OCTOBER 2024 | ISSUE 51

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the October edition of our newsletter – our 51st issue, and we couldn't be more excited to share it with you!

It is dark, cold and wet in London now, and to top it all off, I lost my voice last week. No, it wasn't from celebrating the 50th edition (though that was pretty epic)! Thankfully, my voice is coming back, albeit quite a bit deeper – much to the amusement of my (ex) friends. But don't worry, it should be back to normal soon!

Last month, to celebrate our 50th edition, we hosted a special "Wisdom of the Crowd!" event for our Zyber Global community. The 30-minute session was a hit, featuring an engaging 15-minute presentation by Yolanda Van Setten (Managing Director, Cum Sensu Consultancy) on "The NIS2 Directive – Will This Forever End Cybercrime?" This was followed by an insightful Q&A session with fantastic contributions from our members.

Due to the overwhelming success, we're doing it again! Join us for our next "Wisdom of the Crowd!" session on October 3rd at 3 pm BST, featuring the dynamic Graham Butler. As the Chairman and Founder of Bitek Global Ltd, Graham will share his expertise on "The Truth About OTTs and Their Impact on Carriers Today & Tomorrow." With over 40 years of experience in combating fraud and pioneering internet voice services.

Join Zoom - Meeting ID: 826 6100 3308; Passcode: 614324
This is an event you won't want to miss!

Let us know what topics you would like to see discussed in future newsletters.

Stay safe and secure,

Esther George, CEO Zyber Global Centre

Graham Butler

This Month's Features

1 Wisdom of the Crowd
"The Truth About OTTs and Their Impact on Carriers Today & Tomorrow."

2 Zyber Focus Article
Could AI Lead to a New Era of Miscarriages of Justice? What the Post Office Scandal Teaches Us

3 Zyber News
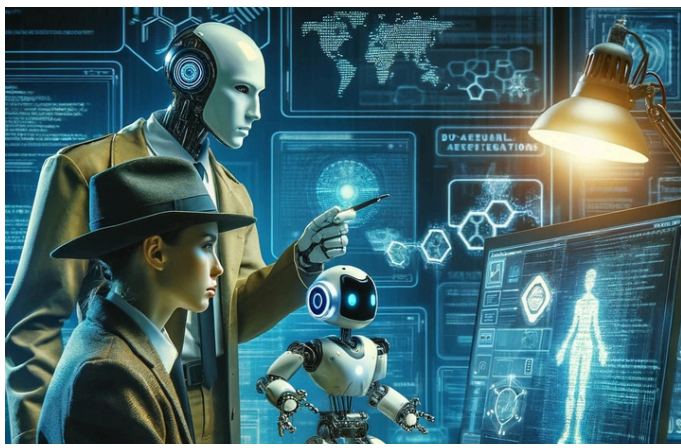We have a roundup of the latest international cybercrime news.

4 Zyber Global Events Information
A focus on forums/conferences around the world.

Zyber Focus Article

Could AI Lead to a New Era of Miscarriages of Justice? What the Post Office Scandal Teaches Us

*by Esther George and
the Zyber Global Research Team*

Last month, to celebrate the 50th edition of the Zyber Global Newsletter, we featured an outstanding article by Yolanda Van Setten (Managing Director, Cum Sensu Consultancy) titled "To Trust or Not to Trust: The Ultimate Question When Dealing with Artificial Intelligence."

This piece resonated with our readers, sparking a high demand for more AI-related content. Listening to your feedback, I thought it would be the right time to voice my concern that our reliance on AI might lead us into a justice crisis even larger than the infamous Post Office Horizon scandal, where 736 sub-postmasters were wrongfully prosecuted.

In response, I teamed up with the Zyber Global research team to dive into this pressing issue, resulting in our latest article, "Could AI Lead to a New Era of Miscarriages of Justice? What the Post Office Scandal Teaches Us." This article serves as a follow-up to my commentary on the Horizon case titled "The Horizon Case – UK's most widespread miscarriage of justice," Featured in the May 2021 newsletter and blog post dated 6 May 2021.

