Zyber Global

APRIL 2021 | ISSUE 9

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 9th Edition, April 2021 of Zyber Global Centre's Monthly Newsletter

I had a great time last month delivering training on cybercrime to my former colleagues, who are members of the National Black Crown Prosecution Association (NBCPA). The NBCPA is hosting a series of three one-hour webinar training sessions from March to May 2021 on Cyber Crime. The next webinar 'An Introduction to Electronic Evidence' will be held on 20th April 2021. The full details for this webinar can be found on the event page.

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Spotlight

The interview spotlight this month is on Mr. Adem Galip Dinçtürk, Chief Judge of the 8th Criminal Chamber, Ankara Regional Court of Justice, Republic of Turkey

Zyber News

This is a roundup of the latest international cybercrime news.

Zyber Focus

This month, the focus is an excerpt of Esther George's presentation and training to the NBCPA by Arsha Gosine, Head of Research, Zyber Global Centre

Zyber Global Events

The next Stay Safe Online Webinar by Zyber Global is on Wednesday 30th April 2021.

" We must be well educated in using technology in all areas of our lives. We must learn how to use this technology in the best and safest way for ourselves and society. We should especially learn how to protect ourselves when using the internet!

Mr. Adem Galip Dinçtürk
Chief Judge of the 8th Criminal Chamber, Ankara Regional Court of Justice, Republic of Turkey

Continued from page 1.....

As we celebrate Easter this weekend it means that lent is over. I gave up chocolate, sweets, biscuits, and cakes for lent and I also took up exercising (walking) three times a week. I feel like shouting "I made it!" It's been a long 40 days but I hope to see if I can keep doing this even when lent ends as I am sure that I am a lot healthier. Normally Easter for me is going to church on Good Friday and Easter Sunday and then getting together with family and friends to celebrate and catch up. This year it may be different with online services and zoom family calls, but we can all still experience the joy of Easter.

The next Stay Safe Online webinar is on 30 April 2021, so do register early. These are tailor-made sessions to help you to understand how to and why you should be safe online.

We hope your Easter is filled with hope, peace, and brightness. Happy Easter!

Be well, stay safe....and do drop us a line on what you would like to read about in our May edition! We always look forward to hearing from you with your suggestions.

ESTHER GEORGE
Editor and CEO Zyber Global Centre

Zyber News Roundup

Cybercriminals are increasingly selling forged vaccination certificates on the darknet

As demand for COVID-19 vaccines increases and people become frustrated with delays in getting their shots, there is a growing market for forged vaccination cards.
A new report from Check Point Research says there has been a surge in fake vaccination certificates online, via the darknet. Users send their details and $200 to hackers and, in return, receive an official-looking vaccination card.

There's also a strong market for negative COVID-19 tests among travellers, including a "buy two, get the third for free" deal. These falsified results can be purchased for $25 in less than 30 minutes.

Check Point says advertisements for fake vaccination documentation are up 300% since January. More worrisome, there's also a growing market for counterfeit coronavirus vaccines.

It's imperative for people to understand that attempting to obtain a vaccine, a vaccination card, or negative COVID-19 by unofficial means is extremely risky, as hackers are more interested in your information and identity for exploitation."

Read more:
https://fortune.com/2021/03/23/covid-vaccine-cards-fake-vaccination-certificates-darknet-cyber-criminals-selling/

continued on page 4.....

Zyber Spotlight

Mr. Adem Galip Dinçtürk
Chief Judge of the 8th Criminal Chamber, Ankara Regional Court of Justice, Republic of Turkey.
Mr. Dinçtürk is an experienced and extremely knowledgeable Judge who has a specialism in cybercrime. He is an influencer and leader in his approach to tackling cybercrime nationally.

