ISSUE №1

DIGITAL WORLD

CONTENT

47% OF ORGANISATIONS SUFFERED A RANSOMWARE ATTACK LAST YEAR

A recent study found that security services are not prepared to deal with ransomware and are struggling to ransomware and are finding it difficult to cope with increasingly complex legal frameworks.

The «Impact of Continuous Security Verification» study, published by SafeBreach and conducted by S&P Global Market Intelligence, surveyed 400 senior security professionals from the US and Europe to identify their most pressing security challenges, which CSV tools they use, the level of adoption and maturity of those tools, and the business results they have achieved.

The majority of respondents stated that regulatory complexity is a major concern, with 46% of respondents indicating that the increasing complexity/demanding nature of compliance with regulations and internal security policies is a major concern. In addition, 45% of respondents are also concerned about the increasing costs/risks associated with the growing attack surface - the total number of possible vulnerabilities.

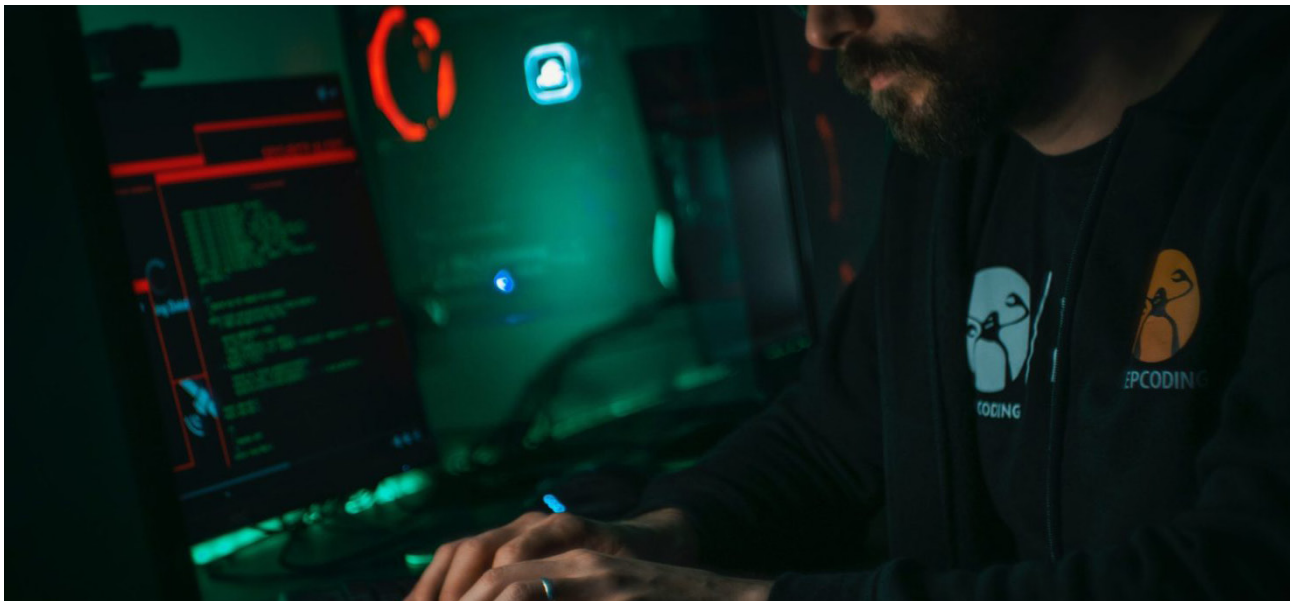
OTHER KEY POINTS

Ransomware attacks are on the rise, but organisations are not prepared: 47% experienced a ransomware attack last year, but only half of these companies had a formal recovery and remediation plan in place. 56% of victims paid ransom, but only 39% of payments resulted in successful data recovery.