We hope it brings fresh insights into the potential pitfalls of AI in our justice system.

Learning from Horizon's Mistakes

The potential use of AI in law enforcement could lead to miscarriages of justice on a scale like the infamous Post Office Horizon scandal if not carefully managed. The Horizon case serves as a chilling reminder of the dangers of over-relying on technology and assuming its infallibility; faulty software falsely accused hundreds of sub-postmasters of theft and fraud, resulting in wrongful prosecutions and devastating consequences. This case clearly illustrates that blind trust in technology, without transparency or oversight, can have life-altering impacts.

If law enforcement treats AI as an unquestionable source of truth, innocent people could face wrongful accusations based on flawed algorithms or biased data, risking systemic injustices. Just as the Post Office's refusal to acknowledge software errors led to countless ruined lives, a similar lack of scrutiny in AI could lead to unfair prosecutions and a deep erosion of public trust in our justice system.

To prevent AI from becoming another instrument of injustice, we must ensure its use in law enforcement is guided by transparency, rigorous oversight, and human judgment. The Horizon scandal should serve as a powerful lesson, urging us to establish robust safeguards and accountability measures to prevent a repeat of such devastating consequences.

Presumption of Infallibility

In the Horizon case, the Post Office treated the Horizon software as infallible, despite evidence of flaws. This led to the assumption that any discrepancies in accounting were due to theft by sub-postmasters, not the system itself.

When looking at AI we need to be careful that law enforcement agencies and the justice system does not similarly treat AI as a "black box" authority, presuming its outputs are always correct. This risks ignoring potential errors or biases in the system. According to the Royal Society report "Machine learning: the power and promise of computers that learn by example," AI systems can often be opaque, making it hard to understand how decisions are made 【Royal Society, 2017】.

There are already many examples of AI hallucinating, making mistakes or just making things up. For example, before it was pulled Meta's Galactica AI was criticized as 'Dangerous' for Science as its answers can be incorrect but written in a way that is...

Read more here: https://zyberglobal.com/blog?blogcategory=Article

Zyber News Roundup

LinkedIn is training AI on you — unless you opt out with this setting

LinkedIn recently introduced a new data privacy setting that allows it to use users' posts, articles, and videos to train its artificial intelligence by default, catching many by surprise. Users who wish to opt out must manually change this setting, but LinkedIn has already begun using existing data, and there's no way to retroactively prevent the company from training its AI with previously shared content. This move has sparked concerns about privacy and transparency, as some users feel their contributions to LinkedIn's AI development were neither fairly valued nor clearly communicated...

Read more:
https://www.washingtonpost.com/technology/2024/09/23/linkedin-training-ai-setting-opt-out/

US moves to ban import of certain connected vehicle parts from China and Russia

The White House announced plans to ban the import of certain auto parts made in China and Russia, following a U.S. Commerce Department probe into potential national security risks associated with connected vehicle components. The import restrictions will focus on two categories: vehicle connectivity systems, which include hardware and software used for wireless communication (e.g., Bluetooth, Wi-Fi, cellular), and automated driving systems, which enable vehicles to navigate autonomously. These restrictions will apply to components designed, developed, manufactured...

Read more:
https://siliconangle.com/2024/09/23/us-moves-ban-import-certain-connected-vehicle-parts-china-russia/

Kiwis lost $6.8 million to cybercrime last quarter

Kiwis reported $6.8 million in cybercrime losses during the second quarter of 2024, with the National Cyber Security Centre (NCSC) revealing that most of this amount stemmed from 11 incidents, each exceeding $100,000, totaling $5.5 million. Despite a 22% drop in the total number of reported cases compared to the first quarter, financial losses remained significant, with unauthorized access accounting for $3.6 million in damages. This type of incident was highlighted as particularly serious, as attackers often remain undetected within systems, leading to more severe consequences...

