Zyber Global
INDEPENDENT CYBERCRIME, CYBERSECURITY, DIGITAL EVIDENCE, LEADERSHIP AND BUSINESS CONSULTANCY
www.zyberglobal.com

FEBRUARY 2025 | ISSUE 55

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the February 2025 edition of the Zyber Global newsletter!

We kicked off the year with a bang, hosting our first Wisdom of the Crowd webinar of 2025, "AI Technology: A Cybercrime View." It was an insightful and thought-provoking session led by expert Lawrence McEwen, diving into AI's role in cybercrime. If you missed it, our next Wisdom of the Crowd webinar is coming up in March, so stay tuned!

January also took me on a whirlwind tour of the Gulf, escaping London's winter for the warmth of Bahrain, Saudi Arabia, and Kuwait. I had the privilege of tutoring prosecutors on a cybercrime training course in Bahrain, an experience I thoroughly enjoyed. With Saudi Arabia just a short drive away, I couldn't resist crossing the border for a quick visit to Al Khobar, I then hopped over to Kuwait—completing my travels so that I can now say I have been to all six Gulf countries! How many have you visited? Now, I'm debating my next personal travel challenge—should I aim to visit every country in the European Union or explore Eastern Europe? What's your vote?

As we step into February, we're looking ahead to another exciting month in the world of cybersecurity. From the latest AI developments to critical cybercrime trends, we'll be keeping you informed on the key issues shaping our industry. We'd love to hear your thoughts, so feel free to share your insights and join the conversation.

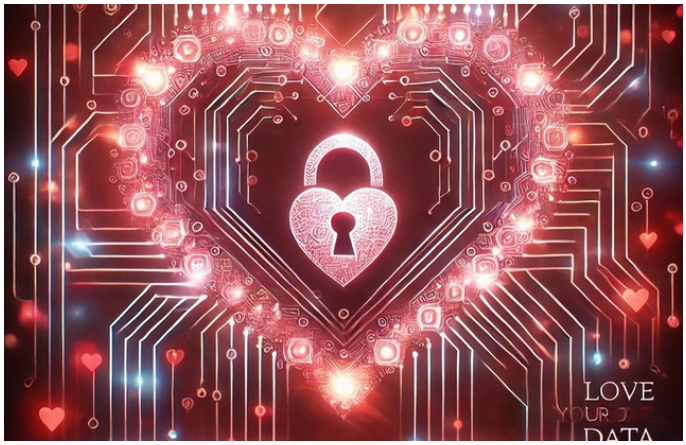
Until next time—stay cyber-aware and keep exploring!

Esther George, CEO Zyber Global Centre

This Month's Features

1. **Zyber Focus Article**
   Love Your Data
2. **Zyber News**
   We have a roundup of the latest international cybercrime news.
3. **Zyber Global Events Information**
   A focus on forums/conferences around the world.

Zyber Global – Tel: 07426719579 Privacy Policy Register
To unsubscribe contact us at office@zyberglobal.com



Zyber Focus Article

Love Your Data

By Esther George, CEO Zyber Global Centre

February is the month of love, a time when we celebrate meaningful relationships and the connections that matter most. But in today's digital world, love isn't just about people—it's about protecting the data that keeps our personal and professional relationships safe. Cybercriminals are constantly finding new ways to exploit trust, whether through phishing scams, ransomware attacks, or social engineering tactics. As we embrace technology to stay connected, it's more important than ever to safeguard our data and ensure that our digital relationships remain built on trust, not deception.

The Rise of Cybercrime in a Connected World
With more people working remotely and socialising online, cybercriminals have more opportunities to manipulate digital trust. Phishing scams have become increasingly sophisticated, often disguised as urgent emails from hospitals, government agencies, or well-known companies. These scams trick victims into clicking malicious links or revealing personal information. Meanwhile, ransomware attacks—where hackers lock vital data and demand a ransom for its release—continue to pose a serious threat to businesses and individuals. The reality is clear: our growing digital dependence comes with increased risks, making cybersecurity a necessity, not an option.

This Valentine's Day, show some love to your data. Just as you protect the people closest to you, protect the information that keeps your digital world secure. By staying informed and taking proactive security measures, you can build stronger, safer connections—both online and offline.

Protecting Your Digital Connections: 5 Practical Steps
Just as we protect our personal relationships, we must take steps to safeguard our online interactions. Here are some simple but effective ways to stay secure:

1. Be Wary of Phishing Scams
🚨 Red flags to watch for:
- Generic greetings like Dear Customer instead of your name.
- Unexpected emails (or SMS text messages) from banks, government agencies, or parcel delivery services.
- Urgent requests asking you to act now by clicking a link or providing sensitive details.

