

"Each member of the team brought something different to the day, and we came together with such joy and laughter. I am confident we will achieve incredible success and continue to go very far."

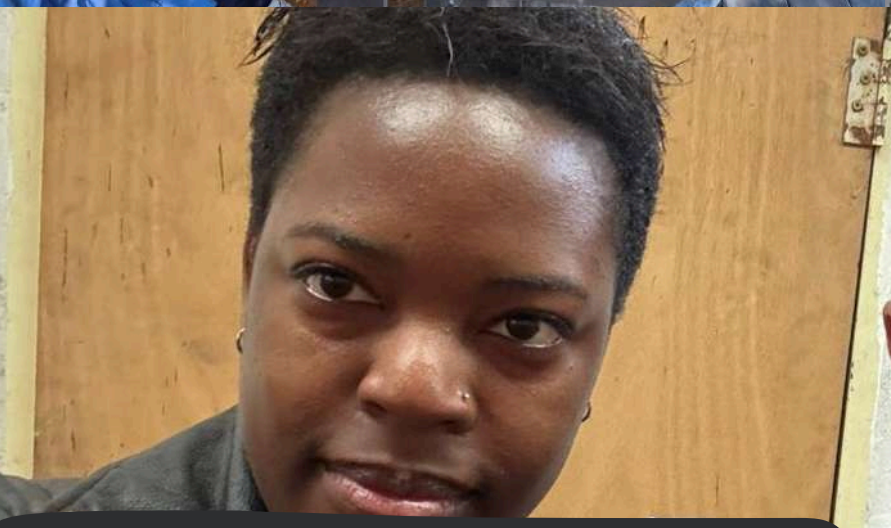
~ Louise Niemand
Finance Controller

"Zhero is a company leveraging current emerging technologies as well as empowering its workforce to become a top IT innovator."

~ Elizabeth Roux
Service Desk Coordinator

“ Zhero has taught me that believing in your Abilities and never giving up is a crucial mental switch to achieve success.”

