Zyber Global

MARCH 2021 | ISSUE 8

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 8th Edition, March 2021 of Zyber Global Centre's Monthly Newsletter

It will be 7 years in April 2021 since I left the Crown Prosecution Service (CPS). Some scholars say that the number '7' denotes completeness or perfection, so I think that it's very significant that I will be delivering online cybercrime training to my former colleagues through the auspices of the National Black Crown Prosecution Association (NBCPA) later this month.

The NBCPA will be hosting a series of three one-hour webinar training sessions from March to May 2021 on Cyber Crime, which I am very proud to be delivering.

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Spotlight

The interview spotlight this month is on the Attorney General of the Kingdom of Tonga, and Chair of the Pacific Islands Law Officers' Network (PILON) Cybercrime Working Group, Ms. Linda Simiki Folaumoetu'i

Zyber News

This is a roundup of the latest international cybercrime news.

Zyber Focus

The focus this month is on the *Impact of COVID-19 on Cyber Security in the Caribbean* by Arsha Gosine, Head of Research, Zyber Global Centre

Zyber Global Events

The next Stay Safe Online Webinar by Zyber Global is on Wednesday 31st of March 2021. Register now to attend.

" In the Pacific, there are various organizations which allow the tracking of cybercrime. There is the Pacific Islands' Legal Officer's Network where legal officers across the region keep each other updated on legal aspects of cybercrimes.

Ms. Linda Simiki Folaumoetu'i
Attorney General, Kingdom of Tonga

Continued from page 1.....

The first webinar is an 'Introduction to Cybercrime' and will be held on 18th March 2021. The full details for this webinar are on the event page.

My thanks to Grace Moronfolu, MBE, the Chair of the NBCPA for her commitment to making this possible and ensuring that NBCPA members receive training on cybercrime, electronic evidence, and international cooperation which in this online interconnected world are basics that we must all get to grips with.

Mala Drepaul (the training lead), thank you for recognising the need for the training and working closely with Grace to ensure that we got the contents right. My thanks also to all those who worked to make this training a reality, especially Ayaz Kishtwari and Parhit Kalia.

I am really looking forward to meeting up with my former colleagues and sharing my expertise and experience in cybercrime!

In the meantime, we continue to live our lives in lockdown in the UK, and I know it's the same for some countries. However, the advent of the vaccine may allow some modicum of normalcy in the near future.

So to all our readers:
Be well, stay safe....and do drop us a line on what you would like to read about in our April edition! We look forward to hearing from you.

ESTHER GEORGE
Editor and CEO Zyber Global Centre

Zyber News Roundup

Cybercrime groups are selling their hacking skills...and some countries are buying

Cyber-criminal hacking operations are now so skilled that nation-states are using them to carry out attacks in an attempt to keep their own involvement hidden.

A report by cybersecurity researchers at BlackBerry warns that the emergence of sophisticated cybercrime-as-a-service schemes means that nation-states increasingly have the option of working with groups that can carry out attacks for them. This cyber-criminal operation provides malicious hacking operations, such as phishing, malware or breaching networks, and gets paid for their actions, while the nation-state that ordered the operation receives the information or access it requires.

It also comes with the added bonus that because the attack was conducted by cyber criminals who use their own infrastructure and techniques, it's difficult to link the activity back to the nation-state that ordered the operation.

"*The emergence, sophistication, and anonymity of crimeware-as-a-service means that nation states can mask their efforts behind third-party contractors and an almost impenetrable wall of plausible deniability*," warns the BlackBery 2021 Threat Report.

Researchers point to the existence of extensive hacking operations like Bahamut as an example of how sophisticated cyber-criminal campaigns have become. While protecting networks from determined cyber attackers can be difficult, there are cybersecurity practices that organisations can apply in order to help keep intrusions out, such as only providing remote access to sensitive information to those who absolutely need it and constantly examining the network for unusual activity that would be classed as suspicious.