«Swivel chair management,» also known as tool overload, creates security gaps: Analysts have access to an average of 21-30 tools in total, using 11-20 of them regularly (at least weekly). Respondents are overwhelmed by the effort to install, maintain, and train on these tools and are concerned about delays in incident response.

Breach and attack simulation (BAS) capabilities help reduce business and operational risk: 95% of respondents value the detection of signatureless and zero-day attacks. 54% said that increased visibility into security controls and their status is a key driver of ROI.

The lack of cybersecurity skills continues to be a concern for respondents. 48% say they are very concerned, and 43% are somewhat concerned about the lack of skills among professionals. 91% are concerned about staffing levels.



MICROSOFT PATENTS A BACKPACK WITH AUTONOMOUS ARTIFICIAL INTELLIGENCE AND A BUNCH OF SENSORS

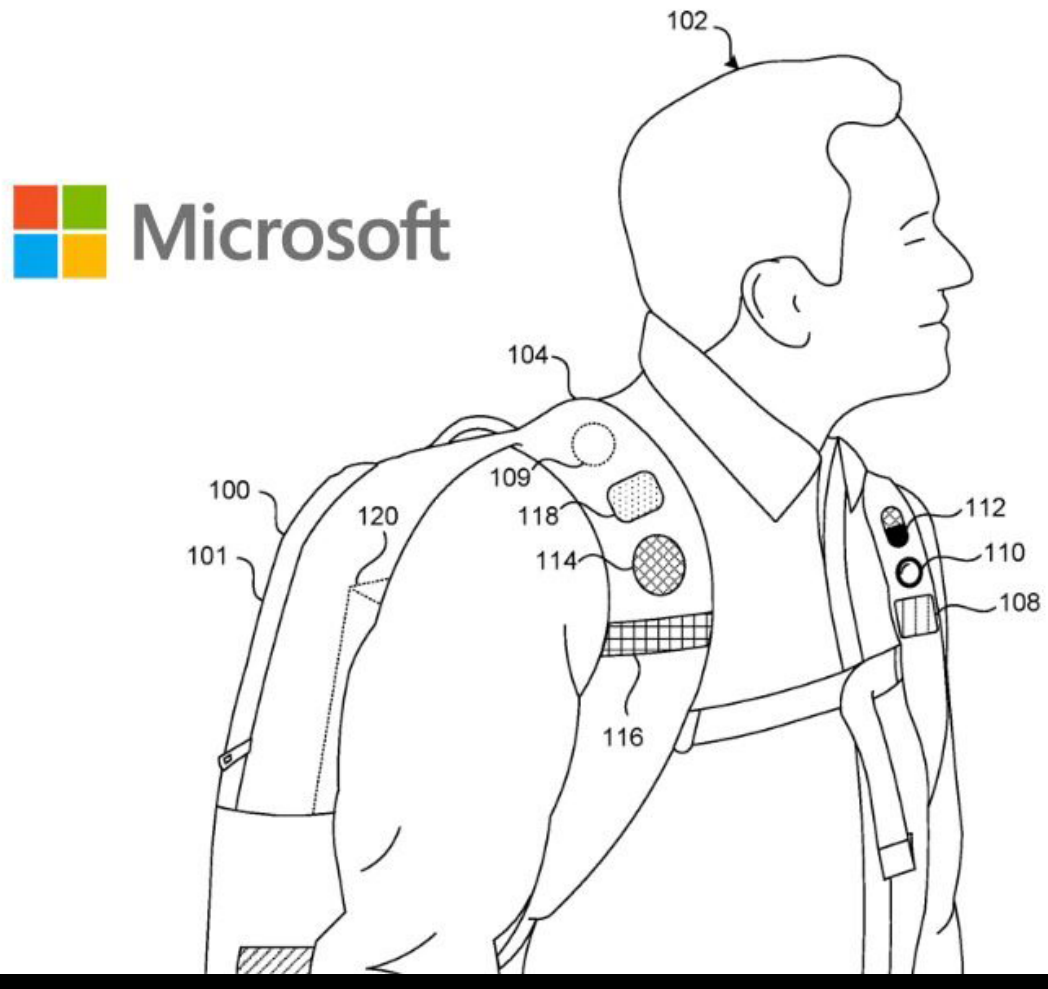
The United States Patent and Trademark Office (USPTO) has granted Microsoft's application for a smart backpack with a large number of sensors and artificial intelligence algorithms.

