MAY 2025

inside zhero

Transformative Cybersecurity

AI and Machine Learning

Ransomware Retail Spree

The Cost of Unpreparedness

Izak's Cyber Insights

AI and Automation

Message from Izak

Welcome to our latest edition of Inside Zhero.

This month, we're focusing on the power of AI, Machine Learning and Automation as effective cybersecurity detection and response tools. We'll also take a look behind the scenes at the recent ransomware attacks on the UK retail sector.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature "Transformative Cybersecurity" explains how we can leverage AI to benefit many aspects of cybersecurity.

70% of cybersecurity professionals say AI proves highly effective for detecting threats that previously would have gone unnoticed.

"I believe AI could become a massive cyber threat. We can effectively counter that threat by using it as an even more powerful cybersecurity tool and ally."

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consultation

30% discount **cyberzhero542**

TRANSFORMATIVE CYBERSECURITY

AI has been part of cybersecurity since at least the late 1980s, when early systems used basic rules to trigger alerts if something didn't look right. In the 2000s, machine learning, a branch of AI that learns from large amounts of data, gave security teams a better way to understand normal traffic and user behaviour, helping them detect unusual or suspicious activity more quickly. The latest evolution, generative AI, can be used through natural language, meaning security professionals can ask complex questions in plain English instead of using technical queries. Around 80% of cybersecurity professionals now use AI in some form, and over 70% say it helps improve threat detection and response times. Cyber attackers also leverage AI to automate attacks, mimic legitimate users, and identify vulnerabilities faster. Some try to manipulate AI systems directly or inject malicious content into training data. There's also a growing risk of people unintentionally leaking sensitive information by pasting it into AI tools without thinking. AI is transforming cybersecurity on both sides, offering faster, smarter protection, and also giving attackers new ways to cause harm. The key is staying ahead of the curve.

How AI works

AI for cybersecurity functions by analysing vast amounts of data from multiple sources to detect patterns of activity, such as user sign-in times and locations, traffic volumes, and the devices and cloud applications employees use. Once the system has a clear understanding of what constitutes typical behaviour, it can identify anomalies that may warrant further investigation. AI relies on global threat intelligence aggregated from numerous organisations. Machine learning algorithms enable the system to learn continuously from the data it processes. When generative AI recognises known cyberthreats, such as malware, it can help to contextualise threat analysis, making the information more accessible by generating explanatory text or images. While human expertise remains essential in cybersecurity, AI enhances our capabilities, enabling us to detect and address threats more swiftly.

Benefits for cybersecurity

AI helps cut through the noise by quickly scanning thousands of events logged in security tools and highlighting the ones that actually matter. This is especially helpful for spotting threats that might seem harmless on their own but become serious when looked at in context. AI also makes reporting a lot easier. Generative AI can pull info from multiple sources and turn it into clear, easy-to-share summaries. It can also flag risks you might not know about, like unknown devices, outdated systems, or unprotected data sitting where it shouldn't be. Generative AI also breaks down complex threat data into natural language, so even team members who aren't super technical can understand what's going on and take action, speeding up response times. Studies show AI can reduce the time it takes to detect and respond to incidents by up to 50%.

AI use cases

- **Identity and access management** - AI supports identity and access management (IAM) by analysing user sign-in patterns to detect and highlight anomalous behaviour for security professionals to investigate. It can automatically enforce two-factor authentication or prompt a password reset when specific conditions are met. In cases of suspected compromise, AI can block sign-in attempts to protect the account.
- **Endpoint security and management** - AI assists security teams in identifying all endpoints in use across an organisation and ensures they remain up to date with the latest operating systems and security measures. It can also detect malware and other signs of cyberattacks targeting organisational devices.
- **Cyberthreat detection** - AI is central to both extended detection and response (XDR) and security information and event management (SIEM) solutions. XDR monitors endpoints, emails, identities, and cloud apps for unusual activity and can either alert security teams or initiate automated responses based on pre-set rules. SIEM aggregates security signals across the enterprise, using AI to enhance visibility and support threat detection.
- **Information protection** - AI helps security teams locate and classify sensitive data throughout an organisation's infrastructure, whether on-premises or in the cloud. It can detect attempts to exfiltrate data and either block these actions or alert the security team for further investigation.