Read more:
https://www.zdnet.com/article/cybercrime-groups-are-selling-their-hacking-skills-some-countries-are-buying/

continued on page 4.....

Zyber Spotlight

Ms. Linda Simiki Folaumoetu'i
The Attorney General of the Kingdom of Tonga and Chair of the Pacific Islands Law Officers' Network (PILON) Cybercrime Working Group

As the Chair of the PILON Cybercrime Working Group, Ms Simiki Folaumoetu'i is pivotal in focusing its efforts on building the awareness of member countries to address cybercrime, to protect Pacific communities and economies. PILON promotes the development and implementation of best practice legislation, evidence gathering powers and international cooperation mechanisms for police, prosecutors and law makers.

Can you tell us a bit about yourself and your journey to where you are today in your career?

After reading law at the University of Auckland, New Zealand, I worked at the Attorney General's Office for 14 years and then as an Advisor to the Attorney General Chambers in the Solomon Islands (7 years). I returned to Tonga in 2014, where I was the Chief Executive Officer of the Office of the Ombudsman until 2019. In 2017, I was privileged to be one of the Law Lords advising the Privy Council and His Majesty on legal matters. I am the first female Law Lord in Tonga. I assumed the position of Attorney General in June 2019.

What is a highlight of your career to date?

A major highlight was being part of the team that worked on legislation to address social media abuse. The legislation received royal assent last week and will come into force once Cabinet gives notice for its gazettal.

As the Attorney General of the Kingdom of Tonga, can you share with us some of the challenges that you have faced since taking up the role.

Two of my major challenges were:
i)Drafting legislative instruments for COVID-19 and putting legislative processes in place to ensure that curfews, lockdowns, and all processes related to COVID-19 are legal.
ii)Trying to manage social media issues as complaints were coming from Cabinet ministers and government agencies on the negative impact that posts, in particular, were having on culture and society as a whole.

How has the development of ICT affected the Kingdom of Tonga and the region in terms of cybercrime?

Pacific communities are quite communal communities so the principle of 'trusting each other' is one that is observed in the Pacific quite strongly. Having said that, ICT development has been a blessing and a curse for Tonga and the Pacific region. Blessing in the sense that it has allowed the Pacific diaspora to stay connected with their family and friends spread out all over the world. On the other hand, it is a curse in the sense that our trusting people have quite easily fallen victim to cybercrime like phishing scams, money laundering, defamation of character, to name a few. In addition, with the lack of resources to properly investigate these offences, restitution in most cases is close to nil so our citizens and economies have lost so much at the hands of these cybercriminals.

What would you like your legacy as Attorney General to be?

An AG that was professional and one who led with integrity.

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

Zyber News Roundup

Zyber News RoundUp cont'd.....

Homebuyer loses life savings to a hacking scam: '*I couldn't believe it happened to me*'

One day Jeannine Fontaine wired money to buy her retirement home. The next day her entire life savings had disappeared. "It was a shock. I couldn't believe it happened. I couldn't believe it happened to me," Fontaine said.
She had found a home to buy near Ocala. Fontaine and used Ellison Realty to write the contract and Ocala Land Title Insurance for the closing.
The day before buying the home, Fontaine got an email from her realtor, or so she thought, with specific instructions to wire $122,000 to the bank so the title company could close the deal.

"*Everything was very professional, and it had the realtor's email account and the attachment wiring instructions, it looked perfect*," Fontaine said. In a sheriff's office report, Fontaine told deputies the wiring instructions were fraudulent and she had sent money to scammers. "*I haven't slept much since. Yeah, it's pretty bad*," Fontaine said.