The sensors are mostly located on the straps. They include cameras, microphones, a GPS sensor, and a compass. It is also known that the patent belongs to the category of "wearable devices with artificial intelligence".

According to Microsoft, the backpack will be equipped with LEDs and speakers, as well as a tactile control system. The device will benefit from the ability to process data in real time, so there are modules for image, text, speech, face recognition, etc. It will also have built-in memory, wireless connectivity, and a built-in battery.

All of the above-mentioned sensors and processing tools are assumed to be in the backpack, so users will benefit from improved object identification and AI analysis, interaction with nearby devices, and contextual information. The flowchart shows how the backpack and its data channel communicate with computers and cloud servers. It is also theoretically possible to check supermarket prices and plan evening activities.

It is worth noting that the existence of a patent does not mean the speed of release of the device described in it. Large tech companies register thousands of patents every year, and at best, only a few of them reach the market. This Microsoft patent is mostly talking about the usefulness of digital assistants outside the home, and this backpack demonstrates the direction of thought.

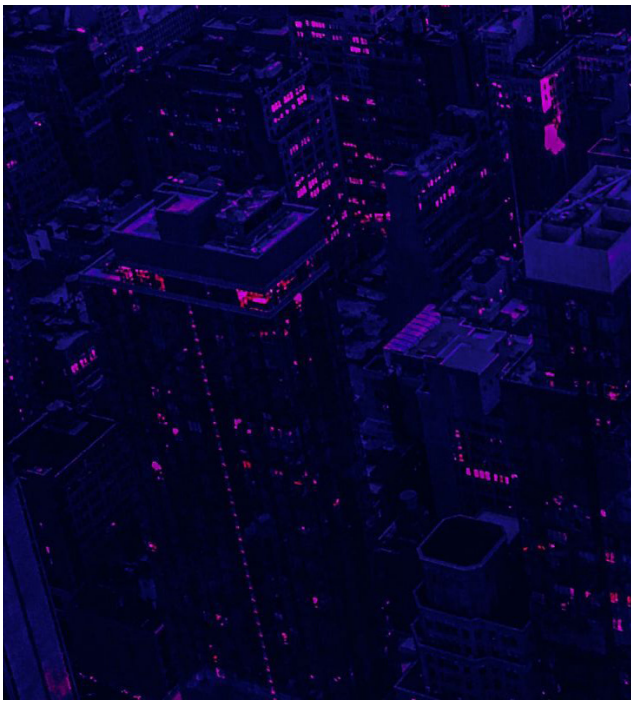


CYBER ASSETS INCREASED BY 133% COMPARED TO 2022

A recent report by JupiterOne analysed cloud access for security leaders. The study found that the number of cyber assets increased by 133% over the year, from an average of 165,000 in 2022 to 393,419 in 2023. Organisations also saw a 589% increase in the number of security vulnerabilities, or unpatched findings, indicating a snowball effect as the number of assets more than doubled.

The number of security vulnerabilities did not increase in direct proportion to the number of assets, which may be due to an actual increase in the number of unpatched vulnerabilities and the introduction of new technologies to detect these vulnerabilities.

Medium-sized organisations with 50 to 499 employees were the most common in building security with the largest number of aggregated data sources. On average, large organisations had 2,011 assets per employee, small organisations had 681, and medium-sized organisations had 489. Medium-sized organisations had the lowest ratio of assets per employee.



