Zyber Global

MAY 2022 | ISSUE 22

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 22nd Edition, May 2022 of Zyber Global Centre's monthly newsletter.

I was recently speaking at an online pre-course meeting organised by the Pacific Islands Law Officers' Network (PILON) Cybercrime Working Group and the Attorney-General's Department, Australia (AGDA).
The purpose of the meeting was to explain the features of the Zyber Global - INsig2 Digital Forensics Intermediate Course and answer any questions that may arise.

We heard opening remarks from Attorney General Linda Folamoetu'i of the Kingdom of Tonga and Chair of the PILON Cybercrime Working Group, who emphasised the pressing need to develop skills to tackle cybercrime, which has been fuelled by COVID-19 and technological change.
We then heard from Lucy Sargeson, Director of the Pacific Section AGDA, who reiterated the importance of the course and explained the bigger picture of Pacific partnerships – including the work of the Australian Federal Police.

My colleague Krešimir Hausknecht (Head of Digital Forensics, INsig2) and me gave some background into the course's development, and some practical experiences from Europe. Lauren Murray and Nick Wilson of the Pacific Section AGDA provided closing remarks.

It was during that meeting, that I realised that it was 20 years ago when I was a Senior Prosecutor with the UK Crown Prosecution Service (CPS) and was appointed the Project Manager for the CPS High-Tec Crime Project. This opened up a whole new world for me of designing and developing training courses such as the CPS ' National High-tec Crime training course for prosecutors and others. This led me to initiating and designing the Global Prosecutor E-Crime Network (GPEN) which was launched in 2008 to enable cybercrime prosecutors around the world to learn and benefit from sharing information, experiences, and strategies with each other.

Looking back I can now put the pattern together and see my journey unfold to where I am today. I am glad that I am part of the bigger picture in helping to train so many committed and talented people. The future is in safe hands!

We continue with our usual features and ask that you engage with us and let us know what topics on cybercrime you would like to hear more of.

The next Stay Safe Online webinar is on the 31 May 2022, so do register early. Stay well!

BEST REGARDS
ESTHER GEORGE

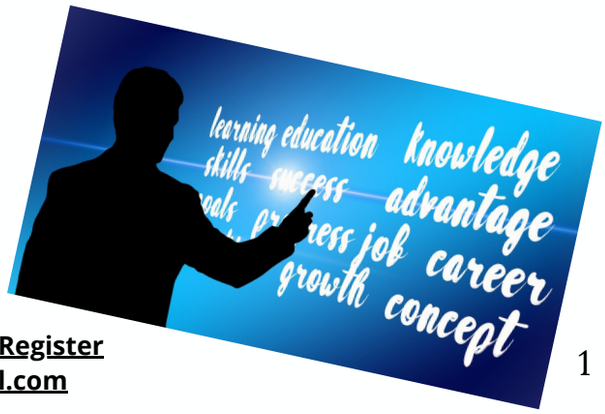
Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Focus
This article is on Money-Mules, which is the second in a series on '*Cyber-Money Laundering*'

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

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



Zyber Focus Article

Cyber-Money Laundering: Part II Money-Mules

Arsha Gosine, Head of Research,
Zyber Global Centre

Criminal money is always everywhere, looking for a way into the legal mainstream – suborning existing accounts to become mules is far easier in some jurisdictions,
Colin Holder, CEO, Identity Intelligence Ltd

Money laundering is the process of making money clean! It underpins most criminal activities and usually has a financial motivation.

Cyber- money laundering goes a step further and is the online digital process of taking profits from crime and corruption and transforming them into legitimate assets. It takes criminally derived 'dirty funds' and converts them into other assets so they can be reintroduced into legitimate commerce. This process conceals the true origin or ownership of the funds, and so 'cleans' them. Following the money is sometimes difficult for law enforcement agencies due to the use of highly sophisticated technologies.

Over the last few years cyber-money laundering has increased exponentially. Covid-19 brought a 'tidal wave of fraudulent activities' in many forms and there seems to be no abatement. The tactics used get more sophisticated daily. Moyara Ruehsen, Associate Professor and Director of the Financial Crime Management Programme at the Middlebury Institute of International studies, Monterey, California, USA said that business email compromise (BEC) is still a huge problem, as is ransomware. The ransom demands continue to grow and both State and private entities continue to be targeted. The threat remains, if you don't pay up, private personally identifiable information will be released. Once your personal information is out there, nothing can be done.

