Zyber Global

FEBRUARY 2022 | ISSUE 19

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 19th Edition, February 2022 of Zyber Global Centre's monthly newsletter.

Its February already, time really does fly or so it seems, as a friend and I were discussing the other day. I used to find it funny back in the day when my older relatives remarked that the time was passing so quickly. I could never see it myself! Now I find myself agreeing with them.

The first month of 2022 just whizzed pass and I still haven't completed all my goals for January! However, I must say I am not sad to see the end of January - the papers here in the UK are full of the alleged UK government's Covid breaking activities which are still under investigation.

The biggest natural disaster at the start of 2022 was the eruption in Tonga of an undersea volcano, which triggered a tsunami that caused major damage to its infrastructure, contamination of water and damage and destruction to food crops.

I was saddened, shocked and horrified at the news as I had visited Tonga in 2016 when I represented the Global Prosecutors E-Crime Network (https://www.iap-association.org/GPEN/Home.aspx) at the Joint Regional Training which we co -organised with the Commonwealth Secretariat, Government of Tonga and the Council of Europe.

I was fortunate to spent time on Tonga, which I fondly remember as a very beautiful island with some of the warmest and nicest people I have ever met. I made some very good friends with whom I am still in touch. My prayers and thoughts are with them all and their families.

If you are interested in assisting our friends in Tonga, TearFund, New Zealand is urgently requesting donations. Any funds donated now is being distributed immediately to bring swift relief to affected Tongan communities.

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

TearFund, is a charity that I have long been a supporter of as I admire the work that they do globally.

I have made a personal contribution to the emergency appeal they have set up at:
https://www.tearfund.org.nz/tonga

If you haven't yet donated to a charity to help in the relief effort, please consider donating to TearFund, New Zealand.

Esther George: happy times in Tonga, 2016

This Month's Features

Zyber Spotlight

The interview spotlight this month is on Capacity Building, in the Pacific, Pacific Section, Attorney-General's Department Australia.

Zyber Focus

Capacity Building Regarding Cyber Security and Cyber Crime Prevention

Zyber News

We have a roundup of the latest international cybercrime news.

Zyber Global Events Information

A focus on forums/conferences around the world.

"The borderless nature of cybercrime means that international cooperation, investigative assistance, and consistent substantive and procedural legislative provisions, are of paramount importance".

Pacific Section, Attorney-General's Department, Australia.

Zyber Spotlight

Interview on Capacity Building in the Pacific, Pacific Section, Attorney-General's Department Australia

Can you tell us about your work in the pacific to date?

Our team administers the Australian Attorney-General Department's (AGD) Pacific Law and Justice Program. We work to strengthen legal systems and contribute to effective governance in a stable, prosperous, resilient Pacific in the wake of COVID-19. The Program has three objectives:
(i) improved Pacific capacity to develop policy and laws (particularly policing and criminal law); (ii) demonstrated improvements in policy and laws across the Pacific (particularly policing and criminal law); and
(iii) more effective Pacific law and justice collaboration and cooperation on domestic and transnational issues.

We seek to achieve these outcomes primarily through training and mentoring Pacific officials, partnering on bilateral or regional legal policy and legislative reform projects and enhancing regional collaboration on law and justice issues. We are proud of our longstanding involvement in the Pacific Islands Law Officers' Network (PILON), over the last 40 years. PILON is a network of senior law officers from 19 Pacific Island countries, including Australia and New Zealand, who work together to contribute to a safe and secure Pacific by advancing key law and justice issues.

Can you tell us something about how cybercrime affects the Pacific regions?

Internet connectivity has steadily improved across the Pacific region, resulting in faster and better internet access. While this enables greater social and economic possibilities, it also enables cybercriminals to reach across to the Pacific to commit new crimes, or old crimes in new ways. The borderless nature of cybercrime means that international cooperation, investigative assistance, and consistent substantive and procedural legislative provisions, are of paramount importance.
Pacific leaders have acknowledged that cybercrime is a rapidly growing threat to the region and, in the Boe Declaration on Regional Security, called for an increasing emphasis on regional cooperation to address key vulnerabilities. PILON contributes to regional efforts to address this issue through promoting accession by PILON Member countries to the Budapest Convention. The Convention is important because it provides a framework for regional cooperation and collaboration on investigating and prosecuting cybercrime including information sharing and mutual legal assistance (providing evidence across international borders).