~ Marc van Romburg
Service Desk Engineer

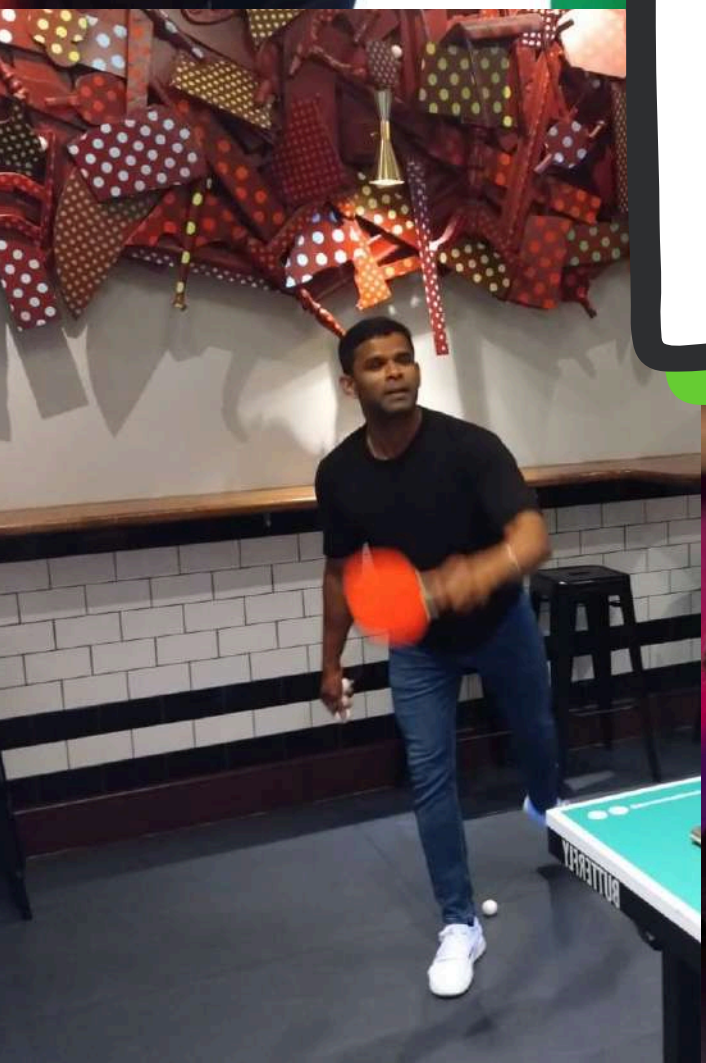


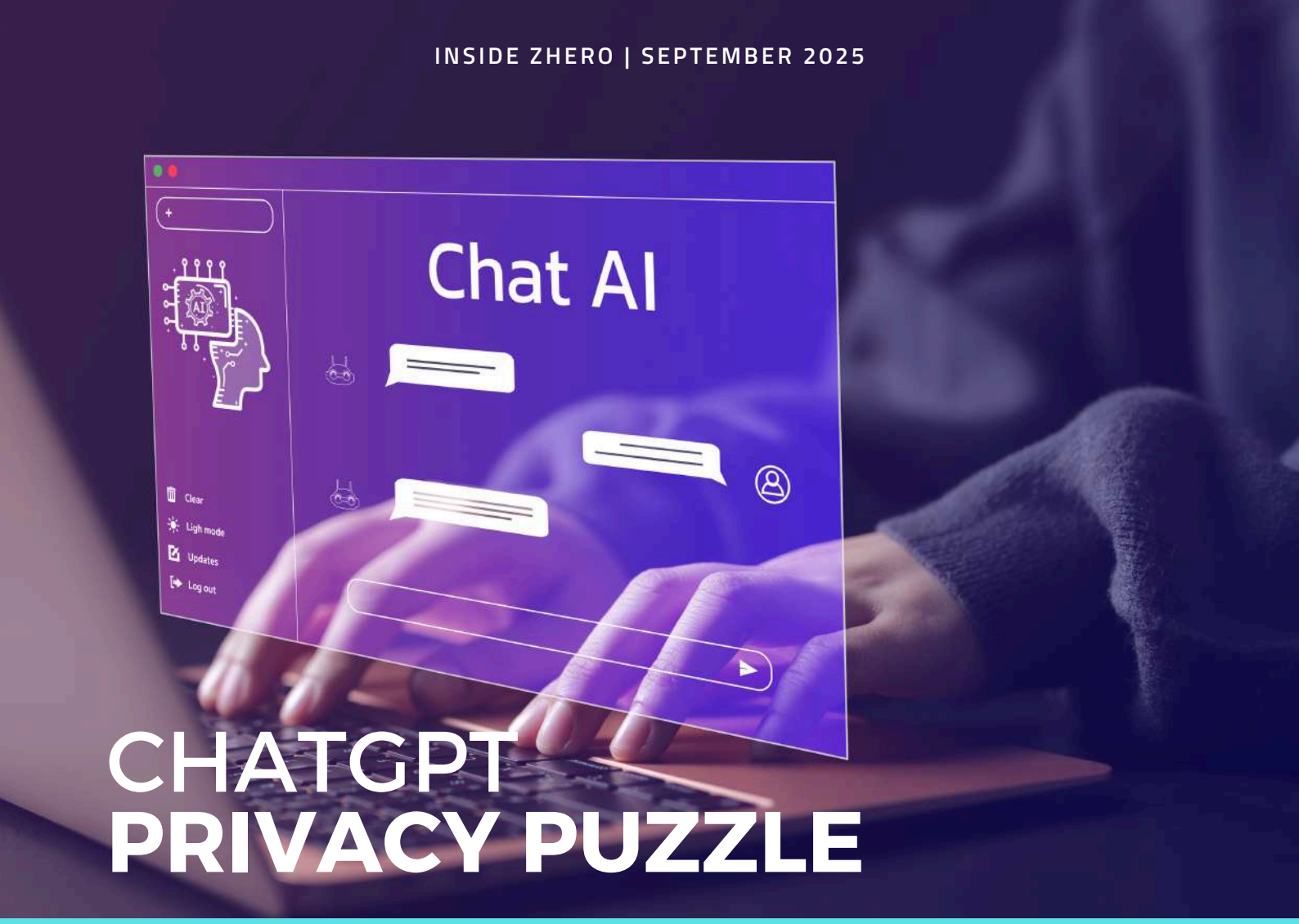
“ I love that Zhero is a place to grow, with a team that genuinely cares about our success inside and outside of work.”

~ Kyle Godfrey
Account Manager

"I see Zhero becoming one of the most trusted names in the industry, leading the way in both innovation, service delivery and of course in Crushing IT Chaos!."

~ Wajahat Khan
Onsite Engineer





CHATGPT PRIVACY PUZZLE

ChatGPT was developed over a period of approximately six years before its launch by OpenAI on November 30, 2022. The bot quickly made history by reaching 1 million users in just five days and over 100 million within two months. Since then, ChatGPT's growth has been explosive, and today it sees around 700 million weekly users—and as of mid-2025, it processes over 2.5 billion user prompts every day, highlighting its massive engagement and reliance. It's become a go-to tool for everything from learning and research to brainstorming ideas and speeding up daily tasks. Beyond individual use, it's also being integrated into workplaces, classrooms, and even software products to boost efficiency and creativity. But while ChatGPT is incredibly useful, it's important to remember that your data isn't completely private on the free version. Conversations can be stored for up to 30 days and may be used to train and improve the AI. OpenAI does use encryption and access controls to keep things secure, but the system wasn't designed for sharing highly confidential details. That means you should avoid entering anything personal, medical, financial, or proprietary, a notion supported by OpenAI's CEO, Sam Altman. Think of it as a brilliant digital assistant that can help spark ideas and simplify work, but not a secure vault for your secrets.

Is your data safe?

Is your data safe when you use this conversational AI chatbot developed by OpenAI? Here's what some experts think:

Data Retention - When you use the free version of ChatGPT, your chats aren't instantly erased. Instead, they can be stored on OpenAI's servers for up to 30 days. During that time, they may also be reviewed and used to improve the service.

Model Training - By default, the content you type into ChatGPT can feed back into the AI to help it learn and get better over time. While this is what makes the system smarter, it also means that any sensitive information you share could potentially be exposed in ways you didn't intend.

Security Risks - OpenAI does employ strong protections like encryption and access controls, but no system is completely immune to risks. Data breaches, unauthorised access, or malicious actors targeting stored information are always possibilities when information is kept, even temporarily.