We now look at Money – mules who are individuals who wittingly or unwittingly help criminals launder money through their individual and business checking accounts. Professor Ruehsen states that although this technique has been around for decades, there has been a surge in this typology since the Covid-19 lockdowns. This is because people are spending more time at home on their computers and responding to "work from home" ads and other dubious schemes.

Professor Ruehsen says that It's a target rich environment for criminals looking for naïve marks online, who can be persuaded to move criminal funds through their accounts. Criminals use 'mule accounts' to launder their ill-gotten gains which is a constant problem for financial institutions fighting financial crime and trying to prevent them accessing the global financial system. Failure to stop the activity can also result in material financial penalties.

University students are often targeted by criminals and organised crime gangs on Snapchat and Instagram where they are trucked into clearing dirty money in return for 'easy' money. However, the moment a victim chooses to take part in a scam of this nature, they themselves become complicit in the crime. In the UK, the penalty for such a crime is up to 14 years imprisonment.

In 2017 UK banks identified 8,500 money mule accounts owned by people under the age of 21- some belonging to teenagers as young as 14, according to Cifas, the UK's Fraud Prevention Community. Young people are the perfect target for fraudsters, as their accounts are likely to be "clean" without a history of criminal activity, and they might not understand the potential repercussions of taking part in a scam like this.

One victim who was approached to become a money mule at only 15 said "I had nothing in my bank account, I figured I really had nothing to lose. They couldn't steal any of my money - I had none." However, after her money mule transaction was noticed by her bank her account was closed down, she didn't see any of the money and she was left without a debit card for months.
Colin Holder, CEO, Identity Intelligence Ltd says that fraudsters create mule accounts either by taking over the account of a legitimate customer, or when a customer knowingly, or unknowingly, receives and transmits payments through their account. Alternatively, criminals exploit the inadequate client onboarding procedures used by the "challenger" banks, which are often more about a "seamless" customer experience than identifying who they are actually dealing with.

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

Zyber News Roundup

WhatsApp warning as all 2 BILLION users told to delete text immediately

All WhatsApp users are being warned to look out for a dangerous type of scam text. Crooks are now posing as WhatsApp Support to hoodwink you into handing over private info.

Messaging apps are popular with scammers who want to steal your information or money. Popular WhatsApp blog **WABetaInfo** is now warning users to watch out for fake "support accounts". These tricksters use profile pictures that look official and verified.

******* WARNING *******

If anyone ever asks for your login code or banking info over WhatsApp, be very cautious and don't reply.
You can also block and report the scammer within WhatsApp, which will alert the real support team about the issue.

Read more:
https://www.thesun.co.uk/tech/18380304/whatsapp-warning-text-danger-delete/?rec_article=true

European Union Has Rules On Illegal Online Content

Big Tech companies will have to meet new European Union (EU) requirements to curb illegal content and disinformation on their platforms.

This comes after negotiators reached a landmark deal on how Europe governs the Internet, as the EU lawmakers have agreed on new rules requiring tech giants such as Google, Twitter and Facebook, among others, to do more to moderate illegal content on their platforms. The wide-ranging Digital Services Act (DSA) can fine a company up to 6% of its global turnover for violating the rules, which would be $7bn (£5.9bn) in the case of Facebook's owner, while repeated breaches could result in a tech firm being banned from doing business in the EU. Executive Vice-President for a Europe Fit for the Digital Age, Margrethe Vestager, added: "*With the DSA we help create a safe and accountable online environment...* "

Read more:
https://www.cybersecurityintelligence.com/blog/eus-new-online-rules-on-illegal-content-6267.html

AUSTRAC new guidelines aims to help fight digital currency cybercrimes

The Australian Transaction Reports and Analysis Centre (AUSTRAC) is determined to work with businesses to curtail financial crimes connected to digital assets. The financial compliance enforcement agency has released two new guidelines for businesses to protect themselves and their clients from cybercrime.
In a notice, AUSTRAC said that even as digital assets are getting more popular and valuable, their employment in criminal activities is also increasing. In 2020-21, 500 ransomware attacks were reported, marking a 15% increase from the previous fiscal year, the body found.
"*Financial service providers need to be alert to the signs of criminal use of digital currencies, including their use in ransomware attacks*," AUSTRAC CEO Nicole Rose said.