Cybercriminal tactics seem to be evolving at an alarming rate. Do you think we are doing enough to combat cybercrime?

Cybercriminals will continue to adapt to new technologies and everyone needs to remain vigilant, agile and coordinated to effectively combat these threats. This includes having strong cybercrime legislation with coordinated mutual legal assistance provisions, in line with best practice. As countries in the region continue to develop their cybercrime laws and accede to the Budapest Convention, the strength of cybercrime legislation and cooperation in the Pacific will continue to improve.
We also need to continue to train law enforcement agencies on identifying and responding to existing and novel types of cybercrime. This will ultimately result in better investigations and prosecutions, resulting in improved protection of Pacific communities. Finally, by continuously sharing lessons learned through our various regional networks, we can ensure that we have the most up-to-date knowledge about how to detect and deter new cybercrimes.

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

Zyber News Article

Capacity Building Regarding Cyber Security and Cyber Crime Prevention

by
Esther George & the Zyber Global Research Team

In this article, we are going to look at why it is so important for countries to build capacity in cyber security and the principles that countries should embrace to promote cybersecurity and cybercrime prevention.

Cybersecurity is defined as a process of securing computer systems, programs, networks, and other forms of digital data from cyber-attacks. It is also referred to as IT security or computer security.

Cybersecurity is extremely important because most businesses and governments transmit information via on-line technology so it is essential that data is protected from cyber-attacks, as a data breach can have destructive and devastating consequences such as financial impact and data loss. The core aspects of cybersecurity are confidentiality, integrity, and availability.
Capacity building, is defined as a dynamic process where the needs of stakeholders are in constant evolution.

Specifically, cybersecurity capacity building is defined as a way of empowering individuals, communities, and governments to achieve their developmental goals by reducing digital security risks stemming from access and use of information and communication technologies. A strong cyber security strategy is important for countries to progress and develop their own economic, political, and social spheres which in effect, creates a safe and stable cyberspace. Furthermore, the aim of cybercrime capacity building includes achieving transformation of domestic legislation and institutional arrangements in line with global principles and this is critical when looking at national security policies and sovereignty of states. To build capacity in another country, the donor country must first have knowledge, know-how and technology of its own that it can share.

For example, donor countries like the United States of America (USA) and some countries in Europe are well positioned regarding their level of Information and Communications technology (ICT) development and are committed to supporting other countries.

Capacity building efforts include training of government officials; and drafting regulatory frameworks etc. In this way, donor countries can also export their understanding of norms or ideas of cyberspace governance and their understanding of what risks are involved

Communication is extremely important when promoting cybersecurity capacity building as there must be clear and frank communication and cooperation among all parties involved.

Previously this was not being done. I remember an occasion some years ago when I was in Eastern Europe, training members of the criminal justice system on cybercrime. During the training it was pointed out that similar training (from another donor country) was taking place across town. Back then this was not a rare occurrence and I know several colleagues who can tell their own stories of something similar happening to them. This probably still happens occasionally but nowadays to prevent this happening, organisations are more likely to hold a jointly branded training event. Donors and organisations are now communicating more effectively and working collaboratively with each other.

A lot of the credit for this must go to the Global Forum on Cyber Expertise (GFCE) as it coordinates regional and global cyber capacity projects and initiatives. It also hosts an annual multistakeholder conference where stakeholders get to interact with others who are also active in this field. The GFCE has also created a very useful resource in the Cybil Portal which hosts best practice, research papers, and self-assessment tools etc. that are freely available and accessible to all.

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

Zyber News Roundup

Sweden's spy agency probes drones over 3 nuclear plants

Sweden's domestic security agency said it has taken over the preliminary investigation into drones, that last week were seen hovering over or near the country's three nuclear power plants.