Detection and prevention

One of the most powerful ways AI is being used in cybersecurity is for spotting and stopping threats. Machine learning plays a big role here, helping systems quickly pick up on potential risks and take action before things get out of hand. There are different ways this works. Supervised learning uses labelled data, such as known malware signatures, to train systems to recognise specific types of attacks. On the flip side, unsupervised learning looks for patterns in unlabelled data, which helps uncover new or more sophisticated threats by flagging anything that seems unusual or similar to past incidents. AI also gets smarter with behaviour tracking. By learning what's "normal" for users and devices, it can catch things that seem out of the ordinary, like someone logging in at strange hours or accessing systems they usually don't touch. This kind of behaviour analysis is great for spotting compromised accounts. AI also doesn't just rely on technical data. With natural language processing (NLP), it can scan through unstructured sources like social media or forums to pick up early signs of emerging threats and help teams stay ahead with real-time insights.

"AI in security is like a seasoned chess grandmaster, anticipating threats and countering moves before they unfold on the board. It dynamically adapts to new vulnerabilities, proactively fortifying systems against sophisticated cyber attacks."

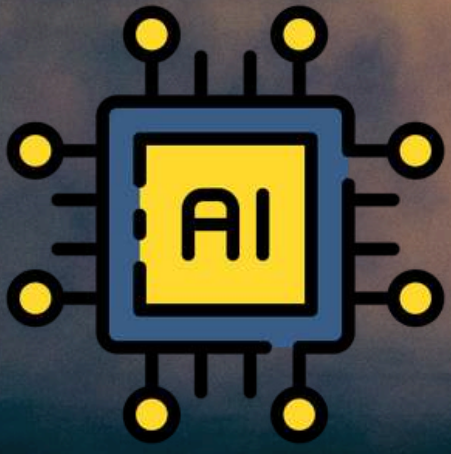
Jason Hishmeh, CTO

Security tools

AI is now built into all kinds of cybersecurity tools, making them smarter and more effective across the board. Take next-gen firewalls, for example, unlike older ones that just follow preset rules, these use AI to tap into threat intelligence and spot new or evolving attacks in real time. On the endpoint side, AI-powered security tools can detect outdated systems, catch malware, watch for odd data transfers, and even isolate compromised devices before they spread the damage. AI-driven intrusion detection systems do something similar on the network, scanning traffic to spot and stop intruders faster and more accurately than older systems could.

In the cloud

In cloud environments, where things can get complicated fast, AI helps by analysing data across different platforms and flagging potential threats or weak spots across multi-cloud setups. It also keeps an eye on IoT devices, which are often harder to secure, spotting risks on individual gadgets and picking up unusual patterns across big networks of connected devices. And when it comes to pulling everything together, tools like XDR and SIEM rely heavily on AI to sort through mountains of data from logs, devices, apps, and external sources. Instead of drowning in alerts, security teams get clear, actionable insights they can use to respond quickly and effectively.



"Some people call this artificial intelligence, but the reality is this technology will enhance us. So instead of artificial intelligence, I think we'll augment our intelligence."

Ginni Rometty, Former IBM CEO

AI implementation

Develop a strategy - Not every AI solution will suit your organisation. Focus on your most pressing security challenges and choose AI tools that align with your existing systems. A clear integration plan will ensure the tools improve, rather than complicate, your operations.

