Zyber Global

APRIL 2024 | ISSUE 45

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the April edition of Zyber Global Newsletter, the 45th edition! Dive into the latest and most thrilling developments in the dynamic realm of cybersecurity with us!

March unfolded as a chapter of premieres in my journey diary, set against the vibrant backdrop of Southeast Asia. I made my debut in the bustling streets of Thailand; navigated the rich tapestry of Vietnam; and wandered through the historical echoes of Cambodia. Each land left a stamp of warmth in my heart, a promise of return lingering in the air. Back in London, the chill and drizzle were constants, yet here I was, basking in the sultry embrace of temperatures soaring between 32 to 35 degrees. The weather was nothing short of splendid, a stark contrast to Hanoi's rainy 20s, which playfully mirrored the London skies. Nostalgia, however, had to take a rain check, as Bangkok summoned me back to its sizzling climes with no time to spare for homesickness

The highlights of my trip were two meetings that I had. The first was in Bangkok with Narin Phetthong CHFI, CCCE Director of Transaction Monitoring and Cooperation, Anti Money Laundering Office Thailand; it was great to spend some time with him discussing issues related to cybercrime and money laundering in South East Asia.
The second meeting was in Cambodia with Seila Samleang, the Executive Director of APLE Cambodia. APLE Cambodia is a dedicated NGO, working tirelessly to create a safer community where children are protected from sexual abuse and exploitation. Their mission is to tackle all kinds of child sexual abuse by promoting prevention, ensuring protection, and enhancing the enforcement of laws. APLE also helps to train law enforcement and it was really helpful to discuss both the training and protection of children.

Back in the London groove, I found myself in a brisk dance with the 10 to 11 celsius weather. But hey, silver linings - the rainclouds have taken a hiatus today!

Looking ahead, I'm thrilled at the prospect of spotlighting the inspiring Narin Phetthong and Seila Samleang in upcoming editions of the newsletter. Their stories are sure to be a beacon of enlightenment and a splash of colour on our pages. Stay tuned!

Lastly, in April, I will be presenting at the Insig2 Data Focus 2024 conference. The conference will take place on the 9th of April in Zagreb, Croatia. This is a great conference to attend as there is so much to share. You can register here https://insig2.com/en/data-focus/data-focus-2023/ Do arrange to attend and let's meet up at the conference.

Remember to stay vigilant and informed as we continue to navigate the ever-evolving landscape of cybersecurity.

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Focus Article
The Reality of Cyber Flashing - Arsha Gosine, Head of Research, ZGC.

Zyber News
A roundup of the latest international cybercrime news.

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

Zyber Focus Article

The Reality of Cyber Flashing

Arsha Gosine, Head of Research,ZGC

'Whilst the online world offers important opportunities to share ideas and engage with one another, it has also increased the scope for abuse and harm. Reports of cyberflashing are rising worryingly. This offence will close loopholes in the existing law and ensure that cyberflashing is treated as seriously as in-person flashing'.

Professor Penney Lewis, Criminal Law Commissioner
Law Commission, UK

Cybercrime is multifaceted. There are so many physical criminal areas where there is now a cybercrime equivalent. Cyber based abuses include deepfake pornography, revenge porn, and upskirting. Laws have been enacted to cover those crimes. However, a new criminal activity has emerged - cyber flashing.

So, what is cyber-flashing? Cyber-flashing involves sending obscene pictures to strangers online, via social media or dating apps and often through the use of data sharing apps such as Bluetooth or Airdrop.

An appropriately equipped device can seek out any active peers within about 10 meters. The harassing individual can make an initial connection with any device that is open to all users. A photo can then be sent with a preview of the photo being shown to the device's owner at the same time as a request to allow the connection. Therefore, the harassment (the "flashing") can occur before a specific connection is authorized. So even if one rejects the photo, one is still forced into viewing the image.

The first mainstream coinage of the term occurred around 13 August 2015, after a female commuter was 'AirDropped' two pictures of a penis. She declined the photos and reported the matter to the British Transport Police. As she had declined the photos, insufficient data was recorded by the receiving phone and there was not enough evidence to build a case.

International Legislation

In New South Wales, Australia, The Crimes Amendment (Intimate Images) Act 2017 was implemented to make it an offense to "intentionally record or distribute, or threaten to record or distribute, an intimate image of a person without their consent". This legislation would cover cyber-flashing by its prohibition on distributing intimate images without consent.

In Singapore, cyberflashing, upskirt photography, and revenge porn have been criminalized since May 2019.

