Zyber Global

DECEMBER 2022 | ISSUE 29

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 29th "Christmas" Edition, December 2022 of Zyber Global Centre's monthly newsletter.

Christmas is one of my favourite celebrations, and no it's not all about the presents!

November was very busy for me, so I am looking forward to the Christmas break and taking time off for a traditional family Christmas. Like everyone else during the Covid pandemic we had limited contact with family, so it's nice to be able to reconnect with some of our old traditions to add to the new normal we are now living.

For me, the Covid pandemic dramatically changed the way I worked. Before Covid, I spent a lot of time travelling abroad to provide training. I loved travelling to new places and meeting new people (this month's article is about a conference I attended in Costa Rica).

As we were in lockdown, I and many others moved to online training. I seemed to have let that particular genie out of the bottle and now most of my training is online. Although there has been less travel, as always the positives far outweigh the negatives and the great positive for me is that I can be involved in so many more projects than before Covid, as long as I have a good internet connection.

I look forward to meeting you (the readers) at an online conference somewhere in 2023.

Wishing you all a Merry Christmas and a fantastic 2023!!

This Month's Features

Zyber Focus
This month's focus is an article on highlights from a conference promoting the role of women in preventing investigating and prosecuting cyber crimes, held in Costco Rico from the 10th - 11th of November 2022.

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

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

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

"Women have a crucial role to play in effective criminal justice responses to cybercrime; whether as policymakers or legislators developing and adopting legislation on cybercrime, or as law enforcement, prosecutorial or judicial practitioners investigating and prosecuting offences".

Zyber Focus Article

My Notes on the International Conference on promoting the role of women in preventing investigating and prosecuting cyber crimes
Costa Rica 10th - 11th of November 2022.

Esther George, CEO, ZGC

I represented the International Association of Prosecutors (IAP) at the conference on promoting the role of women in preventing, investigating, and prosecuting cybercrime in Costa Rica. I moderated the Practitioner Workshop 2: Experiences and opportunities from the prosecutor's perspective.

The IAP has a rich history of working collaboratively with the Council of Europe. So, I was delighted to hear from our Senior Legal Advisor Edith Van den Broeck that the Council of Europe was organising a conference on promoting the role of women in preventing, investigating, and prosecuting cybercrime. It was to be an in-person event over 1.5 days in Costa Rica. I had never been to Costa Rica and most people I spoke to about it had either been and had a great time or it was on their bucket list. So, I had high hopes for this conference, and I was not disappointed.

The conference was held in the capital San Jose. Costa Rica is a beautiful country, with volcanoes, beautiful beaches and certainly lives up to its reputation of being a haven for wildlife.

The conference was organised by the Public Ministry of Costa Rica, in cooperation with the Council of Europe and with the support of other organisations.

The conference recognised that women have a crucial role to play in effective criminal justice responses to cybercrime; whether as policymakers or legislators developing and adopting legislation on cybercrime, or as law enforcement, prosecutorial or judicial practitioners investigating and prosecuting offences. Despite this, cybercrime and electronic evidence are often perceived as a predominantly male domain. This certainly seems to be the case at senior levels and with respect to more technical fields such as digital forensics, CERTs, cybersecurity or the development and deployment of new technologies.

The conference consisted of plenary sessions as well as Four Thematic workshops on:

- Promoting women in technical domains
- Women preventing cybercrime and preventing cybercrime against women
- Women as victims of cybercrime – ensuring access to effective remedies
- Combatting cyberviolence against women

There were also four practitioner workshops to share experiences and opportunities from the perspectives of:

- Policymakers and legislators
- Prosecutors
- Police/investigators
- Judges.

I moderated the workshop on "*Experiences and opportunities from the prosecutor's perspective*". The rapporteur for this session was Ms Ranjani Padmanabhan, Principal Federal Prosecutor, Commonwealth Director of Public Prosecutions Australia.