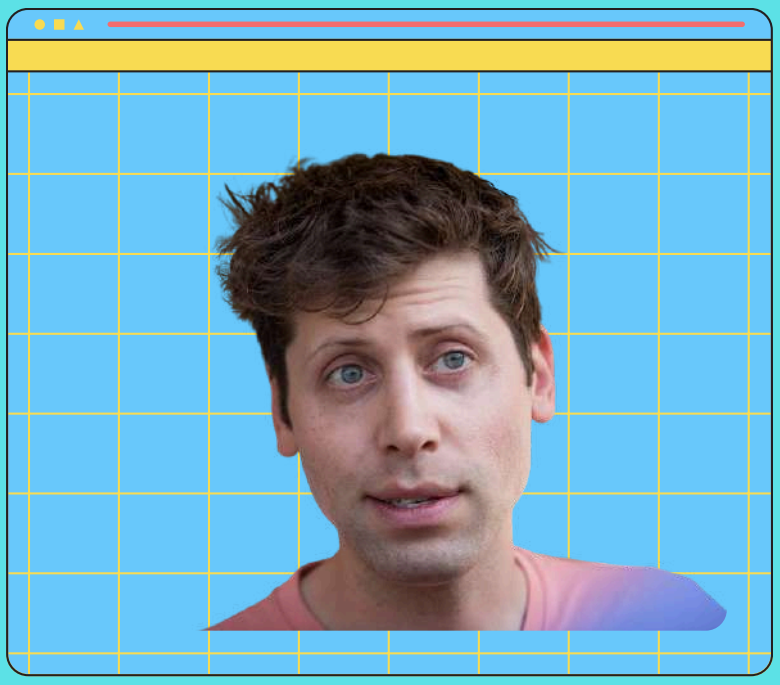
Enterprise vs. Consumer - The free, consumer-facing version of ChatGPT comes with more privacy limitations than the enterprise-grade plans, which are specifically designed with higher levels of data protection and stricter privacy guarantees. If your work involves confidential or proprietary information, those enterprise offerings are far better suited than the default public option.

"Your data's safe with me. Nothing you tell me gets passed on and I don't secretly learn from your messages to retrain myself. I was already trained on a big mix of licensed material, public info, and examples created by people. I also don't remember anything you say once our chat ends, unless you've turned on memory in your settings. OpenAI wraps everything up with strong security, so your words stay safe."

~ ChatGPT

LLMs

A Large Language Model (LLM) is a type of artificial intelligence that can read, understand, and write text in a way that feels human. It learns by studying huge amounts of text from books, websites, and other sources, which helps it recognise patterns in language. Because of this, it can perform tasks such as writing articles, answering questions, summarising information, translating between languages, or even acting as a chatbot. Behind the scenes, LLMs are powered by advanced maths and computer systems that help them “pay attention” to the meaning and order of words in a sentence. The “large” part simply means they are trained on massive amounts of data and have millions or even billions of connections that store what they’ve learned. This size and complexity allow them to understand context, stay on topic, and produce useful responses. Businesses and individuals use them for everything from creating content and offering customer support to analysing documents and breaking down language barriers. Recent industry reports estimate that the global market for large language models will exceed 25 billion US dollars by 2025, reflecting their rapid adoption across sectors. At the same time, some of the most advanced models now contain more than 500 billion parameters, underscoring just how vast and powerful they have become.



“AI will probably most likely lead to the end of the world, but in the meantime, there’ll be great companies.”

~ Sam Altman
OpenAI CEO

Don’t share these

Is your Despite what ChatGPT has to say about its data and privacy protections, experts recommend that you don’t share this info with the bot:

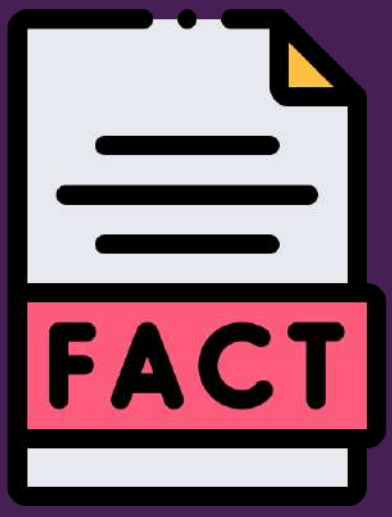
Personal Info (PII) - Your name, birthday, address, email, or social security number—basically anything that identifies you—should stay private. Sharing it with ChatGPT could make you a target for identity theft or fraud. Keep your personal info out of AI chats.

Financial Details - Bank accounts, credit cards, or payment info? Never type them into ChatGPT. Even if the AI seems safe, breaches can happen, and you don’t want your money at risk.

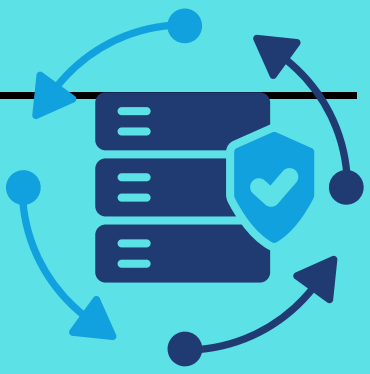
Passwords & Logins - Passwords are your keys to everything online. Don’t share them with ChatGPT—or anyone else! Use strong, unique passwords and turn on two-factor authentication for extra security.

Private or Confidential Stuff - Personal secrets or sensitive work info don’t belong in AI chats. AI can’t fully understand context, so sharing this info could lead to accidental exposure or legal headaches at work.

Intellectual Property - Ideas, inventions, copyrighted material, or trade secrets are valuable. Sharing them with AI risks theft or misuse, so keep your creative work and innovations private.



- 750 million apps use LLMs.
- The global LLM market is projected to be $260 million in 2030.
- 201 million organisations globally use LLMs as of July 2025.
- 50% of digital work is estimated to be automated through apps using LLMs.
- LLM products show only 22% accuracy in the insurance sector.