OTHER FINDINGS OF THE REPORT

A COMMON UNDERSTANDING OF CYBERSPACE IS CRUCIAL

Security professionals are not omniscient. Visibility of cross-system connections is only good if data sets are integrated and correlated. The average security team correlates 8.67 security data sources to obtain a single cyber intelligence. A single cyber intelligence is essential if one wants to effectively defend the cloud attack surface. However, it can be difficult for teams to justify the need to access data from systems owned or managed by other teams.

CYBER ASSETS ARE BUSINESS ASSETS

Everyone knows that a modern business cannot function, let alone succeed, without its cyber assets, whether in the cloud or in the physical environment. Yet security services have long struggled to convince business leaders of the value of cyber assets. Understanding that the average asset will be worth $17,711 in 2023 may not help security teams get a sufficient budget. However, it is the beginning of a journey to quantify the value of cyber assets.

THE MODERN ATTACK SURFACE IS DISTRIBUTED

In 2023, security professionals will be responsible for an average of 334 unique cloud service provider (CSP) accounts across all organisations of all sizes, or an average of 225 and 559 unique accounts in large and medium-sized organisations, respectively. Distributed cloud architecture techniques create resilience in an era of devastating ransomware attacks. However, the rapid growth of distributed cloud architectures has led to unprecedented complexity for cybersecurity teams, who must contend with more assets, less CSP standardisation, and the need for a common cyber understanding.

TOYOTA IN ITALY IS EMBARRASSED BY DATA BREACH

At the end of March 2023, Toyota Italy reported a confidential data leak that had been going on for more than a year. This resulted in the disclosure of confidential information of Toyota customers. The data was obtained from the Salesforce Marketing Cloud (a provider of software and services for digital marketing automation and analytics) and the Mapbox API (used to request mapping data).

The Italian company Toyota is a major car manufacturer, selling between 71,000 and 91,000 cars a year.

This latest example of corporate data disclosure shows that Toyota needs to do much more to ensure privacy security. This is according to Mark Scheinman, senior director of data management products at Securiti, who outlined the weaknesses to Digital Journal.

Shainman began by describing the areas affected by the automakers' unsafe data practices: "Toyota's customer phone numbers and email addresses are among the confidential information exposed, and this can lead to fines, lawsuits, reputational damage, financial losses and other serious consequences for the brand."

Shainman also notes: "The main long-term consequence of a data breach caused by unauthorised disclosure may well be the loss of customer confidence, which can lead to catastrophic business losses."

As for other consequences, Shainman is blunt: "For the security of customer data and for regulatory reasons, businesses must maintain and implement comprehensive security, privacy and compliance programmes."

