Zyber Global

NOVEMBER 2023 | ISSUE 40

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to Zyber Global Centre's monthly newsletter - November 2023, the 40th edition!

Greetings, cyber enthusiasts! Dive into the insights featured in our November newsletter!

October marked both Cybersecurity Awareness Month and Black History Month. While pondering how to commemorate these occasions, OCWAR-C (the West African Response on Cybersecurity and Fight against Cybercrime) invited me to serve as an instructor for a foundational judicial training on cybercrime and electronic evidence for judges. The fact that it was part of Ghana's Cybersecurity Awareness Month made it even more special.

This three-day training, organized by Ghana's National Cybersecurity Authority in collaboration with the European Commission, OCWAR-C, and GLACY+ (EU-funded projects), received support from the Judicial Training Institute. Chief Justice Gertrude Esaaba Torkornoo inaugurated the training, emphasizing its goal of equipping judges with a comprehensive understanding of cybercrime laws and electronic evidence to enhance the judicial system's capacity to handle cybercrime cases. She encouraged judges to embrace such training opportunities to deepen their knowledge of technology-related laws.

The Chief Justice also called for the training of other key players in the criminal justice system, including the Narcotics Control Board and the Financial Intelligence Centre, to empower them to fulfil their roles effectively.

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Serving as an instructor for this foundational judicial training was a great opportunity to contribute to the empowerment of judges and further enhance the judicial system's capacity to address cybercrime cases effectively.
I look forward to future opportunities to support and collaborate on initiatives that strengthen cybersecurity and the rule of law.

"Let us know what topics you would like to see discussed in future newsletters and remember to stay vigilant in the digital realm!

Keep safe!"

Judicial Training in Ghana

Zyber Focus Article

Defending Your Dreams: A Guide to Fraud Prevention and Data Breach Recovery

Sadie Cohen (Guest Writer)

In today's digital-centric world, small enterprises are increasingly at risk of becoming targets for deceptive schemes and unauthorized data intrusion. This threat is not just hypothetical but real and present, posing grave consequences that can impact both your revenue stream and hard-earned reputation. Simply being aware of these risks is insufficient; proactive actions must be undertaken to effectively minimize them. The process of implementing a robust security protocol may seem daunting, but it's a critical factor in ensuring the survival and prosperity of your business.

As an entrepreneur, it's essential to adopt a proactive stance, rather than a reactive one, when it comes to security. This entails meticulous planning, thorough preparation, and decisive implementation of protective measures designed to shield your business from the increasing digital threats. By doing so, you're not only fortifying your business but also creating a safer environment for your employees, and establishing trust with your clients. It's important not to wait for disaster to strike before taking action to defend your enterprise. The time to act is now, not later. In this article I aim to provide you with a comprehensive guide to equip your small business with the necessary defenses against deception and information intrusions.

The Password Puzzle: The Why and How of Routine Updates

The importance of regularly changing employee passwords is a point that cannot be emphasized enough. Leaving passwords unchanged for long periods is equivalent to leaving your front door unlocked, practically inviting trouble. It's essential to opt for passwords that are complex and hard to guess, ideally combining letters, numbers, and special characters for added security. Another effective measure is to employ two-factor authentication wherever possible, introducing an additional layer of protection. Various systems and tools are available that can enforce mandatory password changes at specified intervals, making this crucial process easier to manage. It's also beneficial to conduct occasional security audits focusing on password strength and the last changed date, as these can reveal potential vulnerabilities. Employee training should not only cover the importance of keeping passwords confidential but also stress the risks associated with using the same password for multiple business-related platforms. Auditing, changing, and strengthening passwords should be ingrained as a routine yet critical step in your overall security protocol.

-

The PDF Security Suite: More Than Just Document Sharing

When sharing sensitive information with clients or within your team, using PDFs is highly advisable. These files can be password-protected, offering an additional layer of security. Moreover, if you have a large PDF that needs to be divided into smaller sections for easier dissemination, using this tool will split a PDF, allowing you to share only the necessary information. PDFs provide multiple levels of security, including encryption options that protect the data contained within them. You can also set permissions on what the recipient can do with the document—be it viewing, editing, or printing. Use specialized software that allows you to track who opened the document and when. These features make PDFs an excellent tool for secure document sharing. Ensure your team knows how to enable these features to maximize security.

Virtual Safety Deposit Box: Secure Online Backup Systems

A robust online backup system functions like a virtual safety deposit box, safeguarding your invaluable business data. It's advisable to utilize cloud-based solutions that offer high-level encryption, ensuring that your data remains secure even in transit. These backup systems should be configured to update automatically, capturing any new data or changes as they occur. A sound practice is to maintain multiple backups in different geographical locations, offering an added layer of protection against natural disasters or localized server failures.

It's crucial to regularly test your backups, ensuring that the data can be restored successfully in the event of a loss. Access to these backups should be granted only to personnel who genuinely need it, and a system should be in place to monitor who accessed what data and when. In the unfortunate event of data loss or theft, a secure online backup system provides the means for quick recovery of essential data, effectively minimizing business downtime.

The Emergency Handbook: Your Go-To Guide

Preparation is key when dealing with potential deception or information intrusion events. A comprehensive response plan should be in place, outlining the immediate steps to be taken following such an event. Each team member must understand their specific role and responsibilities to ensure a swift and efficient response. Regular rehearsals of this plan are crucial to keep everyone well-prepared and updated on any changes to the protocol. This level of preparation can transform a potentially catastrophic situation into a manageable incident. Remember, always prepare for the worst while hoping for the best.