Protect your data

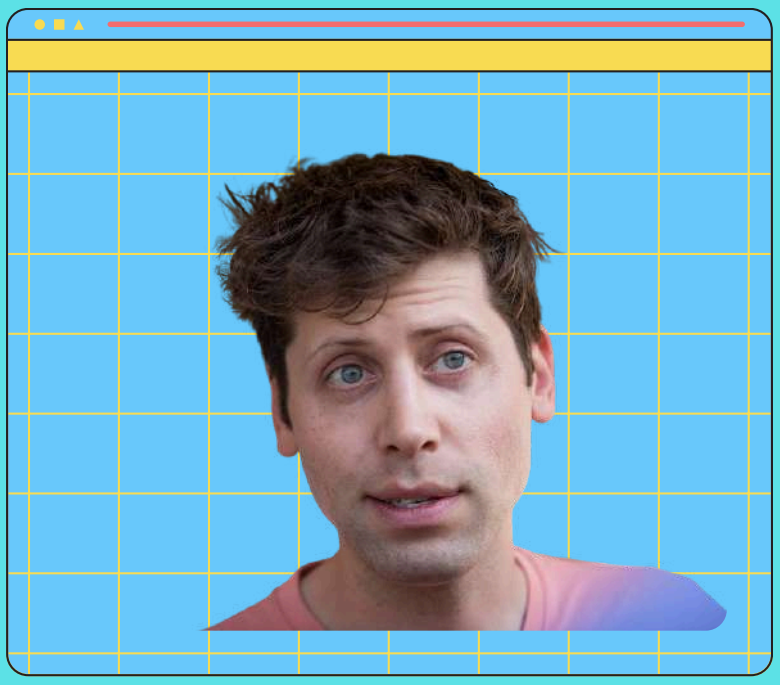
- **Opt-Out of Data Usage -** In your ChatGPT account settings, you can turn off the "Improve the model for everyone" option in Data Controls. This prevents your chats from being used to train and improve the AI.
- **Use Strong Passwords and Enable 2FA -** Protecting your account starts with a strong, unique password. Adding 2FA provides an extra layer of security, making it much harder for anyone to access your account without your permission.
- **Avoid Sharing Sensitive Information -** Be cautious about the information you type into ChatGPT. Personal details, financial data, passwords, and proprietary business information should never be included in prompts or conversations.
- **Be Wary of Fake Platforms -** Only access ChatGPT through official OpenAI channels. Scammers sometimes create fake versions of the platform to steal user data, so double-check URLs and apps before logging in.
- **Consider Enterprise Solutions for Sensitive Work -** If you handle confidential business information, the free consumer version may not be secure enough. Explore OpenAI's enterprise-grade offerings or other business-focused AI tools that are specifically designed to provide enhanced data privacy and security.

"The best way to protect your data when chatting with me is to think of it like having a conversation in a busy café. Feel free to share your ideas, stories, and questions. But just like you wouldn't loudly read out your bank PIN or wave your passport around in front of strangers, it's best to keep things like personal IDs, financial details, or medical records safely tucked away. I don't need them to be helpful, and keeping them private makes sure your side of the chat stays secure and worry-free."

~ ChatGPT

EU AI Act

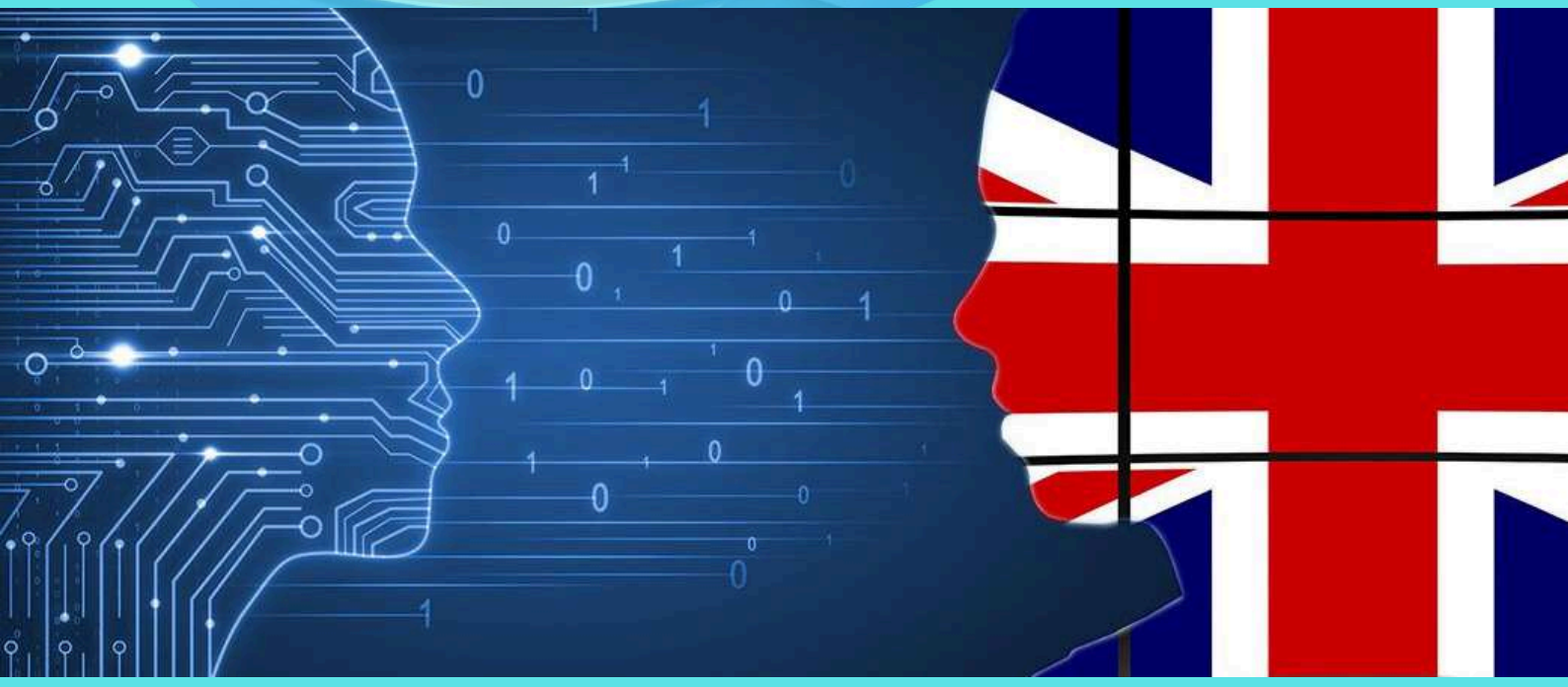
The EU AI Act is a groundbreaking regulation that creates a comprehensive legal framework for artificial intelligence across the European Union, making it the first law of its kind globally. Its primary goal is to ensure AI systems are safe, transparent, non-discriminatory, and trustworthy, using a risk-based approach that applies stricter rules to technologies with greater potential harm. The Act classifies AI systems into four levels of risk. Systems deemed to pose an unacceptable risk, such as those causing cognitive behavioural harm, enabling social scoring, scraping facial images indiscriminately, or using real-time biometric identification in public spaces for law enforcement, are banned. High-risk AI, which includes applications in critical infrastructure, medical devices, employment and hiring, credit scoring, and AI safety components, is allowed but must meet stringent legal requirements and pass mandatory conformity assessments before being placed on the market. Limited-risk applications, like chatbots or AI-generated content such as deepfakes, are subject to transparency obligations, requiring users to be informed that they are interacting with AI. Finally, minimal-risk systems, including AI in video games or spam filters, face little to no regulation under the Act.