UK Legislation

On 13 March 2022, the UK Government announced cyberflashing would be criminalised with perpetrators facing up to two years behind bars under new laws applying to England and Wales.
Cyber-flashing is now an offence in the United Kingdom. Included in the UK Government's landmark Online Safety Act 2023 alongside wide-ranging reforms to keep people safe on the internet, the offence of cyber-flashing came into force on 31 January 2024.
Cyber flashing has been illegal in Scotland since 2010.

CyberFlashing

Cyberflashing is when someone sends sexting materials without permission in chats, gaming apps, or forum groups.

England and Wales - First Prosecution

A registered sex offender from Basildon became the first person in England and Wales to be convicted of cyber-flashing.

On 19 March, Nicholas Hawkes, was sentenced at Southend Crown Court to a total of 66 weeks in prison. He received 52 weeks for the cyberflashing offences and an additional 14 weeks for breaching a previous court order and a suspended sentence was activated. He was also made subject of a restraining order for 10 years, and a Sexual Harm Prevention Order for 15 years.

Using his father's phone on the pretext of making a call to Probation, Nicholas sent unsolicited photos of his erect penis to a 15-year-old girl and a woman on 9 February. The woman took screenshots of the image on WhatsApp and reported Hawkes to Essex Police the same day.

At a remand hearing at Southend Magistrates' Court on Monday, 12 February Hawkes pleaded guilty to two counts of sending a photograph or film of genitals to cause alarm, distress, or humiliation.

Responding to his sentence, Hannah von Dadelzsen, Deputy Chief Crown Prosecutor for CPS East of England, had this to say:
"Cyberflashing is a serious crime which leaves a lasting impact on victims, but all too often it can be dismissed as thoughtless 'banter' or a harmless joke.
"Just as those who commit indecent exposure in the physical world can expect to face the consequences, so too should offenders who commit their crimes online; hiding behind a screen does not hide you from the law".

Read more:
https://zyberglobal.com/blog

Zyber News Roundup

Executives in Japan busted for winning development bids then outsourcing to North Koreans

In Japan, arrest warrants were issued for two executives, a South Korean national named Pak Hyon-il and a Japanese individual, Toshiron Minomo, on charges related to their involvement in a scheme that outsourced IT work to North Korean engineers, potentially without the knowledge or consent of their Japanese customers. The police investigation into these activities, which might have inadvertently supported North Korea's foreign currency acquisition efforts, led to further suspicions of fraudulent financial practices, including falsifying company capital and unemployment benefit fraud, highlighting the complex legal and security implications of such outsourcing practices.

The case underscores broader concerns regarding the hiring of North Korean IT professionals, given the potential for malware risks, cybersecurity threats, and the inadvertent support of North Korea's sanctioned activities, including its nuclear and missile development programs. The U.S. and South Korean governments have previously issued guidance to help businesses avoid unwittingly employing North Korean agents, with the Japanese government also issuing warnings about North Korean IT contractors. These developments reflect the international community's efforts to curb North Korea's access to foreign currency and mitigate cybersecurity risks, emphasizing the need for vigilance and due diligence in international IT contracting.

Read more: https://www.theregister.com/2024/03/28/japan_nk_arrests/

Binance speaks on escape of executive from Nigerian custody

Nadeem Anjarwalla, a senior executive at the global cryptocurrency exchange platform Binance, made a daring escape from lawful custody in Nigeria just a day after the Nigerian government charged him, along with Tigran Gambaryan and Binance, with tax evasion and other criminal offenses. Anjarwalla, holding both British and Kenyan citizenship, reportedly fled Nigeria using a Middle Eastern airline, under the cover of a Kenyan passport. This incident has sparked Binance to engage actively with Nigerian authorities, aiming to address and resolve the situation while prioritizing the safety of its personnel amid these legal challenges.

The case against Binance and its executives represents a significant episode in the global regulatory scrutiny facing cryptocurrency platforms, reflecting broader concerns over the potential misuse of digital currencies for illegal purposes. As Binance navigates these legal challenges in Nigeria, the incident underscores the complexities of operating a global cryptocurrency exchange amid varying international regulatory environments. The case against Binance and its executives represents a significant episode in the global regulatory scrutiny facing cryptocurrency platforms, reflecting broader concerns over the potential misuse of digital currencies for illegal purposes. As Binance navigates these legal challenges in Nigeria, the incident underscores the complexities of operating a global cryptocurrency exchange amid varying international regulatory environments.