At first, police said there had been drones over two nuclear plants — Forsmark, north of Stockholm, and Oscarshamn in the southeast. The intelligence service, known by its Swedish acronym SAPO, said a drone also was reported over a third nuclear power facility, Ringhals, which is the largest of them and sits on the country's western coast.
Police have no suspects. "*With regard to the cases of drone overflights at three nuclear power plants, the assessment is made that they are of such a nature that preliminary investigations have been taken over from the police authority in order to be able to investigate the incidents in more detail*," SAPO said in a statement.

Late Friday, police were alerted about the drones but lost track of the unmanned aircraft. Swedish media said the drones were large enough to withstand the wind that was blowing over the area.

Read more:
https://www.euronews.com/2022/01/17/sweden-s-spy-agency-probes-drones-over-3-nuclear-plants

How tech is a weapon in modern domestic abuse -- and how to protect yourself.

Increasingly, we are using technology to perform everyday tasks like banking, shopping, socializing, and, in cases of domestic abuse, monitoring individuals without their consent -- or with their "permission" through coercion. Through technology, it is possible to stalk someone with little effort. This can involve anything from sleuthing to find information about your Tinder date to checking a potential work candidate's social profiles to planting spyware on your partner's phone.
In short, technology has provided new avenues for stalking to take place. Recorded cases of spyware and stalkerware have dropped in number in recent years -- only to be replaced with mobile applications that can be difficult to detect and remove, covert cameras, and item trackers.
Spyware is usually generic and is rarely personal. For the cybercriminals who develop these forms of malicious software, it's about grabbing personal data like financial account details to conduct theft and fraud.
Stalkerware has a different nature. Deployed to actively monitor an individual through their mobile device, stalkerware apps can be used to track spouses, exes, children, and even employees on their work devices.
Stalkerware capabilities can include tracking a location through GPS, eavesdropping on calls and social media conversations, stealing logs, monitoring browser activity, and compromising a device's camera and microphone to listen/take photos of a real-world environment.

Read more: https://www.infosecurity-magazine.com/news/russia-fines-google-100m-over/

Amazon fake crypto token investment scam steals Bitcoin from victims

A new cryptocurrency-related scam is abusing the Amazon brand to dupe would-be investors into handing over Bitcoin (BTC).
Cryptocurrency and digital token scams have become a common threat facing investors and the general public today.
Even though regulators worldwide are clamping down on fraud -- through tax legislation, securities offering registration, tighter rules surrounding cryptocurrency adverts, and by keeping a close eye on initial coin offerings (ICOs), exit scams, rug pulls, and theft is still rampant.
Interest in cryptocurrency -- and now NFTs -- continues to escalate, providing a breeding ground for new scams to appear on a daily basis.
Chainalysis estimates that fraudsters received approximately $14 billion in deposits in 2021.
Cybersecurity researchers from Akamai Technologies outlined a new, fraudulent campaign that leverages Amazon's name to promote a fraudulent "Amazon to create its own digital token" scheme. Generating panic and encouraging victims to make a rash decision are common tactics used in various scams, and this is no exception.

Read more: https://www.zdnet.com/article/amazon-fake-crypto-token-investment-scam-steals-bitcoin-from-victims/

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

International Conference on Cyberlaw, Cybersecurity and Cybercrime **February 07-08, 2022** **Lisbon, Portugal**	**International Conference on Cyberlaw** **February 15-16, 2022** **London, United Kingdom**	**International Conference on Cybersecurity and Cyber Threats** **February 24-25, 2022** **Buenos Aires, Argentina**
The International Conference on Cyberlaw, Cybersecurity 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 Cyberlaw, Cybersecurity 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 Cyberlaw, Cybersecurity and Cybercrime.	The International Conference on Cyberlaw aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Cyberlaw. 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 Cyberlaw.	The International Conference on Cybersecurity and Cyber Threats 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 Cyber Threats. 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 Cyber Threats.
For further information: https://waset.org/cyberlaw-cybersecurity-and-cybercrime-conference-in-february-2022-in-lisbon	For further information: https://waset.org/cyberlaw-conference-in-february-2022-in-london	For further information: https://waset.org/cybersecurity-and-cyber-threats-conference-in-february-2022-in-buenos-aires

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