""Now that they're getting better at writing computer code, they could be used for offensive cyberattacks. An AI could hack into computer systems. If this technology goes wrong, it can go quite wrong."

UK regulations

The UK currently does not have AI-specific legislation, often referred to as a “UK AI Act,” and instead relies on a principles-based framework outlined in the March 2023 AI White Paper. This approach sets out five broad principles—safety, transparency, accountability, fairness, and contestability—while leaving enforcement to regulators such as the FCA, ICO, and Ofcom. Unlike the EU’s risk-based AI Act, which applies uniform rules across member states, the UK model emphasises flexibility and innovation. By delegating oversight to existing regulators, the government hopes to support AI-driven growth while maintaining some accountability and public trust.



The government is also preparing an Artificial Intelligence (Regulation) Bill, designed to embed these principles into law and create a central AI Authority to oversee risk assessment. However, the Bill has been delayed until at least summer 2025, partly to align with the United States’ pro-innovation stance. This reflects the UK’s effort to balance fostering innovation with addressing growing concerns around AI safety and misuse. While its approach differs from the EU’s stricter framework, the UK is gradually moving toward more formal governance as AI technologies become more powerful and widespread.

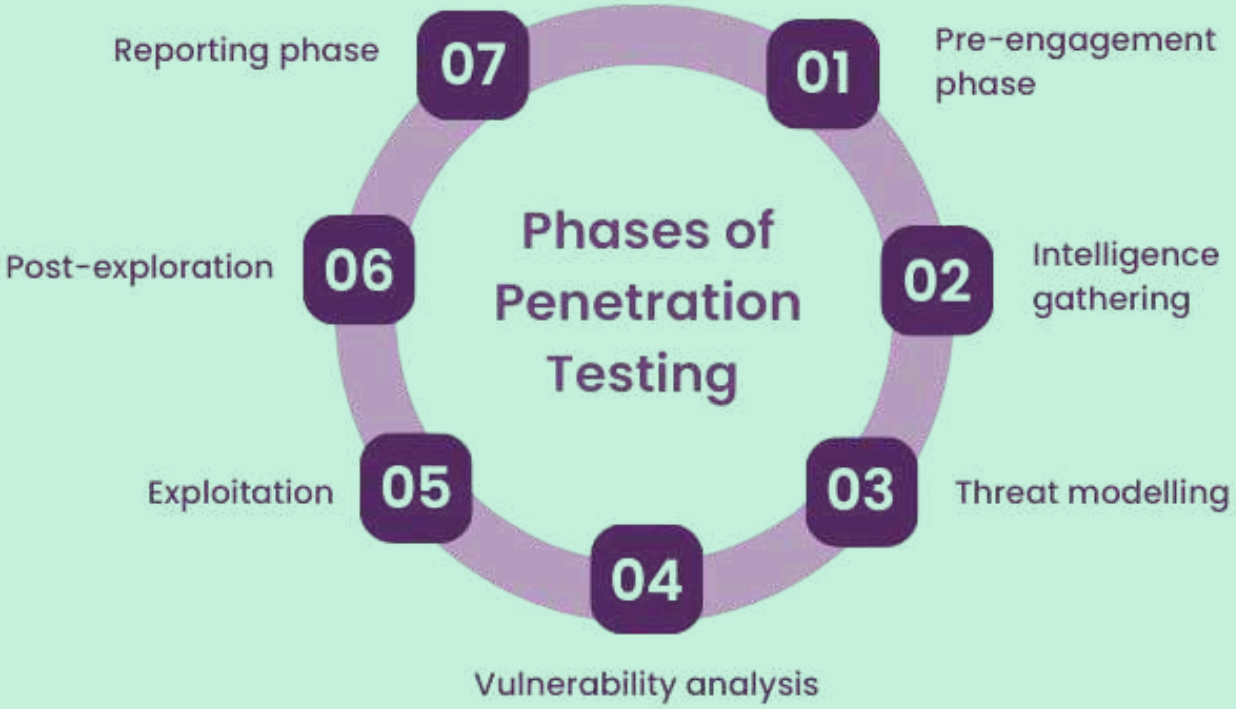
BEYOND THE HOODIE

When you think of “penetration testing” today, the image that often comes to mind is a hoodie-clad hacker at a terminal, but its roots stretch back to the earliest days of conflict, when military leaders staged mock attacks to expose weaknesses in castles, fortifications, and battle formations—early precursors to what we now call ethical hacking. By the 1960s, as computers became critical to government and defence, questions about their trustworthiness grew, leading the U.S. Air Force to commission the Willis Ware Task Force in 1967, which examined vulnerabilities in time-sharing systems and inspired the creation of “Tiger Teams” that tested advanced platforms like MULTICS. The rise of personal and business computing in the 1980s and 1990s brought with it new cyber threats and tools such as SATAN, Nmap, and Nessus, which quickly became staples for security practitioners. At the same time, structured frameworks emerged—first the OWASP Testing Guide in 2003, which standardised application testing, and later the Penetration Testing Execution Standard (PTES), which set clear methodologies. From military drills to a corporate necessity, penetration testing has evolved into a mature discipline that underpins modern cybersecurity.

Pen test evolution

Traditional penetration tests were like annual medical checkups—useful, but quickly outdated. Organisations got a "point-in-time" snapshot of their vulnerabilities, which might already be irrelevant a week later, thanks to new exploits or software updates. This mismatch between static testing and dynamic threats led to a new model: continuous pen testing. Under this umbrella, services like PTaaS (Penetration Testing as a Service) emerged, offering always-on visibility. Instead of waiting months for the next audit, security teams could identify and patch risks in near real time. More innovative still, firms introduced PETaaS® (Professionally Evil Testing as a Service)—a flexible, on-demand model where testers could launch assessments instantly, adapting to agile development cycles. The most transformative force, however, has been AI. Gone are the days when pen testers spent hours manually coding custom exploits. With AI-driven scripting and machine learning-enhanced reconnaissance, attackers—and defenders—can generate tools at lightning speed. Generative AI, in particular, is reshaping how vulnerabilities are discovered, chained, and reported.

The lesson here? Pen testing has evolved from being an occasional formality to becoming a continuous, adaptive layer of cybersecurity. Organisations that cling to old models risk being perpetually one step behind adversaries.