Some of the highlights of this workshop included the following snippets from the speakers:

Miriam Bahmonde Blanco, Senior Prosecutor Spain, spoke on '*What is needed to make the prosecution of cybercrime against women more effective and the need to increase/incentivise the level of reporting of online crimes*'. Ms Blanco told us about some positive examples in Spain such as the introduction of measures to make content that infringes on legal rights inaccessible online. She also explained the gender perspective in the field of cybercrime in Spanish law.

Denisa Asko, Public Prosecutor's Office, Albania then spoke on the '*Role of women in prosecution and how to further promote women in prosecuting cybercrimes and the need to strengthen the prosecution of cybercrimes against women*'. Ms Asko referred to evidence of good practice in Albania.

Lolita Lomanta, Senior Assistant Provincial Prosecutor, Philippines said that the Philippines is the most-gender equal country in Asia, based on the world economic forum global gender gap report 2022. She said that there are women at all sectors of society in the Philippines and that 4 out of 10 prosecutors nationally are women. Ms Lomanta shared other good practice that the Philippines was doing in this field.

Lastly Edwige Tangni, Prosecutor at the Tribunal and former member of the Special Prosecutor's Office of the Court for the Repression of Economic Offences and Terrorism, Benin, spoke about the reforms that were taking place in this field in Benin and the classification of such crimes. There has been an increase in reporting of such crimes in Benin but also an increase in those sentenced for such crimes. Ms Tangni also told us about the National Institute for women in Benin and the work that the Institute is doing to help women to obtain justice.

Finally the Q&A session which concluded with the rapporteur Ranjani Padmanabhan summarising the sessions and presenting the key takeaways. I then closed the session by reminding everyone about the IAP and the helpful materials etc it holds and the Global Prosecutors E-crime Network (GPEN) and how it can assist them and that the IAP and Council of Europe plan to organise some webinars to take the outputs from this workshop forward. The workshop was extremely well received, and it was a pleasure to be involved.

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

Zyber News Roundup

Estonian Duo Arrested for Masterminding $575m Ponzi Scheme

Two Estonian men have been arrested in the capital city of Tallinn for their alleged role in an "enormous" Ponzi scheme which defrauded cryptocurrency investors out of hundreds of millions of dollars.

Sergei Potapenko and Ivan Turõgin, both 37, allegedly defrauded hundreds of thousands of investors in two schemes running from 2015 to 2019.

The most serious was their solicitation of investment in HashFlare, which they claimed would enable clients to rent a percentage of the firm's cryptocurrency mining operations in exchange for the virtual currency it produced.

Over the four-year period, customers are said to have invested over $550m in the firm. However, while the HashFlare website showed they were making big profits, in reality the firm's equipment allegedly performed Bitcoin mining at a rate of less than 1% of the computing power it purported to have.

When investors asked to withdraw funds, the duo either refused or paid them using virtual currency they purchased on the open market, according to the Department of Justice (DoJ).

A second alleged fraudulent investment scheme was launched by the two in 2017. This time it was a bank specializing in virtual currency, which they claimed would generate dividends for investors from its profits.

Potapenko and Turõgin are said to have raised $25m for this fictitious bank, dubbed Polybius, but it never actually existed. In both schemes, the duo are said to have laundered funds by using "shell companies and phony contracts and invoices" to buy at least 75 properties, six luxury vehicles, cryptocurrency wallets and thousands of cryptocurrency mining machines.

Potapenko and Turõgin are charged with conspiracy to commit wire fraud, 16 counts of wire fraud and one count of conspiracy to commit money laundering. Each faces a maximum of 20 years behind bars if found guilty.

Read more:
https://www.infosecurity-magazine.com/news/estonian-duo-arrested-575m-ponzi/

Aussies warned to avoid crypto paper wallets they find on the street

Fraudsters have reportedly been leaving fake crypto paper wallets in public places as part of a scam to dupe Australians out of their crypto.