Read more: https://coingeek.com/austrac-new-guidelines-aims-to-help-fight-digital-currency-cybercrimes/

Binance wants out of $8M romance scam, denies any responsibility

Binance exchange is in court in a digital asset romance scam case in which the victim claims it should have done more to protect its users. The exchange filed in a Texas court to be exempted from the $8 million lawsuit, arguing that it doesn't fall under the jurisdiction of the Texas court.

Divya Gadasalli filed a lawsuit in a federal court, claiming that Binance failed in its duty to stop the scammers. She allegedly lost digital assets she had purchased on Coinbase to the scammers and believes that Binance, fellow exchange Poloniex (which is now owned by TRON founder Justin Sun), and American banks TD Bank and Abacus Federal Savings Bank should be held liable for the loss. She is demanding $8 million from the defendants. Binance has fought back and the exchange told a Texas federal court that the plaintiff based her allegations on 'paper-thin assertions' and that she had failed to establish a claim. Binance further claimed to be beyond the jurisdiction of the Texas court as it doesn't operate in the United States. Being a foreign entity, it was beyond the reach of the local Texan civil laws, its filing claimed. Digital asset romance scams have been on the rise, with scammers faking an emotional connection to their victims before convincing them to either send them digital assets or invest in a dubious company.
Read more: https://coingeek.com/binance-wants-out-of-8m-romance-scam-denies-any-responsibility/

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

4th IAP Africa and Indian Ocean Regional Conference Effective Mechanisms to Respond to Emerging and Transnational Organised Crime in Africa: Country Experiences and Challenges **May 16 - 20, 2022** **Mombasa,Kenya**	**IAP / COE series of online webinars.** Webinar 5 - Data protection safeguards and principles in cybercrime investigations **23rd of May 2022 at 15.00 (Central European Time.)**	**ICCCC 2022: 16. International Conference on Cybersecurity, Cybercrime and Cyberthreats** **May 23rd - 24th 2022** **Montreal, Canada**
We are very pleased to announce that the Online Registration for the 4th IAP Africa and Indian Ocean Regional Conference is now open. The event is hosted by the Director of Public Prosecution of Kenya at Sarova Whitesands Beach Resort in Mombasa, Kenya from 16 – 20 May 2022 under the title "Effective Mechanisms to Respond to Emerging and Transnational Organised Crime in Africa: Country Experiences and Challenges". Please note: The number of participants is limited to 120. Registration will be accepted on "first-come, first-served basis", register now. Deadline for registration is 9 May 2022. You can find the provisional programme and more information about this event on the conference website from which you can also access the Online Registration System.	The International Association of Prosecutors, the GLACY+ project of the Council of Europe and the European Commission and the Octopus project of the Council of Europe are co-organising a series of thematic webinars to exchange views and share experiences on the existing and new forms of cooperation for effective access to electronic evidence, as well as solutions proposed by the 2nd Additional Protocol to the Budapest Convention. The webinar will be held in English and the discussion will be recorded. Cybercrime is a threat to human rights, democracy and the rule of law. Criminal justice authorities are confronted with a continuous increase in the scale and quantity of cyber offences and other electronic crimes. The COVID-19 pandemic is accompanied by further proliferation of cybercrime.	You are invited to a series of webinars jointly organised by the IAP and the Council of Europe on the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence from May 2021 to May 2022. The fifth thematic webinar to be organised on 23rd of May 2022 will focus specifically on Data protection safeguards ensuring that personal data received under this Protocol will be protected.
For further information: **https://events.iap-association.org/Mombasa2022/Home**	For further information: Registration is now open for the webinar. **https://primetime.bluejeans.com/a2m/register/zzedfxhh** **before 20 May 2022, 15h00 CET.**	For further information: **https://waset.org/cybersecurity-cybercrime-and-cyberthreats-conference-in-may-2022-in-montreal**

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