Zyber Global

MARCH 2024 | ISSUE 44

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the March edition of Zyber Global Newsletter, the 44th edition!

Explore the most recent and exhilarating updates from the fast-paced world of cybersecurity with us!"

February, the shortest month, seemed to fly by even quicker this leap year with its bonus day. Interestingly, I crossed paths with a leap day baby who shared a peculiar challenge – not the rare birthday celebrations you'd expect, but rather the struggle with airlines and travel sites that fail to recognize February 29 as a valid date. It's a quirky reminder of the unexpected twists life throws our way, beyond the anticipated wait for quadrennial birthday gifts!

In February, I had the privilege of being invited by Lawrence McEwen, Executive Director, EST Applied Intelligence UK, to participate as a panellist at the Cyber Security & Financial Inclusion Symposium. The panel discussion on cybercrime, protecting customer data, regulatory frameworks and compliance was very well received.

Lawrence McEwen, a renowned expert in cyber security, organized this event in collaboration with Rokel Commercial Bank to celebrate Dr. Ekundayo Walton Gilpin, the bank's Managing Director, who was honoured as Africa's Best Banker of the Year 2023.

The event took place at the Freetown City Council Auditorium Hall, assembling esteemed professionals from the cyber security sector, government representatives, financial entities, telecom firms, and industry regulators. The focus was on the critical importance of cyber vigilance across various business technology interfaces for secure data exchange and to elevate awareness about financial inclusion and cyber security within Sierra Leone.

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

At the symposium, Dr. Walton Gilpin, the bank's Managing Director, highlighted the bank's top five priorities: developing a cashless ecosystem, automating banking processes, driving digital transformation, bolstering cybersecurity resilience, and achieving gender parity. Lawrence McEwen shared insights on the pivotal role of cybersecurity in the financial services sector. The symposium served as a vital platform for shedding light on cyber threats and disseminating the latest methodologies and technological advancements to safeguard the financial infrastructure against cyberattacks.

Lastly, in April, I will have the opportunity to present at the Insig2 Data Focus 2024 conference. The conference will take place on the 9th of April in Zagreb, Croatia. This is a great conference to attend, register here https://insig2.com/en/data-focus/data-focus-2023/ Do arrange to attend and let's meet up at the conference.
In the meantime, let us keep up-to-date and watchful in the dynamic realm of cyber security.

Zyber Focus Article

The Importance of Cyber Hygiene in Personal and Professional Context

Zyber Global Research Team

Last week a friend messaged to say that he had been hacked on Facebook and if I received any weird messages, that it did not come from him. A story that many of us will be all too familiar with. How many times have you received phone calls purporting to be from the Bank or a financial institution seeking your personal details or scamming emails. How many times have you been hacked? It had me thinking about my own accounts and had I secured them properly.

This article reminds us of the things we should be doing to ensure that we are safe online in this burgeoning world of cybercrime.

The latest phrase around the block is 'cyber hygiene'. Alissa Irei, the Senior Site Editor at TechTarget says that 'Cyber hygiene', or 'cybersecurity hygiene', is a set of practices organizations and individuals perform regularly to maintain the health and security of users, devices, networks and data. In the very same way that we engage in regular hygiene practices to maintain our good health and well-being, so too by following recommended cyber hygiene practices, we can keep our data safe and protected. The goal being to keep sensitive data secure and to ensure that we are able to recover that data should there be a successful attack or data breach.

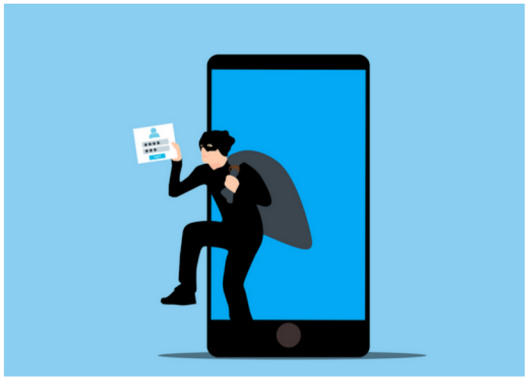
One of the risks that we face today both personally and professional is 'phishing'. This is when criminals use scam emails, text messages or phone calls to trick their victims. The aim is often to make you visit a website, which may download a virus onto your computer, or steal bank details or other personal information.

As of January 2024, the National Cyber Security Centre (NCSC) UK stated that the number of reports received stood at 29M scams which resulted in 168K scams being removed across 306,400 URLs. The NCSC stated that criminals use information about you that's available online (including on social media sites) to make their phishing messages more convincing. However you can reduce the likelihood of being phished by thinking about what personal information you (and others) post about you, and by reviewing your privacy settings within your social media accounts.

For organisations and businesses, TechTarget suggests having a risk based security strategy which would help navigate the constantly shifting threat landscape, enabling security teams to employ and prioritise practices that would safeguard the business while still letting it operate in an efficient manner. Employees also have a part to play as this is a shared responsibility. By following online security measures and best practice for example regularly changing passwords; being wary of suspicious attachments; and ensuring that you are aware of the latest threats and risks.

