DECEMBER 2024 | ISSUE 53

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the December edition of our newsletter – our 53rd issue.

Christmas is a season I absolutely love so as the festive season approaches, I am excited to bring you this month's feature article: "Staying Zyber-Safe This Christmas: Tips for Protecting Your Data During the Festive Season." With the holidays being a prime time for cybercriminals, this edition is packed with practical advice to help you stay secure while shopping, travelling, and celebrating. From spotting holiday-themed phishing scams to safeguarding devices gifted during the season, we've got you covered.

November in the UK was particularly dark, wet, and very cold! I was delighted to escape the dreary weather for a visit to Bahrain, where I had the opportunity to conduct a Training Needs Analysis (TNA). It was a productive and rewarding experience, and I look forward to sharing insights from this work in the coming months.

I hope that you find this month's newsletter both informative and engaging.
As always, we welcome your feedback and suggestions for future topics.
Wishing you a cyber-safe and joyful holiday season! May your Christmas be filled with warmth, joy, and plenty of cyber-safety tips to keep you secure!

Esther George, CEO Zyber Global Centre

This Month's Features

1 **Zyber Focus Article**
Staying Zyber-Safe This Christmas: Tips for Protecting Your Data During the Festive Season

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

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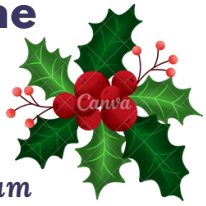A focus on forums/ conferences around the world.

1

Zyber Focus Article

Staying Zyber-Safe This Christmas: Tips for Protecting Your Data During the Festive Season

by Esther George and the Zyber Global Research Team

The festive season is here, it is a time of joy and celebration, but it's unfortunately also a time when cybercriminals ramp up their activities. As online shopping, travel, and digital gift-giving surge, so do opportunities for cybercriminals. According to the FBI, 12,000 victims lost $73 million to online scams during the holiday season in 2022, and this number is expected to grow. With cyber risks on the rise, it's crucial to adopt safe practices to protect your loved ones, data and finances during this festive time.
We have set out below our favourite tips on how you can stay safe online at Christmas.

Safe Online Shopping Practices

Online shopping spikes during the holiday season, and so does the number of fraudulent websites and scams.
To shop safely:

- **Verify website legitimacy:** Ensure the website's URL (address on the internet) is accurate and look for security indicators such as "HTTPS" and a padlock icon.
- **Avoid storing card details:** Refrain from saving your credit card information on websites.
- **Use secure payment methods:** Opt for credit cards or digital wallets like Apple Pay, which offer fraud protection and encryption.
- **Beware of deals that seem too good to be true:** Scammers often promote heavily discounted prices to lure victims. Be cautious of unsolicited emails, ads, or links offering too-good-to-be-true deals. Avoid clicking on suspicious links instead, visit the retailer's website directly by typing the URL into your browser.

Recognizing and Avoiding Holiday-Themed Phishing Scams

Phishing scams become more sophisticated during the holidays, often mimicking trusted brands or services.
Watch out for:

- **Emails or messages urging immediate action:** Scammers create urgency to trick you into clicking malicious links.

Emails or texts claiming you'll lose an exclusive deal unless you act immediately are common scams. Take a moment to verify the authenticity of such messages.

- **Authentic-looking phishing attempts:** AI-generated scams can appear highly credible. Always scrutinize sender details and email headers.
- **Fake promotions or giveaways:** Scammers often mimic popular brands with fake holiday offers or gift cards. Be cautious of unsolicited offers for popular items at discounted rates.

When in doubt, avoid clicking links and verify the sender's authenticity by visiting the official website directly.

Securing Devices Gifted During the Holidays

Many people receive new devices as gifts during Christmas, making them prime targets for cyberattacks.
To secure your new devices:

- **Update software and firmware:** Install the latest updates to patch security vulnerabilities.
- **Use strong passwords:** Immediately change the default login credentials to unique, strong passwords for your devices and accounts.
- **Enable two-factor authentication (2FA):** This add an extra layer of security to your accounts.
- **Install antivirus software:** Equip your devices with antivirus software and enable firewalls to protect your devices from malware and other threats.