🔎 What to do:
- Never click on suspicious links or open attachments from unknown sources.
- Verify messages by contacting the sender directly through official channels.
- If you are based in England, Wales or Northern Ireland report phishing emails to Action Fraud or forward them to report@phishing.gov.uk

2. Secure Your Accounts with Strong Authentication
💡 Best practices:
- Use unique, complex passwords for each account (consider a password manager).
- Enable Multi-Factor Authentication (MFA) to add an extra layer of security.
- Change passwords regularly, especially after a data breach.

3. Protect Your Devices and Networks
🔒 How to stay safe:
- Keep your software, apps, and antivirus protection up to date.
- Avoid using public Wi-Fi for sensitive transactions—use a VPN (Virtual Private Network) instead.
- Lock devices with strong PINs or biometric authentication (fingerprint, facial recognition).

4. Be Mindful of What You Share Online...

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

Zyber News Roundup

Argentina approves the "Federal Plan for the Prevention of Cybercrime and Strategic Management of Cybersecurity (2025 – 2027)"

Argentina has approved the Federal Plan for the Prevention of Cybercrime and Strategic Management of Cybersecurity (2025-2027) through Resolution 72/2025, published by the Ministry of Security on 15 January 2025. The plan aims to enhance the country's ability to prevent, detect, and investigate cybercrimes while reinforcing the security of digital infrastructure. It seeks to coordinate efforts between national and provincial governments to address...

Read more:
https://allende.com/en/privacy-and-cybersecurity/argentina-approves-the-federal-plan-for-the-prevention-of-cybercrime-and-strategic-management-of-cybersecurity-2025-2027-01-21-2025/

Majority of Dutch citizens support social media ban for children under 16

A recent study, the Nationaal Social Media Onderzoek 2025, found that 57 percent of Dutch citizens now support raising the minimum age for social media use from 13 to 16. This marks a significant shift in public opinion, with many believing that young teenagers are not yet equipped to handle the potential harms of excessive social media use. Neil van der Veer, director of research firm Newcom, highlighted that the data shows a clear link between increased social media consumption and declining happiness among young users.

Read more:
https://nltimes.nl/2025/01/25/majority-dutch-citizens-support-social-media-ban-children-16

Privacy Commissioner warns the 'John Smiths' of the world can acquire 'digital doppelgangers'

Australia's privacy commissioner, Karly Kind, has found that government agencies failed to adequately protect data related to "digital doppelgangers" – individuals who share the same name and date of birth, leading to their records being mistakenly merged. One such case involved a complainant, identified as "ATQ," whose healthcare records became intertwined with those of three other individuals, resulting in inaccurate medical history and financial complications. ATQ was wrongly warned they were nearing Medicare payment caps due to charges belonging to their doppelgangers. Despite efforts to prevent further data mix-ups...

Read more:
https://www.theregister.com/2025/02/03/australia_digital_doppelgangers_privacy_award/

FBI Strikes 'The Manipulaters' in Major Cyber Crackdown, 17 Million Americans Affected

The global fight against cybercrime is escalating as law enforcement agencies deploy advanced tactics to dismantle criminal networks. The U.S. Department of Justice has confirmed that Operation Talent, led by the FBI in collaboration with international agencies, has impacted 17 million Americans. A key target of the crackdown was The Manipulaters, a shadowy cybercrime group, and the notorious dark web marketplace Cracked, which facilitated the sale of stolen credentials, hacking tools, and malware services. With over four million users and illicit earnings of Rs 33.2 crore, Cracked played a major role...

Read more:
https://www.the420.in/fbi-strikes-the-manipulaters-in-major-cyber-crackdown-17-million-americans-affected/

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

SEE MORE >

Africa Tech Summit Nairobi 2025 | 12- 13 February 2025 | Nairobi, Kenya

Africa Tech Summit Nairobi connects tech leaders from the African ecosystem and international players under one roof. Network with key stakeholders including tech corporates, mobile operators, fintechs, DeFi & crypto ventures, investors, leading start-ups, regulators and industry stakeholders driving business and investment forward.

Following a record breaking 2024, the seventh edition will convene in Nairobi, Kenya 2025.

SEE MORE >

SmartTech Asia | 13- 14 February 2025 | Mumbai, India

SmartTech Asia Expo represents AI, IoT, RFID, biometrics, barcodes, digital payment, smart cards technologies. The show has seen unprecedented success in the past two decades.

The event focusing on pioneering solutions in AI, IoT, RFID ,biometrics, barcodes, digital payment, smart cards technologies will present unmatched networking opportunities and unlock ample business opportunities.

SEE MORE >

Digital Transformation Summit 2025 | 20 February 2025 | Kuala Lumpur, Malaysia

The Digital Transformation Summit unites C-Level Executives and Technology leaders to explore AI, Web 3.0, IoT, Quantum Computing, Cyber Security, and other 4IR technologies for impactful change.

Digital Transformation is a requisite on the corporate agenda. It is fundamentally changing how businesses operate and deliver value to customers. The agenda at the Digital Transformation Summit has been meticulously crafted to identify critical approaches needed to make informed business decisions, improve operational efficiency, and drive digital culture forward.

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