Zyber Global

AUGUST 2020 | ISSUE 1

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the first edition of our monthly newsletter.

I am very excited to launch this newsletter which will inform and inspire you on a monthly basis about all things Zyber.

You'll find that it is filled with educational information, helpful hints and tips, news, events, and even some discount offerings.

We want this newsletter to be valuable for you so please share your feedback and suggestions to help us improve.

Esther George, CEO
www.zyberglobal.com

This Month's Features

Zyber Spotlight
The interview spotlight this month is on Krešimir Hausknecht, Head of Digital Forensics Department at INsig2, Croatia a leading provider of digital forensic services based in Zagreb Croatia

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

Zyber Focus
Our focus this month looks at Scams and Covid19; this feature is by our Head of Research Arsha Gosine.

Zyber Global Events
The next Stay Safe Online Webinars by Zyber Global are due to take place on the 27 August and the 29 September 2020 register now to attend.

Coming soon:
We have an exciting new webinar series in development for later this year.

We wish you a relaxing summer break!

"For those who want to be safe online, it is all about awareness and education."

***KREŠIMIR* HAUSKNECHT**, HEAD OF DIGITAL FORENSICS DEPARTMENT AT INSIG2.

Zyber Spotlight

Leading Lights

Interview with Krešimir Hausknecht,
Head of Digital Forensics Department at INsig2

Can you tell us about your background and career?

I am from Croatia although I have a German surname. I am currently the Head of Digital Forensics Department at INsig2, where I have worked for the last seven years where our main focus is providing training in the field of Digital Forensics. I find digital forensics highly interesting and lots of fun. It is what I would do in my spare time, so doing it as a day job is very rewarding and fulfilling. It is my dream job.

What is your vision for INsig2 and Zyber Global online training programmes?

Initially we recognised that there was a need for education and training among law enforcement personnel primarily, lawyers, prosecutors and judges. We saw experts were being called to give evidence in court at great cost. Our thinking was if law enforcement personnel were trained on the subject, they would have a better understanding of what was required in working with digital evidence. InSig2 and Zyber Global both have online courses to address these issues. The online classes are easy to understand and takes the end user through practical and real life examples. There are quizzes along the way to test the knowledge acquired. There is communication and interface between the tutor and the end user with courses being graded manually. Certificates are awarded to those who have passed the assessments. These courses are great for the total beginner and more experienced persons; IT professionals; law enforcement personnel; companies; government agencies and those who want to be safe online. It is all about awareness and education.

(For the full interview see https://zyberglobal.com/my-blog)

What do you think are the major cyber challenges facing the world today and how would we overcome them?

Cyber challenges have changed rapidly especially with Covid-19. There has been a huge increase in online fraud as many are trying to earn money. Hackers and scammers are exploiting the fact that a large section of the population is

working from home. There are many cases of malware and ransomware being reported. Another big problem is that companies have spent the last decades building their IT infrastructure and now in a matter of months with Covid-19 this has been eroded. By this I mean that workers are working from home without a secure connection and this can create problems for the security of their companies. The other issue is the use of shared devices which is a security risk....

Finally, I would like to say that the weakest link in the chain is the average man in the street with a lack of awareness and understanding on the intricacies of surfing the web and knowing how to spot the online hackers and scammers. Basically how to keep safe online. I would like to stress that education is key; knowing how to use these devices responsibly and safely. We need to invest in our children and educate them on being aware and safe online as cyber technology continues to advance rapidly.

(For the full interview see https://zyberglobal.com/my-blog)

"The weakest link in the chain is the average man in the street with a lack of awareness and understanding on the intricacies of surfing the web and knowing how to spot the online hackers and scammers"

***KREŠIMIR* HAUSKNECHT,**
HEAD OF DIGITAL FORENSICS DEPARTMENT AT INSIG2.

Zyber Roundup

Data Breaches

The Zyber News Roundup this week is on prominent recent data breaches. If you think that your personal information might have been exposed call the company concerned or go to their secure website to confirm the breach and find out if your information was compromised. Change your passwords, security questions etc for that account and any other accounts that have similar passwords. If you have not already done so ensure that you implement two-factor authentication.

US DIGITAL BANK DAVE ADMITS CUSTOMER DATA BREACH

A US fintech giant has admitted that it suffered a breach of customers' personal data via a third party supplier, after researchers found a database containing millions of records for sale online. LA based Dave offers digital banking services, and in 2019 hit a valuation of $1bn after just two years in business.

However, reports emerged over the past week that its customers' details were being traded on the dark web. Prolific cybercrime trader **ShinyHunters released the trove** for free on Friday, although in the weeks previous it was being auctioned by a new user on a separate forum.

It is claimed that there are over 7.5 million records associated with three million email addresses in the haul.