Read more:
https://www.1news.co.nz/2024/09/18/kiwis-lost-68-million-to-cybercrime-last-quarter/

Schools overpay ransomware demands – study

A global study on ransomware's impact revealed that over half of schools paid more than the initial ransom demand, highlighting the financial strain cybercrime places on the education sector. Despite a decrease in ransomware attacks on educational institutions from 80% in 2023 to 63% in 2024, median ransom payments remained high, averaging $6.6 million for schools and $4.4 million for higher education institutions. The survey, conducted by Sophos across 14 countries, included responses from over 600 education sector representatives...

Read more:
https://www.theeducatoronline.com/k12/news/schools-overpay-ransomware-demands--study/285665

Zyber Global Events
Information Page

GLOBAL CYBERSECURITY EVENTS

Cybertech Europe | October 8-9, 2024 | Rome, Italy

Both a conference and an exhibition, presenting cutting-edge solutions from diverse companies. The event will host a lineup of esteemed speakers, including senior government officials, C-level executives, and industry leaders from Europe and across the globe. Cybertech's conferences and exhibitions have become a must for building business connections and staying up to date on the latest technological advancements, challenges, and solutions.

The event unites thought leaders, innovators, and cybersecurity enthusiasts from Europe and globally, exploring cutting-edge solutions, emerging challenges, and the latest technological breakthroughs.

SEE MORE >

RISK London 2024 | October 9-10, 2024 | ExCel, London, UK

To thrive in today's competitive landscape, organisations must integrate data and processes across the enterprise, gaining a holistic view that enables streamlined decision-making, greater efficiency, and an enhanced customer experience.

GRC World Forums (#RISK, PrivSec, GRC Connect Series, #RISK A.I. Series and all associated brands) aim to bring you the best information and insights from the data protection, privacy, security.

SEE MORE >

CYBERGOV - National Cyber Security Strategy Confex | October 15, 2024 | Victoria Park Plaza Hotel, London, UK

The new National Cyber Security Strategy sets out the means by which the UK can continue to play a leading role in shaping the cyber space of today and tomorrow. A cyber space that not only supports innovation, collaboration, engagement and interaction, but defends the UK and its allies against the growing threat of cyber criminals, subversive organisations and hostile nation-states.

The cyber realm of today is an increasingly complex one in which it is possible to affect the outcome of elections, disrupt CNI supply chains, and compromise elected members of Parliament purely through the force of cyber.

The Annual CyberGov 2022 Conference and Exhibition is a platform to address key government cybersecurity issues.

SEE MORE >

Zyber Global Online Events

Our Online Courses with INsig2
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/

Courses per sectors

Legal Entities
Customized courses for legal entities: judges, lawyers and public prosecutors.
Explore deeper aspects of digital forensics and the forensic value of evidence while collecting, processing, and presenting digital evidence in criminal and administrative proceedings.

Law Enforcement
Customized courses for law enforcement officials: First responders, forensic investigators and analysts.
Delve into procedures, techniques, and tools used in digital forensic analysis and how to apply them in forensic investigations.

Private Sector Corporations and Small Businesses.
Customized courses for industry professionals working in the private sector; to help them understand the value and the need for digital forensic, and its implications in a corporate environment.

Course Structure

*FULL-TEXT REVISION

*QUIZ AFTER EACH CHAPTER

*CASE-STUDY AFTER FINAL EXAM

At the end of each course, you will be issued a completion e-certificate which is immediately printable for your records. The number of **CPD** (Continuing Professional Development), **CPE** (Continuing Professional Education), and/or **CLE** (Continuing Legal Education) points will depend on the course.

DISCOUNTS

Special discount for groups of 10+ participants on all courses. The bigger the group, the bigger the discount.

BUNDLES

Stay on your forensic digital learning path and get the most from your e-learning experience by using course bundles.

CLICK HERE

FREE COURSE ON PASSWORD MANAGEMENT

This covers different lock security methods, guidelines on securely storing your passwords, various password managers and how to use them.
CLICK HERE