So, let me ask a question. Can you recognise the signs when someone is trying to scam you or do you know how to check when a message is genuine?

Cyber criminals may contact you via email, text, phone call or via social media. They will often pretend to be someone (or an organisation) you trust. It used to be easier to spot scams. They might contain bad spelling or grammar, come from an unusual email address, or feature imagery or design that feels 'off'. But scams are getting smarter and some even fool the experts. Criminals are increasingly using QR codes within phishing emails to trick users into visiting scam websites. While QR codes are usually safe to use in restaurants, you should be wary of scanning QR codes within emails.



How to check if a message is genuine

If you have any doubts about a message, contact the organisation directly. Do not use the numbers or address in the message – use the details from their official website. Remember, your bank (or any other official source) will never ask you to supply personal information via email, or call and ask you to confirm your bank account details. If you suspect someone is not who they claim to be, hang up and contact the organisation directly. If you have paper statements or a credit card from the organisation, official contact details are often written on them. Think before you act.

Finally, what are some of the best cyber hygiene practices to be aware of?

Cybersecurity is everyone's responsibility, which means that while organizations need to prioritize cyber hygiene, so too must individual employees (personally and professionally).

With that in mind, TechTarget recommends that end users need to be aware of the following cyber hygiene best practices:

- **Backups.** Regularly back up important files to a separate, secure location that would remain safe and isolated if the primary network became compromised.

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

Zyber News Roundup

8,000+ Domains of Trusted Brands Hijacked for Massive Spam Operation

The cybersecurity firm Guardio Labs has uncovered a vast and sophisticated operation dubbed SubdoMailing, which has compromised over 8,000 domains and 13,000 subdomains of reputable brands and institutions since at least September 2022. This malicious campaign, orchestrated by a threat actor known as ResurrecAds, focuses on hijacking legitimate domains to distribute spam emails and monetize clicks through deceitful means. These emails, which impersonate legitimate entities, range from counterfeit package delivery alerts to phishing attempts aimed at stealing account credentials, exploiting the trust and credibility of the hijacked domains to bypass standard security measures and deliver spam and malicious content directly to users' inboxes.

ResurrecAds' operation is notable not only for its scale but also for its technical sophistication, employing a complex infrastructure that includes a variety of hosts, SMTP servers, IP addresses, and even private residential ISP connections. This infrastructure is used to send millions of spam and phishing emails daily, cleverly designed to evade text-based spam filters by presenting the malicious content within images. Upon interaction, these emails initiate a series of redirects that check the device type and geographic location of the recipient, leading them to customized content designed to maximize the attackers' profits through ads, affiliate links, quiz scams, phishing sites, or malware downloads.

The campaign's ability to circumvent email authentication methods like SPF, DKIM, and DMARC is particularly alarming, allowing these malicious emails to appear as if they are sent from legitimate sources.

Read more:
https://thehackernews.com/2024/02/8000-subdomains-of-trusted-brands.html

Cybercrime: Why playing catch-up won't cut it with digital thugs

Cybersecurity challenges are escalating globally, with cybercriminals constantly innovating and diversifying their methods, outpacing the development of defensive measures, and many incidents go unreported. Kenya's recent experience, with a reported billion cyber threats in the last quarter of 2023 alone, underscores the urgent need for improved cybersecurity strategies and international collaboration to combat these threats effectively. Governments and organizations are responding to the increasing threat by enhancing their cybersecurity infrastructure and seeking regional cooperation to address cross-border cyber threats.

Read more :
https://www.trtafrika.com/insight/cybercrime-why-playing-catch-up-wont-cut-it-with-digital-thugs-17084403

Commonwealth training on internet safety praised by Papua New Guinea judges

Judges in Papua New Guinea have received training through a Commonwealth course designed to improve their handling of cybercrime cases, aiming to enhance internet safety for citizens. The training, supported by the UK and conducted in Port Moresby, involved over 40 judges and magistrates who participated in simulations to understand cyber threats and were taught to apply international practices, gather electronic evidence, and engage in cross-border cooperation for prosecuting cybercrimes. This initiative addresses the judicial challenges in tackling the growing issue of cybercrime, emphasizing the need for updated approaches in evidence-gathering and prosecution.

The Asia-Pacific region, including Papua New Guinea, faces a significant rise in cybercrime, with financial implications amounting to about US $1.75 trillion in losses, underscoring the urgent need for specialized training in this field. The training, lauded by local judicial officials, aims to equip participants with the necessary skills to make the internet safer and handle the complexities of cybercrime cases. The Commonwealth Assistant Secretary-General and the UK's Commissioner to Papua New Guinea both highlighted the importance of continuous vigilance and international cooperation to combat these threats effectively, pledging ongoing support for enhancing cybersecurity measures in the region.