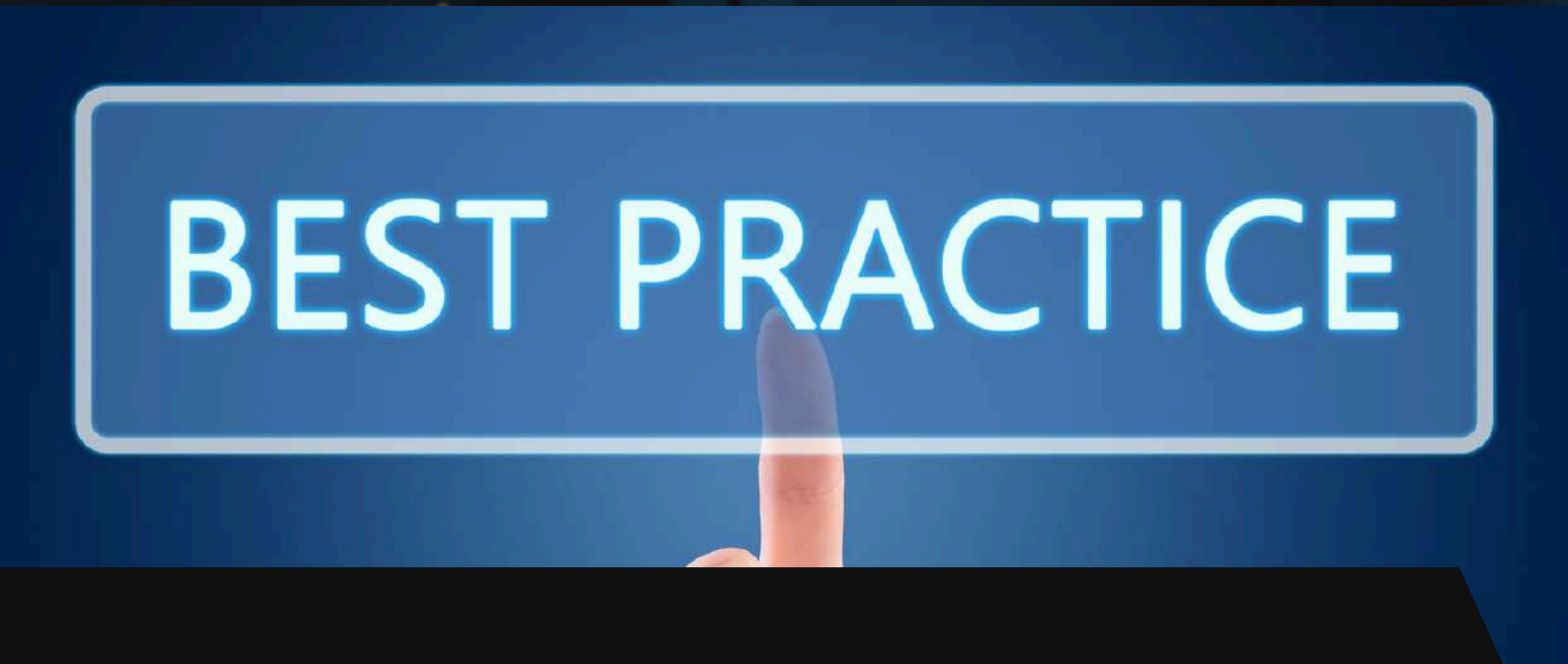
Integrate your security tools - AI works best when it can analyse data across your entire environment. Avoid tool siloes by using integrated solutions like XDR and SIEM or invest time in connecting existing tools to achieve full visibility.

Manage data privacy and quality - AI relies on high-quality, accurate data. Ensure your systems include processes for cleaning data and protecting privacy, as poor data leads to poor insights and decisions.

Continuously test your AI systems - Regular testing helps uncover issues like bias or degraded performance as new data is introduced, keeping your AI systems effective over time.

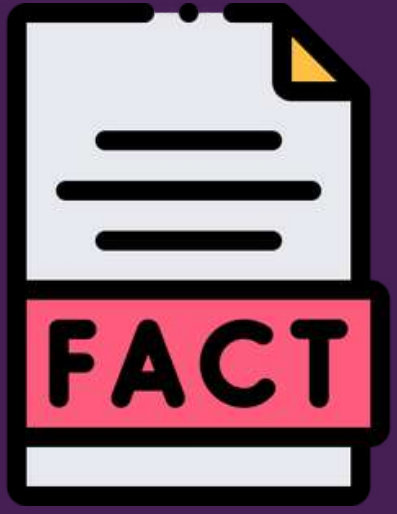
Use AI ethically - AI can reflect outdated or biased data, and its decision-making process isn't always transparent. Avoid relying on AI for final decisions in sensitive areas and prioritise fairness and accountability.