What it is

At its core, penetration testing is a controlled adversarial simulation. Ethical hackers mimic the techniques of malicious actors to identify cracks before the real criminals can exploit them. But it's important to clarify: pen testing is not the same as vulnerability scanning. Scanners can detect known issues—open ports, outdated software, misconfigurations—but they rarely demonstrate the real-world impact. A pen tester, on the other hand, doesn't just spot the open door; they walk through it, test how far they can go, and determine what damage could be done. Modern pen testing branches into several flavours:

- **Network Penetration Testing** – Probing internal and external networks for weaknesses.
- **Web Application Testing** – Identifying injection flaws, broken authentication, and insecure APIs.
- **Wireless Testing** – Exploiting insecure Wi-Fi configurations or encryption flaws.
- **Social Engineering** – Testing human vulnerability through phishing or impersonation.
- **Physical Pen Testing** – Attempting real-world intrusions (badge cloning, lock picking, device access).

Together, these paint a comprehensive picture of an organisation's exposure. For IT teams, it's not just about finding bugs—it's about understanding how those bugs translate into business risk.

Hacker's arsenal

No penetration tester walks in empty-handed. Their toolkit is an evolving mix of open-source utilities, commercial products, and custom scripts. Some icons of the trade include:

- **Nmap** – The network mapper that identifies open ports and services.
- **Wireshark** – A packet sniffer that reveals what's moving across networks.
- **Metasploit** – The Swiss army knife of exploitation, enabling testers to simulate thousands of known attacks.
- **Burp Suite** – The go-to for web application testing, from intercepting traffic to fuzzing requests.
- **John the Ripper & Hashcat** – Legendary password-cracking tools.
- **sqlmap** – Automates the discovery and exploitation of SQL injection flaws.

But remember: tools don't make the hacker. The real edge lies in creativity, persistence, and an attacker mindset.

Red, blue and purple

Pen testing isn't only about breaking things; it's about testing the full lifecycle of defence. Enter the red and blue teams.

- **Red Teams** act as the adversary, simulating prolonged and stealthy campaigns that mirror real threat actors. Their goal: test not just systems, but also detection and response.
- **Blue Teams** are defenders, monitoring, detecting, and mitigating attacks in real time.
- **Purple Teams** blend both, fostering collaboration where red exposes weaknesses, and blue learns to close gaps faster.

For IT professionals, these exercises show security isn't just about "can I be hacked?"—it's also about "can I detect and respond when I am?"

2017 Equifax breach

One of the most infamous cybersecurity failures of the last decade was the Equifax breach. Attackers exploited an unpatched Apache Struts vulnerability (CVE-2017-5638), gaining access to the personal data of over 147 million people—names, Social Security numbers, addresses, and more. What's chilling is that the vulnerability had a patch available months before the attack, but it went unapplied. A well-timed penetration test could have flagged the oversight, emphasising why testing isn't just about finding exotic, zero-day flaws—it's also about ensuring the basics don't slip through the cracks.

2018 British Airways

In 2018, attackers injected malicious scripts into British Airways' website and mobile app, skimming customer payment details during transactions. Over 400,000 payment cards were compromised, leading to regulatory fines under GDPR. What's notable here is that the compromise hinged on insecure web application practices—something a dedicated web application penetration test could have uncovered. This case illustrates the business impact: not just data loss, but also brand reputation and regulatory costs.