Australians have been warned to stay away from suspicious-looking fake Bitcoin According to a Nov. 22 post on the Facebook page of the NSW Police Force, the scam starts as a paper cryptocurrency wallet with a QR code, which is made to appear like a legitimate Bitcoin paper wallet. These are strewn by scammers in public locations such as streets or parks.

An individual that locates the paper wallet and scans the QR code is directed to click on a link to access a crypto wallet with up to $16,000 Australian dollars ($10,000).

The person is then asked to pay a withdrawal fee and provide their own wallet credentials that will purportedly allow them to transfer the balance into their own crypto wallet.

"Once the withdrawal fee is paid and person's crypto wallet details provided, the person's cryptocurrency is stolen from their crypto wallets," explained the NSW police.

Read more: https://cointelegraph.com/news/aussies-warned-to-avoid-scanning-crypto-paper-wallets-they-find-on-the-street

US offshore oil and gas rigs at 'significant' risk of cyberattacks, warns government watchdog

U.S. offshore oil and gas infrastructure faces "significant and increasing" cybersecurity risks that require "urgent" attention, a U.S. government's watchdog has warned. The Government Accountability Office said in a new report that the network of over 1,600 offshore facilities that produces a significant portion of U.S. domestic oil and gas are at a growing risk of cyberattacks. The warning comes more than a year after ransomware actors targeted Colonial Pipeline, bringing the U.S. oil pipeline system relied on by millions of Americans to a standstill.

The watchdog warned that not only has the government identified the offshore oil and gas sector as a target of malicious state actors, particularly those backed by China, Iran, North Korea and Russia, but said operational technology (OT) — often used by these facilities to monitor and control physical equipment — contains multiple security flaws that could allow attackers to remotely take control of various functions, including those critical to safety.

The U.S. watchdog is calling on the Department of the Interior's Bureau of Safety and Environmental Enforcement (BSEE), which oversees offshore oil and gas operations, to address these growing security risks. It says that the agency had initiated efforts to address these cybersecurity risks as far back as 2015, but has yet to take any "substantial" action almost a decade later.
Read more: https://techcrunch.com/2022/11/22/offshore-oil-gas-cyberattacks-watchdog/

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

Black Hat Europe 2022 **Excel London,** **United Kingdom** **December 5-8, 2022**	**The 6th International Workshop on Big Data Analytic for Cyber Crime Investigation and Prevention 2022 Osaka, Japan** **December 17-20, 2022**	**International Conference on Internet Forensics, Cybersecurity, Cyberthreats and Cybercrime Istanbul, Turkey** **December 20-21, 2022,**
Black Hat provides attendees with the latest in research, development, and trends in Information Security. Here the brightest professionals and researchers in the industry come together for a total of four days—two or four days of deeply technical hands-on Trainings, followed by two days of the latest research and vulnerability disclosures in the Briefings. Black Hat Europe will be a Live, In-Person Event in London, December 5-8, followed one week later by a Virtual Experience including recordings of all Briefings and Sponsored Sessions, available December 14.	Following the positive feedback and great interest last year, we are delighted to announce the 6th International Workshop on Big Data Analytic for Cybercrime Investigation and Prevention, co-located with IEEE Big Data 2022 conference. There is a need for advanced big data analytics to aid in cyber crime investigations, which requires novel approaches for automated analysis. This workshop is organized to bring together recent development in big data analysis to aid in current challenges in cybercrime investigations.	This International Conference on Internet Forensics, Cybersecurity, Cyberthreats and Cybercrime aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Internet Forensics, Cybersecurity, Cyberthreats and Cybercrime. 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 Internet Forensics, Cybersecurity, Cyberthreats and Cybercrime.
For further information **https://www.blackhat.com/eu-22/?cid=smartbox_techweb_session_16.500275&_mc=smartbox_techweb_session_16.500275**	**For further information** **http://wikicfp.com/cfp/servlet/event.showcfp?eventid=161049&copyownerid=101185**	**For further information** **https://waset.org/internet-forensics-cybersecurity-cyberthreats-and-cybercrime-conference-in-december-2022-in-istanbul**

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