Define policies for generative AI - Clearly communicate policies for using generative AI, especially around data security. Employees and partners should avoid entering confidential or sensitive information into AI prompts to prevent accidental data exposure.



The future

According to IBM, organisations that use AI and automation in their security systems can reduce the cost of a data breach by up to $1.76 million on average. As AI continues to evolve, security teams can expect smarter threat detection with fewer false alarms, helping them focus on real issues instead of chasing down red herrings. Routine tasks like monitoring alerts or analysing logs will increasingly be handled by AI, freeing up human experts to tackle bigger challenges. That means cybersecurity professionals will shift toward more strategic roles—investigating complex incidents, proactively hunting threats, and shaping stronger defence strategies. As we know, it's not just the good guys using AI. Cybercriminals are also getting smarter. They're turning to AI to crack massive numbers of passwords, generate realistic phishing scams, and build stealthier malware. A recent study by the World Economic Forum even found that 48% of cybersecurity leaders believe AI-powered attacks will become mainstream in just a few years. As threat actors incorporate more advanced AI into their tactics, it will be even more critical for the security community to adopt and evolve their own AI capabilities to stay ahead. But with the right mix of people and technology, the future of cybersecurity looks to be a lot more secure.



- 15% of CISOs feel non-AI cybersecurity tools are capable of detecting and stopping AI-generated threats
- 50% of organisations say they're using AI to compensate for a cybersecurity skills gap
- 73% of cybersecurity teams want to shift focus to an AI-powered preventive strategy
- 70% of cybersecurity professionals say AI proves highly effective for detecting threats that

zhero

Security insights

Izak gives us his take on the future of AI in cybersecurity. His insights show that coupled with automation, AI will become an indispensable security tool that will transform data handling, monitoring, detection and response and much more. Here are his words of wisdom.

As we move further into our tech-driven future, I believe AI is set to become a powerful, multi-functional partner in cybersecurity. With automation at its core, AI enables us to analyse massive volumes of data at incredible speeds and identify patterns, whether they're routine or potentially suspicious. One of the major benefits is that once an AI system learns what normal behaviour looks like, it can quickly detect any anomalies that might need further investigation.

Another key advantage of AI is that it continually learns through machine learning. The more data it processes, the more accurate and effective it becomes. For instance, when generative AI can recognise known cyber threats, malware being a prime example, with over 560,000 new instances discovered daily, it can also help by generating clear, accessible explanations or visuals that make complex threats easier to understand. While human expertise remains essential in cybersecurity, AI significantly boosts our ability to detect threats and respond more rapidly.

zhero

Security insights

Many cyberattacks, including those involving malware, ransomware, or stolen credentials, often begin with a phishing email designed to trick someone into clicking a harmful link or downloading an infected file. Here too, AI can be a game changer. It can instantly assess email content and sender information with a level of precision that far exceeds traditional methods. Another advantage is AI's ability to automate security responses, for example, isolating compromised systems or blocking malicious IP addresses, reducing the impact on networks and helping to safeguard sensitive data.
Let's now explore two specific use cases where AI is having a meaningful impact on cybersecurity.

The first is the use of AI in Endpoint Detection and Response (EDR), and more broadly in Managed Detection and Response (MDR). These solutions provide continuous security monitoring, proactive threat hunting, and fast incident response. MDR aims to prevent data breaches and ransomware attacks by combining human insight with advanced machine learning models. AI enhances MDR by identifying all devices connected across an organization and ensuring they are regularly updated with the latest security patches and system updates.

Generative AI also plays a valuable role in detection engineering, which involves developing and refining detection capabilities to stay ahead of evolving threats. AI is especially useful for automating tasks like prioritizing vulnerabilities and enhancing Security Information and Event Management (SIEM) systems. When paired with MDR, AI helps to collect, analyse, and correlate logs from a wide range of data sources, delivering insights at a depth and speed that humans simply can't match. This includes tasks like sentiment analysis and improving reaction times, both of which help security teams respond more quickly and effectively.

zhero

Security insights

The second use case involves the integration of AI with cloud computing. For those less familiar with the term, the cloud refers to accessing servers, storage, and databases over the internet instead of relying on local infrastructure. The cloud is now central to both business and personal use - 96% of companies worldwide use public cloud services like Amazon Web Services, and more than 2.3 billion people use personal cloud platforms like Dropbox, Google Drive, or iCloud. The global cloud market is projected to exceed $940 billion next year.