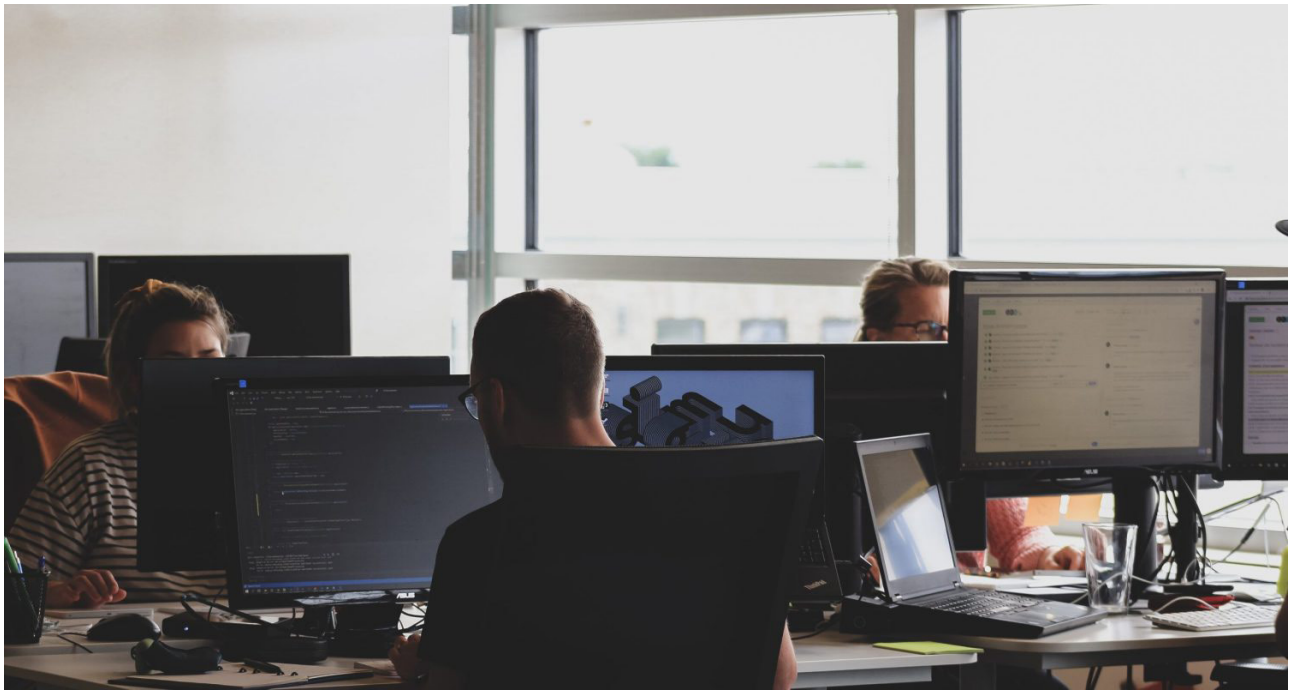
The issue also has legal implications, as Shainman notes: "This breach falls under the General Data Protection Regulation (GDPR), which sets out laws on data protection and privacy. Serious violations can result in a fine of up to €20 million or 4% of the company's annual revenue for the previous year, whichever is greater. Thus, the fines can be huge for companies like Toyota if they are found guilty of negligence."

Not all breaches of the GDPR result in fines. Supervisory authorities can take a number of other actions, including:

- issuing warnings and reprimands
- imposing a temporary or permanent ban on data processing
- ordering the correction, restriction or erasure of data
- Suspension of data transfers to third countries.

In terms of preventative measures for corporate consideration, Shainman states: "Large companies with millions of customers around the world need to continuously assess data breaches to gain real-time insight into the threats they face, ensure they are deploying the right countermeasures, and understand what obligations different regulations impose on them in different regions."

IS INVESTING IN CYBERSECURITY A COST-EFFECTIVE MOVE?



With the biggest cost-of-living crisis in decades, the threat of recession and an unprecedented energy crisis looming, organisations of all sizes are scrambling to find ways to cut costs and save money.

While there are any number of measures that organisations can take in this regard - from the small, in the form of moving people to telecommuting to save on energy, to more drastic measures such as layoffs - the effect is mixed at best.

However, there is a measure that consistently saves organisations money, and that is investing in a proper cybersecurity solution," says JP Perez-Echegoien, CTO of Onapsistells Digital Journal.

In some ways, this may seem counterintuitive, explains Perez-Echegoien. By this he means that cybersecurity looks like "an additional cost that an organisation might not have to deal with".

He adds: "It's really an investment that can pay off in spades. Because the best cybersecurity solutions not only protect organisations from the threat of cyberattacks, but also help mitigate the damage if they do occur."

Pérez-Echegoien adds: "Ironically, the same economic pressures that are forcing organisations to look for ways to cut costs are also making having the right cybersecurity solution in place more important than ever."

SPIKE IN CYBERCRIME DUE TO RISING COST OF LIVING

The cost of living crisis has led to a new surge in cybercrime. For example, in the two weeks leading up to August 2022, the National Cyber Security Centre received more than 1,500 reports of fraudulent phishing emails posing as notifications of electricity discounts from Ofgem.