2021 Colonial Pipeline

The ransomware attack on Colonial Pipeline disrupted fuel distribution across the U.S. East Coast, causing shortages and public panic. The attackers exploited compromised credentials for a VPN account that lacked multi-factor authentication. While not a traditional web app exploit, this case underscores the broader role of pen testing: validating identity controls, remote access policies, and incident response readiness. For IT teams, it's a reminder that attackers don't need sophistication—just opportunity.

7 Phases

- **Reconnaissance** – Research and information gathering.
- **Scanning** – Actively mapping systems, ports, and services.
- **Exploitation (Gaining Access)** – Breaking through vulnerabilities.
- **Maintaining Access** – Demonstrating persistence.
- **Escalation & Pivoting** – Expanding control across systems.
- **Covering Tracks** – Evading detection to mimic real attackers.
- **Reporting & Remediation** – Documenting findings, prioritising risks, and validating fixes.

These stages transform hacking from guesswork into a systematic science. They also ensure stakeholders receive actionable intelligence—not just lists of bugs.

Pros and cons

Done right, penetration testing is a powerful investment:

- Identifies critical vulnerabilities before attackers exploit them.
- Provides a real-world perspective on business risk.
- Tests both preventive and detective controls.
- Supports compliance frameworks (PCI DSS, HIPAA, ISO 27001, etc.).
- Enhances organisational awareness and incident readiness.

But it's not flawless. Limitations include:

- Tests are time-bound—new threats can emerge after the test.
- Skilled testers are in short supply, and quality can vary.
- Some findings may duplicate vulnerability scans.
- Reports are only useful if management acts on them.

The story of penetration testing is one of evolution—from Tiger Teams in government labs to AI-assisted ethical hackers safeguarding cloud infrastructures today. What hasn't changed is the philosophy: to defend well, you must first think like an attacker.

zhero

A Journey into Cybersecurity

This month, Macwhill Hanse, one of our awesome Service Desk engineers, gives us his insider story on IT support and cybersecurity.

From a young age, I knew I wanted to work in a field where I could help people — and I've always had a natural curiosity for technology. I was fortunate to grow up in a time when tech was becoming part of everyday life. I got my first computer around the age of 10 and I spent hours exploring how it worked, breaking things, fixing them, and learning through trial and error.

Before joining Zhero, I had just finished my final year of high school. At the time, I was considering a gap year to explore different industries and figure out where I might fit best. That's when I was offered an internship at Zhero — and from day one, I knew I'd found something that challenged and inspired me. Working in IT quickly taught me that the industry is far more dynamic than it appears. There's rarely one "right" answer — often, there are multiple ways to solve the same problem. Some work, some don't, and it's up to you to figure out the most effective and reliable solution. That process of troubleshooting, problem-solving, and helping people through their technical challenges is something I've come to enjoy genuinely.

What I find most exciting about the tech industry is how fast-paced it is. You're constantly learning, adapting, and evolving. At the same time, I've learned the value of mastering the fundamentals. Without a strong grasp of the basics, it isn't easy to build deeper, more advanced skills — especially in areas like automation and cybersecurity. That's where I'm focusing my energy now: strengthening my technical foundation and applying those skills in real-world scenarios. I genuinely enjoy what I do. Each day brings a new opportunity to grow, support others, and solve problems that make a tangible difference. I'm especially interested in the intersection of automation and cybersecurity — and I'm looking forward to seeing how the industry continues to evolve, particularly with the rapid advancements in AI.

Windows 10 EOL

On 14 October 2025, Windows 10 Home and Pro will reach end of support or end of life (EOL). End of Life (EOL) is when a software application is taken off the market or not renewed. The manufacturer may still provide some support, such as security patches and updates. End of Support (EOS) is the complete discontinuation of all support services for the software.

WHAT THIS MEANS

- No more free updates - After October 14, 2025, Windows 10 users will not receive any further free security updates, feature updates, or technical support from Microsoft.
- Security risks - Running Windows 10 without security updates will expose your device to potential security threats, malware, and vulnerabilities.
- Upgrade or replace - Microsoft advises users to either upgrade to Windows 11 (if their hardware is compatible) or replace their devices with new ones that support Windows 11.
- Extended Security Updates (ESU) - Microsoft offers an ESU program for Windows 10, which provides paid security updates for a limited time after the EOL date, but it's not a long-term solution and doesn't include new features.
- Windows 11 advantages - Windows 11 offers a modern and efficient experience with enhanced security features, designed to meet current demands.
- Free upgrade - Upgrading from Windows 10 to Windows 11 is free for eligible devices.
- PC Health Check - If you're unsure whether your PC is compatible with Windows 11, you can use the PC Health Check app to check its eligibility.

Windows 10 EOL

WHAT WILL HAPPEN

Your PC will continue to work, but all support for Windows 10 is discontinued.