Given its widespread use, securing the cloud is more important than ever. AI helps by providing visibility into potential risks and vulnerabilities across complex multi-cloud environments. This allows security teams to manage and protect cloud assets more effectively. One key area is Cloud Security Posture Management (CSPM), where AI is used to assess configurations and automatically resolve security issues. Another is Cloud Workload Protection (CWP), where AI monitors and protects cloud-hosted applications and data from threats such as malware and unauthorised access.

In short, as technology continues to evolve, AI is transforming the way we approach cybersecurity. While it's true that AI may also make certain types of attacks more sophisticated, it offers us powerful tools to stay ahead. By using AI responsibly and strategically, we can create a safer digital environment for everyone.

RANSOMWARE RETAIL **SPREE**

Disruption continued across the UK retail sector over the first May bank holiday weekend, following a wave of cyberattacks that began two weeks before. Customers reported empty shelves at retailers including Marks & Spencer (M&S) and Co-op as the impact of the breaches persisted. The attacks, which started over the Easter weekend, have been claimed by affiliates of the DragonForce ransomware-as-a-service (RaaS) group. Investigators have linked the activity to Scattered Spider and The Com, two overlapping, English-speaking hacking groups believed to be working with DragonForce. DragonForce previously shared a sample of data involving approximately 10,000 Co-op members with the BBC. The group also warned reporters that additional UK retailers are listed as future targets. Following the M&S and Co-op attacks, the luxury department store Harrods stated that it had also been targeted by a cyberattack, but its flagship store remained open, and it continued to operate its online sales.

What is DragonForce?

DragonForce originally operated as a Malaysia-based hacktivist group supporting Palestinian causes. However, since emerging in the summer of 2023, the group has shifted toward a hybrid model combining political hacktivism with ransomware-driven extortion. DragonForce has launched attacks against government entities in Israel, India, Saudi Arabia, and the UK, as well as against private sector organisations aligned with particular political agendas. The recent wave of attacks on UK businesses underscores the critical importance of robust cybersecurity measures and well-defined incident response strategies.

Gaining access

DragonForce typically infiltrates victim networks through a combination of targeted phishing campaigns and exploitation of known software vulnerabilities. Among their preferred attack vectors are well-known issues such as the Log4j vulnerability and high-profile flaws in Ivanti systems. They are also known to leverage stolen credentials, which may have played a role in the M&S breach. In some cases, credential stuffing attacks are used to access remote desktop protocol (RDP) services or virtual private networks (VPNs). Once inside a network, the group often deploys tools like Cobalt Strike to orchestrate its campaigns. They also utilise remote management and reconnaissance utilities such as Mimikatz, Advanced IP Scanner, and PingCastle to move laterally within systems, establish persistence, and escalate privileges, tactics that are common among ransomware operators.

NCSC responds

Jonathan Ellison and Ollie Whitehouse of the National Cyber Security Centre (NCSC), Director of National Resilience and CTO respectively, said the NCSC is working closely with the organisations affected by the recent cyber incidents to understand the nature of the attacks and minimise their impact, while also guiding the broader retail sector and the wider economy. They noted that, although the NCSC has some insights, it is not yet in a position to determine whether the attacks are linked, represent a coordinated campaign by a single actor, or are unrelated. They added that the NCSC is collaborating with victims and law enforcement to clarify the situation, sharing information with the affected companies and the broader sector through its sector-focused Trust Groups, and encouraging organisations to exchange experiences and mitigation strategies with one another.

Stuart Machin, M&S chief executive:

"To give customers extra peace of mind, they will be prompted to reset their password the next time they visit or log on to their M&S account, and we have shared information on how to stay safe online."