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

After graduating from Ankara University Faculty of Law, I started my career as a candidate Judge and Public Prosecutor and was duly appointed as a Public Prosecutor. After serving as a Public Prosecutor for about 12 years, I was appointed as Rapporteur Judge to the Court of Cassation. I worked in the Criminal Chambers of the Court of Cassation dealing with cybercrimes and the Criminal General Assembly of the Court of Cassation.
During this period, I attended National and International meetings and made presentations on cybercrimes. I participated in all studies of the European Union and the Council of Europe Joint Project - iPROCEEDS.
I also lecture on cybercrimes at the Justice Academy of Turkey to Judges and Public Prosecutors. This is in addition to my daily duties as the Chief Judge of the 8th Criminal Chamber at Ankara Regional Court of Justice, where I was appointed in 2016 and am still there to date.

Like many countries, since the pandemic, it was reported in the news that the Republic of Turkey has seen a prolific rise in the number of phishing sites designed to steal people's online details. How has the Republic of Turkey been responding to that threat?

Since the pandemic, as in many countries, a rise in cybercrime happened in the Republic of Turkey as well. Banking and other important information of companies, government and consumers were targeted. Those exposed to these attacks were harmed.
The current legal regulations in the Republic of Turkey has been sufficient to cover these kinds of crimes. There was no difficulty in terms of legal regulation. That is because our existing laws allowed this combat. However, the biggest problem is international cooperation in reaching the perpetrators. Especially the lack of public-private cooperation, the resistance of multinational service providers such as Facebook, Google, Instagram, Snapchat in sharing information. In order to break this resistance, legal regulations were made by the Republic of Turkey for such service providers to open representative offices in Turkey.
The Republic of Turkey made attempts to raise the awareness of the public against this threat. The awareness of the public was raised in this context by the visual and written media, who warned about cybercrimes and informed the public as to how to protect themselves against these crimes.
In addition, in terms of crimes committed through informatics, law enforcement, ministries and banks enlightened the public and institutions with SMS, radio, television, public spots and banners, posters, advertisements, films, and similar methods in public places in order to protect against this threat. I can say that these activities have been very useful in the combat against cybercrimes.

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

Zyber News Roundup
cont'd.....

EUROPEAN BANKING AUTHORITY ATTACKED (EBA)

The EBA has taken all its email systems offline as its Microsoft Exchange Servers have been hacked by what might be a Chinese state-backed hacking group.

The EBA isn't the only organisation under attack, as there are a lot of hacking groups across the world exploiting vulnerabilities to Microsoft's unpatched servers. The Agency has swiftly launched a full investigation, in close co-operation with its ICT provider, a team of forensic experts, and other relevant entities.

Microsoft has recently issued emergency patches, but these do not fix systems that have already been attacked. Many of the victims appear to be small or medium-sized businesses although larger groups like the EBA have also been hit.

The EBA says that access to personal data through emails held on MS Exchange servers may have been obtained by the attacker. It is currently scrambling to identify what, if any, data was accessed. The EBA has provided the following statement:

"*The Agency has launched a full investigation, in close cooperation with its ICT provider, a team of forensic experts and other relevant entities*,"

Microsoft has attributed the attack to Hafnium, a state-sponsored hacking group operating out of China. The attack, which Microsoft has said started with a Chinese government-backed hacking group, has so far claimed at least 60,000 known victims globally, according to a former senior US official with knowledge of the investigation.

Read more:
https://www.cybersecurityintelligence.com/blog/european-banking-authority-attacked-5520.html

BRITISH COMPANIES COMPROMISED BY EXCHANGE EMAIL HACKING

Hundreds of British companies have been hacked and threatened with ransom payments to recover their vital data as part of a global campaign that Microsoft say is linked to Chinese state-sponsored hackers. The British National Cyber Security Centre (NCSC) is warning businesses to urgently update their Microsoft email servers following a state-sponsored espionage campaign. Governments around the world are warning organisations to secure their systems.

Leading cybersecurity firm ESET thinks there have been more than 500 email servers in the UK that may have been hacked and many companies are not aware they are victims of the attack. Indeed, it may well be too late, as at least 10 hacking teams are taking advantage of the resulting chaos.

The NCSC has joined US authorities in issuing warnings about the hack but says it is still assessing the situation for UK businesses. The Norwegian national cybersecurity agency is actively scanning for companies at risk in the country and is warning them directly.