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

Zyber News Roundup

Boeing assessing Lockbit hacking gang threat of sensitive data leak

Boeing Co (BA.N) said on Friday it was assessing a claim made by the Lockbit cybercrime gang that it had "a tremendous amount" of sensitive data stolen from the aerospace giant that it would dump online if Boeing didn't pay ransom by Nov. 2.

The hacking group posted a countdown clock on its data leak website with a message saying, "Sensitive data was exfiltrated and ready to be published if Boeing do not contact within the deadline!"

"For now we will not send lists or samples to protect the company BUT we will not keep it like that until the deadline," the hacking group said.

The hacking group typically deploys ransomware on a victim organization's system to lock it up and also steals sensitive data for extortion.
"We are assessing this claim," a Boeing spokeswoman said by email.

Read more:

https://www.reuters.com/business/aerospace-defense/boeing-assessing-lockbit-hacking-gang-threat-sensitive-data-leak-2023-10-27/

France says Russian state hackers breached numerous critical networks

The Russian APT28 hacking group (aka 'Strontium' or 'Fancy Bear') has been targeting government entities, businesses, universities, research institutes, and think tanks in France since the second half of 2021.

The threat group, which is considered part of Russia's military intelligence service GRU, was recently linked to the exploitation of CVE-2023-38831, a remote code execution vulnerability in WinRAR, and CVE-2023-23397, a zero-day privilege elevation flaw in Microsoft Outlook.

The Russian hackers have been compromising peripheral devices on critical networks of French organizations and moving away from utilizing backdoors to evade detection.

This is according to a newly published report from ANSSI (Agence Nationale de la sécurité des systèmes d'information), the French National Agency for the Security of Information Systems, that conducted investigations on the activities of the cyber-espionage group.

ANSSI emphasizes a comprehensive approach to security, which entails assessing risks. In the case of the APT28 threat, focusing on email security is crucial.
The agency's key recommendations around email security include:

- Ensure the security and confidentiality of email exchanges.
- Use secure exchange platforms to prevent email diversions or hijacks.
- Minimize the attack surface of webmail interfaces and reduce risks from servers like Microsoft Exchange.
- Implement capabilities to detect malicious emails.

Read more:

https://www.bleepingcomputer.com/news/security/france-says-russian-state-hackers-breached-numerous-critical-networks/

Jordan's New Cybercrime Law Passes Despite Freedom Concerns

In August 2023, Jordan's King Abdullah II approved a revised cybercrime law, despite widespread concerns about its impact on freedom of expression. The law, passed with minimal amendments despite public opposition, faced criticism from digital rights organizations, the US State Department, and the UN High Commissioner for Human Rights.

The law introduces vague terms and harsh penalties for offenses related to online expression, raising concerns about its potential to stifle free speech and impose censorship. It also grants authorities the power to block or control social media accounts without clear legal procedures, potentially impacting economic activities like e-commerce and foreign investments. Jordan has been criticized for increasingly restrictive laws, and the swift passage of this legislation without broad public debate or engagement with civil society organizations has raised transparency and participation concerns.

Read more:

https://timep.org/2023/10/19/jordans-new-cybercrime-law-passes-despite-freedom-concerns/

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

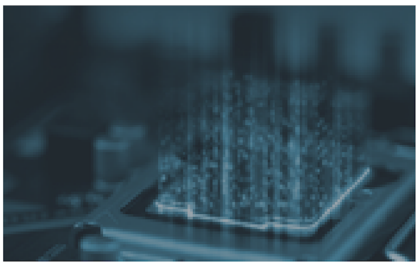
Anti-Financial Crime Summit **Gloucester Hotel, Kensington London** **7-9 November 2023**	**Generative AI in Cyber Security** **Free CS Hub Online Event** **14-15 November 2023**	**CyberThreat 2023** **Novotel London West Hammersmith, London** **20- 21 November 2023**
Join the discussion with Industry Leaders on Battling Financial Crime. Profit is at the centre of many of the most serious criminal activities, including human trafficking, modern-day slavery, the drugs trade and the funding of terrorism via the arms trade. As "*dirty*" money needs to be cleaned before use, it's no surprise that criminality continues to innovate in order to insert this money into the global financial systems – or that financial crime prevention is at the top of the regulatory agenda. Beyond stopping criminal behaviour, the sanctions levied against Russian individuals and entities due to the Ukraine invasion mean war and catastrophic loss of life can be directly impacted by the actions of the risk and compliance groups in financial institutions worldwide	The wave of Generative AI innovation is also causing increases in the scale, frequency and complexity of cyber-attacks. Traditional security measures are inadequate against these evolving AI threats. With cybercriminals using AI to boost ransomware, email phishing scams and other attacks, cybersecurity leaders must fight AI with AI. Generative AI revolutionizes cyber security by harnessing the power of artificial intelligence to proactively detect, defend against, and mitigate emerging threats. By embracing the capabilities offered by Generative AI organizations can start to outpace evolving threats. Generative AI in Cyber Security provides a unique opportunity to gain valuable insights, explore effective solutions, and examine real-world case studies that showcase the transformative power of Generative AI.	Join the National Cyber Security Centre (NCSC) and SANS Institute again for one of the biggest cybersecurity conferences in the UK. Designed for security practitioners and spanning the full spectrum of offensive and defensive disciplines, the event will have a strong technical emphasis with enormous value to cyber security professionals of all levels.
For further information **https://www.cshub.com/events-anti-financial-crime-summit**	**For further information** **https://www.cshub.com/events-generative-ai-cyber-security**	**For further information** **https://www.sans.org/cyber-security-training-events/cyberthreat23/**

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