The home-hacking scam targets home sales posted online. Scammers search real estate listing sites like Zillow to find a sale, then they hack into emails from realtors, title companies, homebuyers and sellers. After gathering insider information, they send spoof emails with phony wiring instructions to steal money the moment a house sells. The scheme has been a growing threat. According to the FBI, in Florida alone home hackers stole $29,000,000 in 2016, and $96,000,000 in 2019, and the losses since COVID-19 could be far worse.
Fontaine says she hired an attorney and is considering a lawsuit against her bank for not questioning the wire transfer.
Consumer experts say victims should tell their bank to recall a wire transfer the same day. Victims should contact their local FBI field office. The agency says if notified within 24 hours, it can freeze most phony bank accounts.

Read more:
https://www.wftv.com/news/action9/i-couldnt-believe-it-happened-me-homebuyer-loses-life-savings-hacking-scam/YFEH6NJ5U5GNZCNV5KP7T3O2BI/

Tens of Thousands of Sextortion Attacks Blocked in the United Kingdom

Tens of thousands of sextortion attacks were blocked in the UK in recent months as fears rise the pandemic is fuelling cybercrime.
Sextortion is a lesser-known type of online harassment which involves perpetrators threatening to use personal intimate images or footage to force the victim into complying with their demands.

New data from Avast, which runs a range of antivirus apps used by Microsoft, Android, and others, shows the platform blocked 66,063 sextortion attacks in the UK between mid-December and mid-February.

The platform said the incidents refer to emails sent by scammers falsely pretending to have explicit images of the victim.

David Jones, who works for the National Crime Agency's anti-kidnap and extortion unit, told The Independent: "*During the past 12 months we have seen increased reporting of sextortion by members of the public to UK police forces.*
"*Our assessment suggests this is due to increased confidence in the police to deal with allegations of cyber-enabled extortion (sextortion) in a sensitive and confidential manner.*"
He said they had worked with police forces to make reporting procedures better as he urged victims to neither "panic" or pay anything and have no more communication with the scammer.

Read more:
https://www.independent.co.uk/news/uk/home-news/sextortion-attacks-block-lockdown-b1805816.html

Zyber Focus

The Impact of COVID-19 on Cyber Security in the Caribbean

by Arsha Gosine, Head of Research, Zyber Global Centre

The Covid-19 pandemic has rendered individuals, and the public and private sectors extremely vulnerable to cyber-attacks, as we rely more than ever on online communication through our phones, our laptops and other mobile devices. From our shopping to banking, everything is completed and recorded online and requires a high level of security measures. As Covid-19 impacted the world, employers were forced to deploy their workers to work from home which resulted in a significant impact on IT infrastructure requirements and a scramble to ensure that security controls were in place to support remote working. For some agencies, this was too costly and they remained vulnerable to the exigencies of hackers.

Data has shown that the five most common cyber threats are:

·Ransomware;
·Phishing;
·Hacking;
·Data Leakage; and
·Insider threat.

While cyber-attacks on information and communication technology systems continue to rise globally, financial services continue to be the most targeted industry.

The Caribbean is often missed out on reports of 'ransomware' attacks but the region is just as susceptible as the rest of the world. Ransomware is one of the deadliest types of cyber-attack. The malware encrypts files and documents and often facilitates exfiltration, preventing work, locking up important information, and then threatening to leak or expose the information in exchange for an enormous amount of money. Once the money is paid, then a decryption key is provided. Often the ransomware is paid because companies and/or organisations do not want the leak to be made public as it may lead to a public lack of confidence in the company and their ability to safely store personal information.

A previous Hitachi Security blog (16 November 2020) mentions a report by PricewaterhouseCoopers (PwC) (See link below) warning that Caribbean firms were "*not paying enough attention to cybersecurity risks*". It said that businesses based in the Caribbean must take preventative action to stop the impact of ransomware attacks already experienced by other areas of the world: Impacts that affect finances, reputation, motivation, and regulatory posture, and that can be a make or break for businesses already under pressure from Covid-19 pandemic challenges.

In October 2020, one of Trinidad and Tobago's largest conglomerates ANSA McAL reported that despite having precautions in place, they had fallen prey to a ransomware attack. A security breach initiated at the Barbados arm of the operations had migrated to Trinidad and affected operations in Tatil and Tatil Life part of the group's financial sector.