M&S impact

Besides empty shelves and lunchtimes sans Meal Deals, insiders at M&S told Sky News that IT staff have been forced to sleep in the office due to the ongoing disruption. Employees described a chaotic response, citing a lack of preparedness for such an incident and warning that it may take considerable time before operations begin to stabilise. Apart from bruising the M&S reputation, this breach led to a major financial loss for the company. M&S's market value plummeted by over £700 million, and the company faced estimated losses of £40 million per week due to the attack, as reported by Reuters and analysts at Bank of America, which would cut its profits by an expected 7% for the coming year. As of 15 May, M&S was still offline for online orders. While customers could still browse and add items to their baskets, they couldn't complete their purchase, and the retailer had not announced a return date. On Tuesday, May 13, Marks and Spencer confirmed that personal customer information was breached in the attack. M&S operations director Jayne Wall urged people to be cautious and avoid giving out any personal details to unknown callers.

Jayne Wall, M&S operations director:

"The nature of the incident means that some personal customer data has been taken, but there is no evidence that it has been shared. You do not need to take any action, but you might receive emails, calls or texts claiming to be from M&S when they are not."

Co-op pulls the IT plug

Co-op narrowly avoided being locked out of its computer systems, according to DragonForce who spoke to the BBC. Fortunately, Co-op's IT team detected the breach in progress and took the company's systems offline. This may help explain why Co-op has started to recover more quickly than M&S. According to the hackers, "Co-op's network never ever suffered ransomware. They yanked their own plug – tanking sales, burning logistics, and torching shareholder value." They expressed anger that the company's proactive response had cut off their access, saying they had been "seated in their network" for some time prior to being discovered. Cybersecurity expert Jen Ellis from the Ransomware Task Force described Co-op's response as sensible, noting that, "Co-op seems to have opted for self-imposed immediate-term disruption as a means of avoiding criminal-imposed, longer-term disruption. A successful ransomware attack would likely have made Co-op's recovery more complex, time-consuming, and costly—problems that M&S now appears to be facing.

Lessons Learnt

- **Prioritise Identity and Access Management** - Implementing multi-factor authentication (MFA) and enforcing strong password policies are non-negotiables in the current cyber threat landscape. The M&S attack also serves as a reminder to regularly audit user access. Any unnecessary or excessive access should be promptly revoked to minimise the potential attack surface.
- **Enhance Employee Awareness and Training**- Social engineering tactics played a role in the M&S attack. Hackers employed social engineering tactics to deceive IT workers into resetting passwords to gain access to systems. A critical layer of defence against such tactics is comprehensive and ongoing cybersecurity training for all employees.
- **Develop and Test Incident Response Plans** - A well-defined and regularly tested incident response plan is crucial for minimising the impact of cyberattacks. Every organisation today has to prioritise having a robust cyber incident response plan. This plan should be crisp, to-the-point and fluff-free.
- **Invest in Cybersecurity Infrastructure** - The Marks & Spencer incident underscores the critical importance of ongoing and substantial investment in cybersecurity infrastructure. This includes the deployment of advanced threat detection systems that are capable of identifying and responding to potential threats in real-time. This can help prevent cyber incidents from escalating into full-blown security breaches.

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.

WHAT THIS MEANS

After 14 October 2025, your Windows 10 PC will no longer receive free security updates and Microsoft will no longer be available to provide Windows 10 technical support. 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.

Meet the team

Lovemore Gurungo

ESCALATION ENGINEER

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

My brothers owned a computer shop where they would buy desktops from auctions, fix them and resell them, I realised then that this is the route I wanted to go.

What's your most-used productivity tool?

OneNote, I write all my cool thoughts, commands, scripts and tips, I can easily pull it up when sorting out a challenge.

How would you describe yourself?

I am an introvert who comes alive when dealing with Technology issues and challenges.

What do you enjoy the most about your role?

Learning about new technologies, finding easier, smarter and quicker ways to solve a challenge, and getting my mind blown every time I find a solution.

Do you have any hidden talents or hobbies?

My hobbies are discovering new music, nature walks, and lately been taking an interest in farming.

What is your favourite movie or TV show?

My favourite movie is Once Upon a Time in China, and I also like The Big Bang Theory on TV.

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