According to Pérez-Echegoien, this is just one example of the attacks used by cybercriminals. There are many others. This comes at a time when many

organisations are under pressure to cut costs. In this environment, it is more likely that such social engineering attacks will succeed and lead to a breach.

Pérez-Echegoien explains that it is hardly surprising that recently published official statistics show that around 81% of UK organisations experienced at least one successful cyber attack in 2022. In addition, 83% believe that the likelihood of a cyberattack is increasing over the next 12 months.

In addition, Palo Alto Unit42 predicts that this year more people will commit cybercrime for financial gain, available tools will become more widespread, and vulnerabilities will be easier to exploit. The intersection of these factors will eventually lead to an increase in the number of cybersecurity incidents.

THE COST OF CYBERCRIME

Cyber-attacks can cost organisations serious money, says Pérez-Echegoien, noting: "According to IBM, the average cost of a data breach in the UK in 2022 was US$5.05 million, making it one of the five most expensive countries for data breaches globally. And that's not to mention the long-term damage that can be done to a company's credibility and reputation."

The risks are obvious: "Even a business disruption can be devastating. Think about it: can your organisation afford the 22 days it takes on average to get back up and running after a breach? This effect can be even more severe if the breach affects business-critical applications. It's no wonder that half of small businesses that suffer a cyberattack collapse within six months."

Pérez-Echegoien adds: "It's also worth remembering that, given the percentage of UK businesses that will be victims of cybercrime in 2022, cyberattacks should be treated as something that will happen, not something that might happen."

INVESTING IN THE RIGHT CYBERSECURITY SOLUTION

This makes investing in the right cybersecurity solution all the more important, says Pérez-Echegoien. He explains: "While it may seem like a big expense now, the cost of mitigating and recovering from attacks will likely far outweigh any initial expenditure on technical controls and assessments."

Pérez-Echegoien continues:

"A good cybersecurity solution will not only alert you to emerging threats and proactively work to protect against them, but will also provide you with the best possible proactive response in the event of a breach. The quicker and more efficiently you can do this, the lesser the impact of a breach.

What's more, cybersecurity solutions will be able to continuously detect, assess, remediate and report vulnerabilities in your organisation's software and network. Ideally, the work should start with identifying and remediating known vulnerabilities. Cybercriminals are constantly looking for ways to infiltrate an organisation, and not addressing vulnerabilities is like leaving a door or window open for them."

A SMALL BLOW CAN HELP YOU AVOID A BIG BLOW

Pérez-Echegoyen concluded: "Ultimately, it should be clear that cybercrime attacks are not going to diminish any time soon. Nor will they become less expensive to eliminate. So even companies that are desperate to cut costs should consider investing in a good cybersecurity solution a must."

SPAM WRITTEN BY ARTIFICIAL INTELLIGENCE MAY SOON FLOOD EMAILS

Every day, messages from Nigerian princes, miracle cure salesmen, and win-win investment advertisers clutter inboxes. Improvements in spam filters only inspire new methods of breaking through defences.

Now, the arms race between spam blockers and spam senders may be heating up with the advent of a new weapon: generative artificial intelligence. Thanks to recent advances in artificial intelligence made famous by ChatGPT, spammers may have new tools to bypass filters, grab people's attention, and convince them to click, buy, or provide personal information.

As the director of the Advancing Human and Machine Reasoning lab at the University of South Florida, I conduct research at the intersection of artificial intelligence, natural language processing, and human reasoning. I've been studying how artificial intelligence can learn individual preferences, beliefs, and quirks.

This can be used to better understand how to interact with people, help them learn, or give them useful advice. But it also means that you should be wary of smarter spam that knows your weaknesses and can use them against you.

SO, WHAT IS SPAM?

