Zyber Global

JANUARY 2023 | ISSUE 30

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to Zyber Global Centre's monthly newsletter - January 2023, the 30th edition!

May the wind of life always be at our backs and the waves gentle, as we sail towards happiness and prosperity.

Our team hopes that this year will be full of new achievements that will bring you success. Happy New Year!

I hope that you have had a relaxing break and are looking forward to achieving great things this year.

The New Year means new opportunities! We took some time out to think about not just what we have achieved in 2022 we also discussed what went well and what lessons we have learnt that will help us do better and be successful in 2023.

We also discussed what we are going to do this year. We had lots of ideas, but one really stood out for us, and we have decided to launch it as a 'new project' this year so keep an eye on the newsletter as we will soon be announcing it.

If you would like to have an online cyber health check, do register early for our Stay Safe Online webinar on the 31 January 2023. See: https://zyberglobal.com/webinars

Let us know what topics you would like to see discussed in the February 2023 newsletter.

Stay safe!

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Focus Interview
This month's focus Interview is with Retired Captain Musa Jalloh, Deputy Director, Regulatory Administration, National Communications Authority (NatCA), Sierra Leone.

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

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

"Engaging in awareness campaign, education and information sharing are effective tools in the fight against cybercrime. We should follow good cyber hygiene and be cyber smart".

Retired Captain Musa Jalloh, Sierra Leone

Zyber Focus Interview

Retired Captain Jalloh uses his energy and talent to help build a more secure cyber-security system for Sierra Leone. He stands for excellence and this is reflected in his work to date in cyber-security.

Retired Captain Musa Jalloh
Deputy Director, Regulatory Administration,
National Communications Authority (NatCA)
Sierra Leone

Q. 1 **Can you tell us about your background and career to date.**

I live in Freetown, the capital city of Sierra Leone. After graduating with a Masters degree in Information Systems from Stratford University, New Delhi Campus, in December 2014, I started my career in the field of Information Technology. On my return back home, the Ebola epidemic was at its height, and I worked for the International Medical Corps at their main treatment Centre as their Database Developer and Administrator. I am an Associate Lecturer at the Institute of Public Administration and Management (IPAM), University of Sierra Leone. I started working at the National Telecommunications Commission (NATCOM), now transformed into the National Communications Authority (NatCA), in June 2019. I am the Deputy Director in the Regulatory Administration Department. I assist the Director in the effective functioning of the department and I am also responsible to provide oversight on Cybercrime and Cybersecurity issues.

Q. 2. **Can you tell us about the National Telecommunications Commission of Sierra Leone and the Regulatory Administration Directorate?**

The National Telecommunications Commission was established by an Act of Parliament in 2006 and charged with the responsibility of licensing and regulating telecommunications operators and for the promotion of universal access to basic telecommunication services, to ensure fair competition and investment in the telecommunications sector. We now have a new Act, the National Communications Authority Act 2022, with our mandate now expanded.
The Department of Regulatory Administration is charged with overseeing the review and generation of all license types for approved telecommunications services, developing effective administration of the National Numbering Plan (NNP) for the telecommunications market based on International Telecommunication Union (ITU) Standards. We also ensure the mitigation of cybercrime and increase cybersecurity awareness. Most importantly, we help in Revenue Assurance, Fraud Management and the International Gateway Monitoring and develop telecommunications Regulations in accordance with Section 82 of Communications Act 2022 (as amended).

Q.4 **What has been Sierra Leone's experience of cybercrime to date?**

The rate of cybercrime is limited however we do experience cyberbullying, fake news, hate speech, telecommunications fraud, denial of service attack, phishing, identity theft, cyberbullying, child sexual abuse, disclosing of private sexual images without consent, online grooming, phishing, and fake news.

Q.5 **What measures have you put in place to effectively combat cybercrime?**

Firstly, we have developed the national cybersecurity policy and strategy, and in November 2021 the cybersecurity and crime law was legislated. Secondly, Sierra Leone is a beneficiary of the establishment of a National Computer Security Incident Response Team (nCSIRT), with support from the Council of Europe. The project is being implemented by Expertise France and ECOWAS under the Organized Crime for West Africa Response to Cybersecurity (OCWARC). Sierra Leone is on the development of its technical capabilities to monitor, defend, and protect its cyberspace. We have conducted training to stakeholders in the justice sector such as judges, magistrates, lawyers, and prosecutors, to be able to handle cyber offences. We are also creating awareness programs and educating citizens on how to keep themselves and their institutions safe.

Q. 6 **Can you tell us something about how cybercrime affects Africa? What regional collaboration are you involved in to tackle cybercrime?**

Cybercrime is estimated to cost Africa about $4bn a year. Apart from financial loss, we also have reputational damages.

Read the full article: https://zyberglobal.com/blog

Zyber News Roundup

FTX Hack: Federal Prosecutors Investigating Alleged Cybercrime Worth Over $370M

Besides the fraud case against the bankrupt crypto exchange and its co-founder Sam Bankman-Fried, The Department of Justice (DOJ) has opened an additional criminal investigation into FTX's missing assets. Bloomberg reported on December 27th a person familiar with the case informed that Federal prosecutors at DOJ are investigating an alleged cybercrime that stole more than $370 million from FTX.