Zero-Day Attack

The hacking campaign was first announced by Microsoft on 2 March and blamed on a Chinese government-backed hacking group called Hafnium. Microsoft said the group was using four hacking techniques not seen before to infiltrate the email systems of US companies. The attackers targeted the popular email system Microsoft Exchange Server, used by large corporations and public bodies across the world.

Read more:
https://www.cybersecurityintelligence.com/blog/british-companies-compromised-by-exchange-email-hacking-5536.html

Zyber Focus

Excerpt from Ms. Esther George's Presentation and Training to the NBCPA

On March 18, 2021, Ms. Esther George, Cybercrime Specialist, gave an '*Introduction to Cybercrime*' for prosecutors and interested persons from the Crown Prosecution Service (CPS) through the auspices of the National Black Crown Prosecutors Association (NBCPA).

Harvey Palmer, the CPS Cybercrime Policy lead, introduced the session by saying that cybercrime had so many facets and elements to it. There are cyber-dependent crimes like hacking and then there are cyber-enabled crimes like encryption etc. He pointed out that there are so many levels on which cybercriminals exist and operate, and there are a range of victims from the individual to government agency to corporate entities. He mentioned the Integrated Review on building the UK's national resilience which was recently published. Cybersecurity was one area touched upon. Mr. Palmer went on to say that there were many challenges with cases involving cybercrimes especially evidence gathering from overseas. He said that he would like to see changes in the Cybercrime Act.

Ms. George gave a succinct and interesting presentation on cybercrime. She said that a study by the United Nations in 2013 stated that there was no one definition of cybercrime. However, they found that cybercrime had fourteen (14) characteristics.

Ms. George said that the definition depended on the country. For example, the UK's National Cyber Security Strategy defined cybercrime as cyber-dependent and cyber-enabled. This meant that:
Cyber-dependent crimes are those crimes that can be committed only through the use of information and communication technology (ICT) devices.

While cyber-enabled crimes are traditional crimes that can be increased in scale or reach by the use of computers, computer networks, or other forms of ICT.

There are many types of cybercrimes and many offences which have a cyber link to them.
For example:

- Ransomware
- Phishing
- Fraud - online
- Cyberstalking
- Child Abuse Images and Online Grooming
- Identity Theft
- Denial of Service Attacks
- Theft - online

We also see that as technology improves, the hackers also improve their response to cybersecurity. In fact, research shows that hackers attack every 39 seconds.

Finally, there are many reasons why cybercrime remains a continuing challenge. This could be due to the fact that there are more countries online. For example, The Pacific Islands has in recent years upgraded their information and communication technology. This led to an increase in cybercrime incidents.
Other reasons why cybercrime remains a challenge include:

- the under-reporting of crimes
- anonymity of technology
- cloud remote storage
- complexity of offending
- increased usage of social networking sites
- the Dark Web and Virtual Currency

In the final analysis, the field of cybercrime is vast and it is incumbent on us all to take responsibility for our online usage, whether it be computers, mobile phones, data sticks, or even the humble oyster card. It is vital that we keep our personal information safe and Ms. George provided some tips to keep safe online.

The next training session is on 20 April 2021....see the events page for further information.

Zyber Global Events

Zyber Global's ***Stay Safe Online Webinar*** is Wednesday 30th April 2021 at 1600 hours BST. ***Register now to attend.***

OTHER CYBER SECURITY EVENTS

International Conference on Cloud Cybersecurity April 22-23, 2021 New York, USA	**NBCPA (CPS) presents: A Series of Webinars to inform on Cybercrime and Cybersecurity** April 20, 2021	**The 1st Webinar: Direct Co-operation with Service Providers in Foreign Jurisdictions** April 27, 2021
This ICCC 2021: International Conference on Cloud Cybersecurity aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Cloud 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 Cloud Cybersecurity	This Series of one-hour Webinars is open to NBCPA members and CPS staff only. **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, 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/cloud-cybersecurity-conference-in-april-2021-in-new-york	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#{%2289787852%22:[3]}

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