Read more:
https://thecommonwealth.org/news/commonwealth-training-internet-safety-praised-papua-new-guinea-judges#:

What impact is AI having on cybersecurity?

A new report underscores the critical role of AI in the cybersecurity industry, with 69% of businesses acknowledging the necessity of AI to manage threats beyond human analysts' capacity. It reveals that AI not only enhances cyber defense mechanisms by improving threat detection and incident analysis but also significantly reduces the financial impact and detection time of breaches. The deployment of AI in cybersecurity is not just a trend but a strategic shift towards a more proactive defense approach, driven by the technology's ability to process vast amounts of data in real-time and identify potential threats that might elude human oversight.

However, the rise of AI in cybersecurity presents a double-edged sword as hackers leverage AI to orchestrate more sophisticated and personalized cyber-attacks, leading to an unprecedented surge in cybercrime.
This growing threat landscape has prompted concerns that AI technologies might render organizations more susceptible to attacks.; highlighting the urgent need for enhanced security measures and AI-driven defenses to counteract these evolving threats.

Read more:
https://www.thehrdirector.com/business-news/ai/impact-ai-cybersecurity/

DATA FOCUS 2024

9th of April | Hilton Garden Inn,
Zagreb, Hrvatska

International Conference on Digital Forensics and Digital Evidence

Join us for the DATA FOCUS 2024, where we bring together law enforcement investigators, prosecutors, judges, court expert witnesses, and other experts, and let them talk about their experiences with digital evidence and digital forensic investigations. Don't miss this opportunity to enhance your skills and be inspired.

Register now!

https://insig2.com/en/data-focus/data-focus-2023/

The Data Focus conference is divided into several sections:

Investigation section
Lecturers address technical aspects of finding, preserving, and processing digital evidence and the legal presentation of digital evidence in criminal and administrative proceedings.

Technical section
Experts provide lectures showcasing and demonstrating the latest products, services, and trends in the digital forensic field.

Legal section
Lecturers explain the legal aspects of collecting, processing and presenting digital evidence in criminal and legal procedures.

Workshops
At the event, our partners will conduct a series of workshops, providing participants with opportunities for personalized inquiries and live demonstrations.

The speakers are from different backgrounds: Ministry of Interior (digital forensics experts), State Attorney office, CERT.hr - the national body for prevention from cyber threats and protection of the security of public information systems in the Republic of Croatia, UNODC, and others.

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

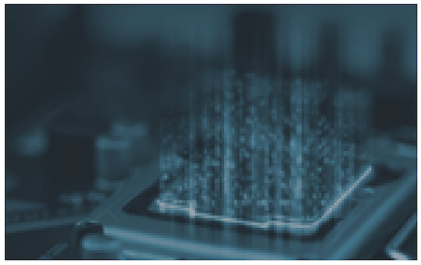
Tech Show London **Excel** **London, UK** **6 – 7 March 2024**	**The European Chatbot & Conversational AI Summit 2024** **Dynamic Earth** **Edinburgh, Scotland.** **12 - 14 March 2024**	**19th International Conference on Cyber Warfare and Security (ICCWS)** **Johannesburg, South Africa.** **26 – 27 March 2024**
Dive into the heart of innovation at Tech Show London 2024. Discover a world where cutting-edge technology reshapes industries, enhances businesses, and drives the future. Join us on 6-7 March 2024 at ExCeL London for an unparalleled journey through the latest in tech. From AI breakthroughs to revolutionary cloud solutions, Tech Show London is your gateway to the trends and technologies that are defining our world. The Tech Show is “co-located” at the city's ExCeL Centre with Cloud Expo Europe, Big Data & Ai World, Data Centre World, Cloud & Cyber Security Expo, and more. Register for your free ticket.	The European Chatbot & Conversational AI Summit is a two-day conference and exhibition designed to host industry executives and adopters of Conversational AI, Generative AI, Chatbots, Virtual Assistants, voice technology, and Conversation Design. The summit will highlight the latest trends and recent application changes in the Conversational AI space within the European market. We believe Conversational AI has the potential to transform millions of lives in Europe, and our goal is to contribute to the creation of a better ecosystem. This is achieved through organizing a series of international conferences in Europe, Africa, and IBEROAMERICA, bringing together leading professionals and organizations that design, build, and market Conversational AI-based technologies.	ICCWS uniquely addresses cyber security, cyber warfare and information warfare. For the past 19 years ICCWS has developed into an important conference in the cybersecurity field, attracting academics, military professionals and practitioners from around the world to present their research findings in the form of empirical studies, case histories and other theoretical and practical contributions. The conference has been attended by a variety of security and military organizations including Cyber Security Policy Research Institute, more than 10 national defense colleges, NATO, SHAPE, and others.
For further information **https://www.techshowlondon.co.uk**	**For further information** **https://theeuropeanchatbot.com**	**For further information** **https://www.academic-conferences.org/conferences/iccws/**

Zyber Global Online Events

Our Online Courses with INsig2
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/
Special discount: 15% Use Code: zyber

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