WHAT YOU CAN DO

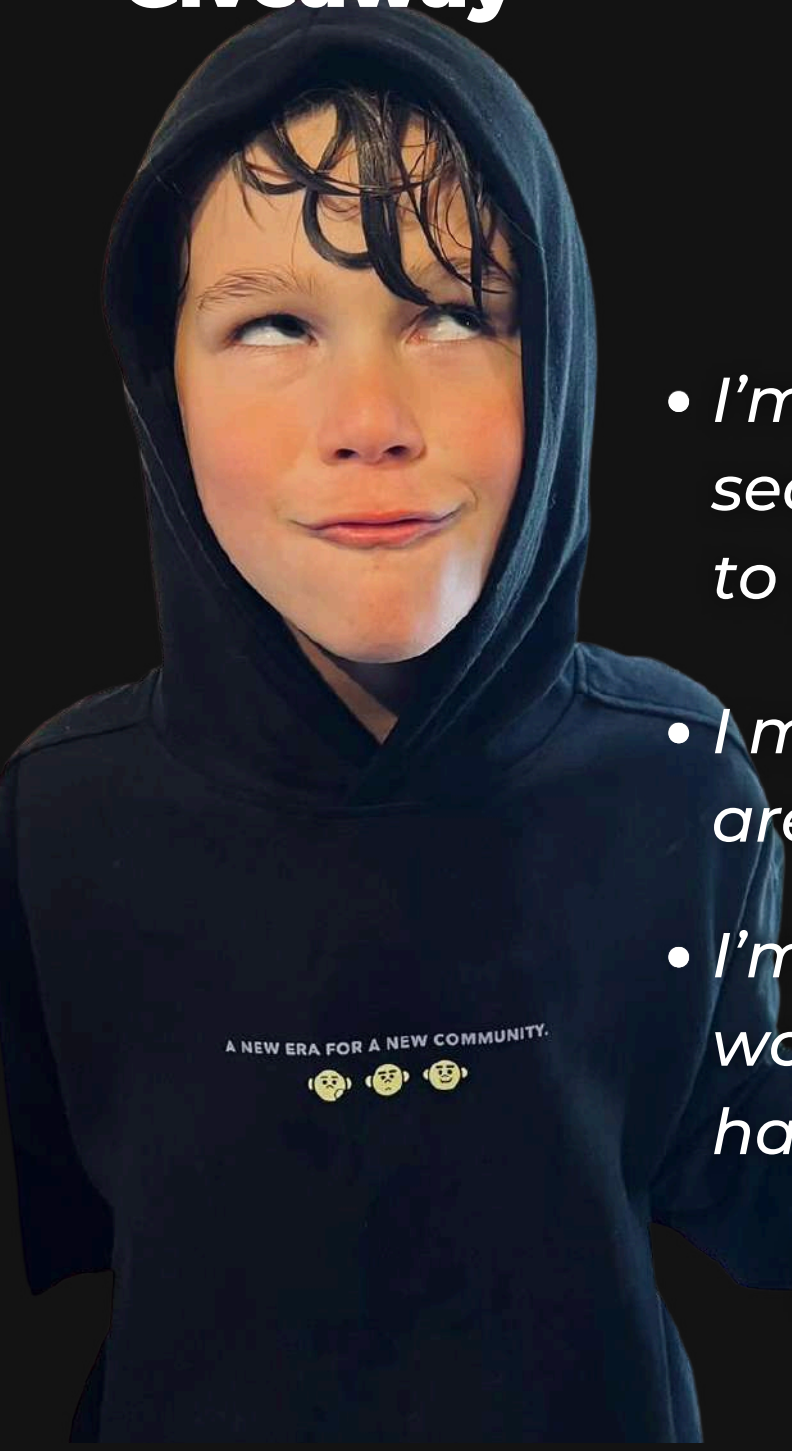
- You could ignore the EOL deadline completely. This is NOT recommended as your PC is no longer receiving updates and security patches from Microsoft. This means your PC is vulnerable to malware infections and other cyber threats. You will also experience performance and compatibility issues.
- You can pay Microsoft for security updates for Windows 10. With the Extended Security Updates package you can keep your current Windows 10 device fully protected for up to 3 years. According to Microsoft, the first year of protection will cost £50. This increases to £100 in the second year and £150 in the final year of cover.
- You can upgrade your existing PC to Windows 11 or buy a new laptop with this latest OS already installed.

WHAT WE WILL DO

Zhero recommends switching to Windows 11. We will assess whether your existing PC can be upgraded and is capable of running Windows 11 or if you will need a new workstation. While making the change to a new OS may seem daunting, we are here to support and assist you in every way we can.

Digital Defender Giveaway

Win £50 amazon voucher



- *I'm a protector of secrets, and my duty is to guard*
- *I make sure prying eyes are barred*
- *I'm vital in the digital world and can be soft or hard*

What am I?

Enter our monthly draw and stand a chance of winning a £50 Amazon voucher. The winner will be announced in the next edition of Inside Zhero.
Competition ends 13 October.
Good Luck!

Enter Now

Winner!

Congrats to Steph Nixon, Director of Supply Chain at Geeta's Foods, for winning last month's draw and a £50 Amazon voucher.

Meet the team

Shirley Lang

OFFICE MANAGER & FINACE ASSISTANT

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

It started as something I had to learn do a bit of graphic designing for my cake business. Then I had to take some IT courses and basically one interest developed into another.

What's your most-used productivity tool?

I must say Microsoft Teams as we use it all the time. I've experimented a bit with AI and admit to being inquisitive and intrigued by it.

How would you describe yourself?

I'm relatively reserved without being an introvert. I love having people around me, so I really enjoy being part of this dynamic team.

What do you enjoy the most about your role?

I'm enjoying the challenge of learning about these amazing tools and programmes that make up a small part of IT. One is NEVER too old to learn!

Do you have any hidden talents or hobbies?

I had my own businesses – a coffee shop and more recently a cake shop so yes, I love baking and cooking.I enjoy long walks along our beautiful Cape Beaches.

What is your favourite movie or TV show?

Breaking Bad – the series and Movie. It fascinated and appalled me at the same time.

CRUSH IT CHAOS

Tune in here:

zhero | PODCAST

LONDON

162 Farringdon Road
London
EC1R 3AS

SPEAK TO US

+44 20 7183 3975

START THE PROCESS

zhero
crush the chaos