Spam is defined as unsolicited commercial emails sent by an unknown person. Sometimes the term is extended to include text messages, direct messages on social media, and fake product reviews. Spammers want to get you to take action: buy something, click on phishing links, install malware, or change your views.

Spam is profitable. A single email campaign can generate $1,000 in revenue in just a few hours and costs spammers only a few dollars - apart from the initial setup. A pharmaceutical company's online spam campaign can generate about $7,000 a day.

Legitimate advertisers also want to push you to take action - buying their products, taking surveys, signing up for newsletters - but while an email from a marketer may include a link to the company's website

and an unsubscribe option in accordance with federal regulations, a spam email may not.

Spammers also don't have access to mailing lists that users have subscribed to. Instead, spammers use counter-intuitive strategies, such as the Nigerian prince scam, in which an actual prince claims to need your help to unlock an absurd amount of money, promising a handsome reward. Experienced digital natives immediately reject such requests, but the absurdity of the request may actually select for naivety or old age, filtering out those most likely to fall for the scam.

However, advances in artificial intelligence mean that spammers may not have to rely on such approaches. AI may allow them to target individuals and make their messages more persuasive based on available information, such as social media posts.

THE FUTURE OF SPAM WITH THE HELP OF ARTIFICIAL INTELLIGENCE

Most likely, you've heard of advances in generative large language models (LLMs) such as ChatGPT. The task they perform is deceptively simple: given a sequence of text, predict which token - think of it as part of a word - comes next. Then predict which token comes after it. And so on, over and over again.

Somehow, training on this task alone, with enough text at a large enough LLM, seems to be enough to give these models the ability to perform surprisingly well on a variety of other tasks.

There are already many uses for this technology that demonstrate its ability to quickly adapt to and learn from people. For example, LLMs can write full-fledged emails in your style with just a few examples of how you write. There's a classic example - from more than a decade ago - of Target finding out a customer was pregnant before her father knew.

Both spammers and marketers stand to gain if they can predict more about people from less data. Given your LinkedIn page, a few messages, and a couple of profile pictures, spammers armed with an LLM can make fairly accurate assumptions about your political views, marital status, or life priorities.

Our research has shown that LLMs can be used to predict which word a person will say next, with accuracy that far outperforms other AI approaches, in a word generation task called the semantic fluency task. We have also shown that LLMs can take certain types of questions from reasoning tests and predict how humans will answer the question. This suggests that LLMs already have some knowledge of what typical human reasoning abilities look like.

If spammers manage to get past the initial filters and get you to read an email, click on a link, or even start a conversation, their ability to apply individual persuasion increases dramatically. This is where LLMs can be a game changer. Initial results show that a Master of Laws can be used to make a persuasive argument on topics ranging from politics to healthcare.

GOOD FOR THE COMMON MAN

AI, however, does not favour one side or the other. Spam filters also stand to benefit from AI advances, allowing them to erect new barriers to unwanted emails.

Spammers often try to trick filters with special characters, misspelled words, or hidden text, relying on the human tendency to forgive small textual anomalies, such as c1îck h.ere n0w. But as AI becomes more aware of spam, filters will be able to better identify and block unwanted spam and possibly even let the right spam through. For example, marketing emails that you have explicitly signed up for. Imagine a filter that predicts whether you want to read an email before you even read it.

Despite the growing concerns about AI, as evidenced by Tesla, SpaceX, and Twitter CEO Elon Musk, Apple founder Steve Wozniak, and other tech leaders calling for a halt to AI development, progress in this technology can bring many benefits. AI can help us understand how weaknesses in human thinking can be exploited by adversaries and come up with ways to counteract malicious intent.

All new technologies can lead to both wonder and danger. The difference lies in who creates and controls the tools and how they are used.

IMPRESSUM

“DIGITAL WORLD”

Hiisku Roman
00950 Helsinki, Vartiokyläntie 11
Tel: + 358407352082
e-mail: hiisku.roman@gmail.com