The hackers behind the attack REvil claimed to have possession of 'numerous financial documentation, agreements, invoices, and reports' and threatened to make the files public unless a ransom was paid'. According to technestt.com REvil reportedly released the information to the dark web. ANSA's response was that they took the decision '*not to place our people and IT systems at risk by seeking to access the dark web for the purpose of downloading any of these alleged files. As a result, we are unable to verify the authenticity of these claims*'.

Earlier this year in February 2021, Jamaica experienced a massive data breach that exposed the immigration and COVID-19 records of hundreds of thousands of people who visited the island over the past year. It was stated that most of the information found on the exposed server was from American visitors. According to TechCrunch, the Jamaican government contractor Amber Group left a storage server on Amazon Web Services (AWS) unprotected and without a password.

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

Zyber Global Events

Zyber Global's ***Stay Safe Online Webinar*** is Wednesday 31st March 2021 at 1600 hours GMT. ***Register now to attend.***

OTHER CYBER SECURITY EVENTS

ICCC 2021: 15. International Conference on Cyberlaw and Cybersecurity March 15-16, 2021	**NBCPA (CPS) presents:** **A Series of Webinars to inform on Cybercrime and Cybersecurity** March 18, 2021	**Enhanced Cooperation and Disclosure of Electronic Evidence: Towards a New Protocol to the Budapest Convention on Cybercrime** Thursday, 25 March 2021
This Conference 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 and Cybersecurity. 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 and Cybersecurity	This Series of one-hour Webinars is open to NBCPA members and CPS staff only. **Webinar 1: 18 March 2021** An introduction to Cybercrime **Webinar 2 :20 April 2021** Electronic Evidence **Webinar 3: 19 May 2021.** Electronic Evidence and International Cooperation The training will be delivered by Esther George LLB (Hons), LLM, MA, Cybercrime and Cybersecurity Consultant and CEO of Zyber Global Global Centre https://zyberglobal.com/	The Council of Europe, European Union (CoE) and The International Association of Prosecutors (IAP) are jointly hosting a series of four webinars from March to December 2021 on **Enhanced Cooperation and Disclosure of Electronic Evidence: Towards a New Protocol to the Budapest Convention on Cybercrime** This free event is open for participation for criminal justice authorities from countries of Europe, Africa, the Americas and Asia Pacific.
For further information https://waset.org/cyberlaw-and-cybersecurity-conference-in-march-2021-in-london	For further information https://www.nbcpa.org.uk	For further information: https://www.coe.int/en/web/cybercrime/enhanced-cooperation-and-disclosure-of-electronic-evidence-towards-a-new-protocol-to-the-budapest-convention

.

Zyber Global Online Events

Our Online Courses with INsig2

Sign up now at https://insig2-and-zyberglobal.learnworlds.com/

Courses per sectors

Legal Entities
Judges, lawyers and public prosecutors
Customized courses for legal entities on deeper aspects of digital forensics and forensic value of the evidence while collecting, processing, and presenting digital evidence in criminal and administrative proceedings. a subheading

Law Enforcement
First responders, forensic investigators and analysts
Customized courses for law enforcement officials on procedures, techniques, and tools used in digital forensic analysis and how to apply them in their forensic investigations.

Private Sector Corporations and small businesses.
Customized courses for various 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 Reading
- Quiz after each chapter
- Case study final exam

At the end of each course, you will be issued a completion e-certificate which is immediately printable for your records. Certificates bring you CPD (Continuing Professional Development), CPE (Continuing Professional Education), CLE (Continuing Legal Education) points. The number of points depends 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 digital forensics learning path and get the most from your e-learning experience by using course bundles. https://bit.ly/3lNRYsj

Free Courses
Password Management

The course covers different lock security methods, guidelines on securely storing your passwords, various password managers and how to use them
https://bit.ly/3eMu7FD