Tips for Using Public Wi-Fi Safely While Travelling

Travelling during the holidays often means relying on public Wi-Fi, which can be a hotspot for cybercrime. Stay safe with these tips:

- **Avoid sensitive transactions:** Don't access banking (or other sensitive accounts) or enter personal information over public Wi-Fi.
- **Use a VPN:** A virtual private network (VPN) secures your data by encrypting it, making it more difficult for cybercriminals to access...

Read more here: https://zyberglobal.com/blog?blogcategory=Article

Zyber News Roundup

Interpol Clamps Down on Cybercrime and Arrests Over 1,000 Suspects in Africa

Interpol, in collaboration with Afripol, arrested 1,006 suspects across 19 African countries during Operation Serengeti, a two-month crackdown on cybercrime that targeted ransomware, online scams, business email compromise, and digital extortion. The operation, running from September 2 to October 31, identified 35,000 victims worldwide and uncovered nearly $193 million in financial losses. Local law enforcement and private sector partners, including internet service providers, played crucial roles in this large-scale effort, which significantly surpassed previous results in the region.

Read more:
https://www.securityweek.com/interpol-clamps-down-on-cybercrime-and-arrests-over-1000-suspects-in-africa/

Social media influencer arrested after filming herself getting ready to steal from store using fake barcodes

A 22-year-old TikTok influencer with nearly 300,000 followers, Marlena Velez, has been arrested for allegedly using fake barcodes to steal $500.32 worth of items from a Target store in Cape Coral, Florida. On October 30, Velez reportedly scanned false barcodes at self-checkout to purchase household goods and clothing at reduced prices. Target's Loss Prevention team identified the theft through security footage, which was later shared on the Cape Coral Police Department's social media to seek public assistance. An anonymous tip led police to Velez's TikTok account, where she had filmed herself preparing for and carrying out the alleged theft.

Read more:
https://www.yahoo.com/news/social-media-influencer-arrested-filming-093601227.html

Mexico's President Says Government Is Investigating Reported Ransomware Hack of Legal Affairs Office

Mexico's President Claudia Sheinbaum announced that her government is investigating an alleged ransomware attack on the presidential legal affairs office. The hacker group Ransomhub claims to have stolen 313 gigabytes of sensitive data, including personal information from a government employee database, and posted a sample of the files online. The group has reportedly given the government 10 days to pay an undisclosed ransom, threatening to publicly release the full cache of files if their demands are not met.

Read more:
https://www.securityweek.com/mexicos-president-says-government-is-investigating-reported-ransomware-hack-of-legal-affairs-office/

USA: Wethersfield police warn about Eventbrite scams

Wethersfield police are cautioning the public about scams on the Eventbrite platform, where cybercriminals create fake events to steal personal information and money. Recently, scammers set up a fraudulent event, using realistic logos and branding in email invitations. These emails directed recipients to a fake webpage that requested sensitive information such as login credentials, tax identification numbers, and credit card details.

Read more:
https://www.yahoo.com/news/wethersfield-police-warn-eventbrite-scams-143554210.html

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

CyberThreat 2024 | December 9 - 10, 2024 | London, UK

The two-day conference is hosted by the National Cyber Security Centre (NCSC) and SANS Institute.

CyberThreat 2024 evidences the UK Government's commitment to equip practitioners with the skills and knowledge required to defend against cyber threats and also addresses the cyber skills gap, by developing and growing talent.
CyberThreat aims to deliver the best technical conference globally for cyber security practitioners.

SEE MORE >

Black Hat Europe 2024 | December 9 - 12, 2024 | London, UK

Black Hat is a renowned global cybersecurity event series that offers unparalleled technical and up-to-date information security research. From its humble beginnings as a single annual conference, it has evolved into the most esteemed international event series in the field.

These multi-day gatherings provide the security community with the latest groundbreaking research, advancements, and emerging trends. Driven by the requirements of the global security community, Black Hat briefings and trainings aim to unite the industry's foremost experts and visionaries.

SEE MORE >

FutureCon Atlanta Cybersecurity Conference | December 11, 2024 | Atlanta, USA

FutureCon has over two decades of experience providing security professionals with the latest insights on emerging threats, cyberattacks, and innovative solutions, while fostering strong community networks to combat cybercrime effectively. Their mission is to equip organizations with the resources needed to stay safe in an evolving digital landscape. This is a hybrid event.

SEE MORE >

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

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.

CLICK HERE

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.
CLICK HERE