Read more: https://www.premiumtimesng.com/business/business-news/680607-exclusive-binance-speaks-on-escape-of-executive-from-nigerian-custody.html

EU launches probe into Meta, Apple and Alphabet under sweeping new tech law

The European Union has initiated an investigation under the Digital Markets Act into Apple, Alphabet, and Meta for potential non-compliance related to "anti-steering rules" and other competitive practices. These investigations target Alphabet and Apple for possibly preventing businesses from directing users to cheaper options outside of app stores and Meta for its "pay or consent" model, which might limit users' choices. This marks the EU's first major action under new tech legislation aimed at curbing the power of major tech companies and ensuring fair competition.

Read more: https://www.cnbc.com/2024/03/25/eu-launches-probe-into-meta-apple-and-alphabet-under-sweeping-new-tech-law.html

Inside Australia's turbocharged battle against hackers

The Australian Signals Directorate (ASD) has significantly enhanced its cyber threat monitoring and intelligence capabilities through a $5 billion threat sharing partnership with Microsoft, described by ASD boss Rachel Noble as a "force multiplier." This collaboration has led to the integration of ASD's own intelligence platform, Cyber Threat Intelligence Sharing (CTIS), with Microsoft's Sentinel threat monitoring software, marking a global first in public-private cybersecurity cooperation. Through this partnership, Australian organizations can confidentially share threat intelligence with the ASD, enabling the agency to better understand and preempt cyber attacks, thereby bolstering the nation's defense against cybercrime.

This initiative not only boosts ASD's ability to detect and warn against potential cyber threats but also empowers Australian businesses to proactively participate in national cybersecurity efforts. This collaborative defense mechanism significantly strengthens Australia's cybersecurity posture, making it a model of effective public-private partnership in combating cyber threats

Read more: https://www.afr.com/technology/inside-australia-s-turbocharged-battle-against-hackers-20240322-p5fegz

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

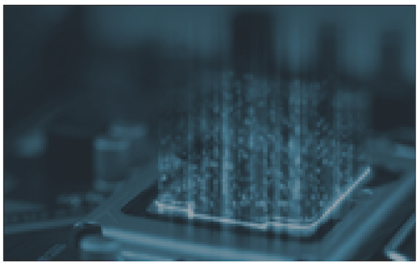
Data Focus Conference 2024 **Zagreb, Croatia** **9 April 2024**	**UK Cyber Week – Expo & Conference** **Olympia, London, UK** **17-18 April 2024**	**Cyber Security Capacity Centre** **Oxford Martin School,** **University of Oxford, UK** **30 April 2024**
Join us for the DATA FOCUS 2024, where we bring together law enforcement investigators, prosecutors, judges, court expert witnesses, and other experts, and let them talk about their experiences with digital evidence and digital forensic investigations. Don't miss this opportunity to enhance your skills and be inspired. The Data Focus conference is divided into several sections: • Investigation section • Technical section • Legal Section Workshops At the event, our partners will conduct a series of workshops, providing participants with opportunities for personalized inquiries and live demonstrations.	Join our community at UK Cyber Week 2024, where collaboration between cyber experts and business leaders is paramount. We believe that, to close the knowledge gap between cyber experts and UK business leaders, we must work together. Policymakers, IT departments, cyber professionals, law enforcement, software developers, educators, and the media all play a critical role in safeguarding against cyber threats. Our event is completely **FREE** to attend and brings together world-class experts to demystify jargon, share the latest thinking, and equip attendees with the knowledge they need to protect their businesses. Whether you're a cybersecurity veteran or new in the industry, you will leave our event feeling empowered and ready to take action against cyber threats.	The cyber-threat continues to evolve and will be benefitting from geopolitical instability, enhanced digital attack capabilities, and growing inter-dependencies and vulnerability throughout supply-chains and our critical infrastructures. Pre-positioning of malware and insider threats must be assumed. We are witnessing a massive progress towards AI-futures. The associated digital technologies and Internet-of-Things is beginning to become pervasive, with quantum and space innovations expected to follow in quick succession. We need to deliver responses that can ensure cyber-resilience in the face of continued capacity deficit in workforce around the world. What should be the community's priorities in cybersecurity capacity building? We invite you to celebrate 10 years of research into cybersecurity capacity for nations by joining the GCSCC to embark upon a critical debate for the next decade
For further information **https://insig2.com/en/data-focus/data-focus-2024/**	**For further information** **https://www.ukcyberweek.co.uk/uk-cyber-week-2**	**For further information** **https://gcscc.ox.ac.uk/event/gcscc-10th-anniversary-conference-oxford**

Zyber Global Online Events

Our Online Courses with INsig2
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/
Special discount: 15% Use Code: zyber

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**

c

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.
https://bit.ly/31NRYsj

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.
https://bit.ly/3eMu7ED