Read the full story here: https://www.infosecurity-magazine.com/news/us-bank-dave-admits-customer-data/

GARMIN SERVICES AND PRODUCTION GO DOWN AFTER RANSOMWARE ATTACK

Smartwatch and wearable maker Garmin planning multi-day maintenance window to deal with ransomware incident.Smartwatch and wearables maker Garmin shut down several of its services on July 23 to deal with a ransomware attack that has encrypted its internal network and some production systems.In messages shared on its website and Twitter, Garmin said the same outage also impacted its call centres, leaving the company in the situation of being unable to answer calls, emails, and online chats sent by users.It remains unclear if any customer data has been lost or stolen during the incident.

Over the past several months, ransomware gangs have modified their modus operandi to also include data theft besides file encryption.

Read the full story here: https://www.zdnet.com/article/garmin-services-and-production-go-down-after-ransomware-attack/?fbclid=IwAR1YVkNR-lSuuciTq4vArLwxa2XGdIZwVQrgler9pdEm89rDBKqvUSvZ8jw

For full Zyber Roundup here: https://zyberglobal.com/my-blog

For up to date cyber news follow me on twitter: https://twitter.com/Esther_George or https://www.linkedin.com/in/esther-george/

Zyber Focus
COVID-19 Online Scams by Asha Gosine - Zyber Global Head of Research

As Covid-19 overtook the world, cyber threats were evolving at an alarming rate. As more and more people began working from home, scammers and hackers seized opportunities to send out phishing emails; ransomware; and malware to infiltrate and wreak havoc on computer systems. Their ultimate gain to steal people's identities and/or defraud them in some way.

Action Fraud has since stated that more than £5M has been lost to fraud since February 2020. One of the more common and prolific scams relate to pension and investments.

The BBC also reported on a few phishing scams in the UK. No one was spared as both individuals and industries were targeted.

The most popular scams were hinged on the Coronavirus. So for example, 'phishing' emails were sent that tried to trick users into clicking on a bad link. Once clicked, the user is sent to a dodgy website which could then download malware onto your computer, or steal passwords. The scams may also claim to have a 'cure' for the virus and there were scammers who claimed to be from the World Health Organisation (WHO). They stated that there were ways in which the virus could be prevented, of course for a small fee. Phishing emails could also offer a financial reward or encourage you to donate.

Another example were scammers who purported to be from the HMRC texting, emailing and/or phoning taxpayers offering spurious financial advice and offering bogus Covid-19 tax refunds. They also threatened arrest if the taxpayer did not pay the fictitious tax owed. It is usually the elderly and the vulnerable who would fall prey to these scams.

The likely conclusion here is to be aware, question everything. Scammers are now using more and more sophisticated technology to create websites that look like the real thing. The psychology of the scam is based on the empathy created by the scammer so do check the official website.

Remember: Never accept any unsolicited emails regarding your finances. Check with your Bank, know their security procedures. Do not be rushed into taking financial decisions especially where you have to part with your money. You can always check with the Financial Conduct authority that the firm you are dealing with is bona fide.

Contact 'Action Fraud' if you think something is not quite right. Safeguard yourself - If something looks too good to be true that is probably because it is! **We are holding webinars on how to stay safe online - sign up now.**

Be aware, question everything!

Zyber Global Events

The next **Stay Safe Online Webinars** by Zyber Global are due to take place on the 27 August and the 29 September 2020. Register now to attend.

Other Virtual Cybersecurity Events in 2020by Juliana De Groot
Source:https://digitalguardian.com/blog/top-50-must-attend-information-security-conferences

Black Hat USA @BlackHatEvents August 1-6, 2020	DEF CON 28 @defcon August 6-9, 2020	AusCERT 2020 @AusCERT September 15-18, 2020
Black Hat USA is the world's leading information security conference. Now in its 23rd year, Black Hat USA will be held entirely virtual in 2020. Trainings will be held from August 1st through the 4th, with briefings taking place on August 5th and 6th. Learn the latest in cutting-edge research on information security risks and trends from security experts from around the world.	DEF CON is a leading hacking conference. DEF CON 28 SAFE MODE will be held virtually. On August 6th, the DEF CONdiscord.io/dc server will open up for attendees to join and begin their DEF CON 28 SAFE MODE experience. Attendees can look forward to a new online MysteryChallenge, remote Capture the Flag events, villages, contests, and even a remote movie night.	The 19th annual AusCERTConference will be held virtually this September, featuring more than 50 speakers, plus workshops, tutorials, networking opportunities, and more. Attendees can attendsessions, interact with cybersecurity and information security thought leaders, andnetwork with peers from around the world, all from the comfort of their home or office.
Cost to Attend: $995USD	Cost to Attend: Free	For more information: www.conference.auscert.org.au

Zyber Global Events

Our Online Courses with INsig2 –
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/
For an extra 15% off use coupon code **ZYBER** during checkout.

Legal Entities

Judges, lawyers and public prosecutors

Customised 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.

Law Enforcement

First responders, forensic investigators and analysts

Customised 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

Customised 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.

Try our free course on Password Management
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/