Only hours after FTX declared bankruptcy in the United States, hackers stole millions of dollars worth of cryptocurrency from the defunct exchange. Then began to convert the stolen money into Bitcoin. Although the stolen money was converted into many other digital currencies, the majority, more than $280 million, was turned into ETH. Co-founder of Elliptic, who spoke with CNBC, said the hackers turn ETH into RenBTC, a crypto product that is then turned into BTC via a bridge.

It was confirmed by the source that US officials had been successful in freezing part of the stolen funds. However, the frozen assets only make up a small portion of the total sum. The report added that uncertainty exists regarding whether this breach was an inside job or the work of a hacker looking to profit from the vulnerabilities of a struggling company.

Nevertheless, the sum taken is a lot less than the alleged misuse of billions of dollars by Bankman-Fried. Authorities claim he illegally acquired $1.8 billion from investors and used it to place high-risk bets at Alameda Research and for personal expenses.

Read more: **https://www.tronweekly.com/ftx-hack-federal-prosecutors-investigating/**

Image by Gerd Altmann Pixaby

Police Anti-cybercrime Team Nabs 2 Suspects Over Computer-related Fraud

A team from the Nigeria Police Force National Cybercrime Centre (NPF-NCCC), has busted a syndicate and arrested two suspects, alleged to be responsible for computer-related fraud, identity theft, cryptocurrency fraud, and obtaining money by false pretence.

The duo is said to run a syndicate, which specialises in defrauding unsuspecting victims from foreign countries, by assuming identities of other persons and promising them romantic relationships, under the pretext of which they defraud their victims. Olumuyiwa Adejobi, Force Public Relations Officer said that a report on their activities was received from Incheon Metropolitan Police Agency in Korea, through the Interpol National Central Bureau that in May, 2021, the suspects approached the victim, one Baek Seong-hee, a Korean national, via Kakaotalk, a mobile messaging application, used in South Korea, in the guise of being a member of the US Armed Forces stationed in Yemen. The suspects used the pretext of a romantic relationship and defrauded the victim of 259,637,941 Korean Won (KRW) worth of cryptocurrency equivalent to about N91 million.

Read more: **https://independent.ng/police-anti-cybercrime-team-nabs-2-suspects-over-computer-related-fraud/**

Experts Warn ChatGPT Could Democratize Cybercrime

A wildly popular new AI bot could be used by would-be cyber-criminals to teach them how to craft attacks and even write ransomware, security experts have warned. ChatGPT was released by artificial intelligence R&D firm OpenAI last month and has already passed one million users.

The prototype chatbot answers questions with apparent authority in natural language, by trawling vast volumes of data across the internet. It can even be creative, for example by writing poetry. However, its undoubted talents could be used to lower the barrier to entry for budding cyber-criminals, warned Picus Security co-founder, Suleyman Ozarslan.He was able to use the bot to create a believable World Cup phishing campaign and even write some macOS ransomware. Although the bot flagged that phishing could be used for malicious purposes, it still went ahead and produced the script. Additionally, although ChatGPT is programmed not to write ransomware directly, Ozarslan was still able to get what he wanted.

Read more: **https://www.infosecurity-magazine.com/news/experts-warn-chatgpt-democratize/**

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

International Conference on Cybersecurity and Hacking **Tokyo, Japan** **January 9-10, 2023**	**Cyber-Threat 2022** **London, United Kingdom** **January 16-17, 2023**	**Oxford Internet Policy & Politics Hybrid Conference** **Oxford, United Kingdom** **January 21, 2023**
The International Conference on Cybersecurity and Hacking aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Cybersecurity and Hacking. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Cybersecurity and Hacking.	CyberThreat 2022 is a hybrid event that will bring together the UK and Europe's cyber security community. Designed for security practitioners and spanning the full spectrum of offensive and defensive disciplines, the event has a strong technical emphasis. This event is hosted by the UK's National Cyber Security Centre (NCSC) and SANS Institute and evidences the UK Government's commitment to equip practitioners with the skills and knowledge required to defend against cyber threats and addresses the cyber skills gap, by developing and growing talent.	This Conference has been convened by the Policy & Internet Journal, and is co-sponsored by the Policy Studies Organization, the Next Century Foundation, American Public University System, and the APUS Center for Cyber Defense. The conference aims to promote interdisciplinary conversation about the implications of the Internet and related technologies for public policy, bringing together scholars, practitioners, NGOs, social and business leaders from a variety of backgrounds, to subject the relationship between the Internet, policy, and politics, to multidisciplinary scrutiny. The rapid change of technologies and the disruption it causes has a significant impact on our public policy, as well as for citizen-government relations, and how the internet itself is governed.
For further information **https://waset.org/cybersecurity-and-hacking-conference-in-january-2023-in-tokyo**	**For further information** **https://www.sans.org/cyber-security-training-events/cyberthreat-2022/**	**For further information** **https://ipsonet.org/conferences/oxford-internet-policy-politics-conference/oxford-internet-policy-politics-conference/**

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

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