Zyber Global

APRIL 2023 | ISSUE 33

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to Zyber Global Centre's monthly newsletter - April 2023, the 33rd edition!

Last month, I had the honour of speaking at the DataFocus Conference in Zagreb, Croatia, where industry leaders gathered to discuss the latest trends and technologies in digital forensics. From insightful plenary lectures to informative workshops, attendees had the opportunity to network with peers and gain valuable insights.

Speaking on the investigation track, I presented on "Prosecuting Cybercrime is a Team Sport," and it was great to catch up with old friends like Judge Kornelija Ivanušić, who gave an excellent speech on the "Second Additional Protocol to the Convention on Cybercrime."

I am back home now, and I am looking forward to the Easter celebrations this weekend and I will be making the most of the two public holidays. As Easter approaches, we wish you all a joyful and meaningful holiday shared with loved ones.

The next Stay Safe Online webinar is on the 27 April 2023, so do register early. Spaces are limited!
See: https://zyberglobal.com/webinars

As always, do let us know what topics you would like to see discussed in the May 2023 newsletter. Stay safe!

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Focus Article

This month's article focuses on Deep Fake Technology and its Ill-Effects: A brief Examination of the Technology and its impact on Society

Zyber News

We have a roundup of the latest international cybercrime news.

Zyber Global Events Information

A focus on forums/conferences around the world.

Kornelija Ivanusic - Judge of the Municipal Court, Velika Gorica, Croatia

Esther George and Goran Oparnica - Managing Director, Insig2

'In the old days, if you wanted to threaten the United States, you needed 10 aircraft carriers, and nuclear weapons, and long-range missiles. Today.....all you need is the ability to produce a very realistic fake video that could undermine our elections, that could throw our country into tremendous crisis internally and weaken us deeply,'

U.S Senator Marco Rubio

Zyber Focus Article

Deep Fake Technology and its Ill-Effects: A brief Examination of the Technology and its impact on Society

Esther George & Zyber Global Research Team

In recent years, the development of artificial intelligence (AI) has revolutionized various industries, including the creation of deepfake technology. Deepfake technology is a type of AI that uses deep learning algorithms to create multimedia content that appears almost identical to real images, videos, and audio. While the technology has many potential uses, it also poses significant risks to society, including the spread of misinformation, invasion of privacy, evidentiary issues, and loss of trust. In this article, we will explore the ill-effects of deepfake technology and possible solutions to prevent its negative impacts.

Understanding Deepfake Technology

Deepfake technology is composed of two A.I. algorithms: a generator and a discriminator. The generator creates fake multimedia, while the discriminator determines whether the multimedia is real or fake. The better the discriminator gets at detecting fakes, the better the generator gets at creating them, and vice versa.

The use of deepfake technology has become widespread in various fields. For instance, the fashion industry is using deepfake technology to create virtual try-on features to allow customers to create their full-body image and virtually try different outfits. A clinical-stage drug discovery company is using deepfake technology to design new molecules to treat various diseases. However, despite its many potential uses, deepfake technology is also widely used to manipulate public opinion, spread false information, and invade people's privacy.

In 2018, a Belgian Socialist party circulated a deepfake video of Donald Trump wherein he persuades Belgium to withdraw from Paris Climate Agreement as “climate change is fake just like this video”. Although the party made it clear that its intention was to start a public debate on climate change, many people believed that the video was true. On one hand, this could be called an innovative way to campaign but on the other hand, it could lead to misinformation.

The Ill-Effects of Deepfake Technology

Deepfake technology has the potential to cause widespread harm to society. The following are some of the ill-effects of deepfake technology:

1.Political Deepfakes

Political deepfakes have become a major concern in recent years, as they can be used to spread false information, manipulate public opinion, and disrupt elections.

Deepfake videos can be created to make it appear as though a politician has said or done something that they did not actually say or do. This can lead to political instability and undermine public trust in the government. For example, a deepfake video of the US House of Representatives Speaker, Nancy Pelosi, went viral in 2019, in which she appeared to be drunkenly slurring words and criticizing Donald Trump. The video damaged her reputation, even though it was later debunked. In Italy, a deepfake video of the Prime Minister, Matteo Renzi was used in an Italian TV show where he was insulting politicians. When this went viral on social media, the Prime Minister had to face public outrage as many believed the video to be true.

2. Dangerous to Privacy and Modesty

Deepfake technology poses a serious threat to privacy and modesty, particularly when it comes to non-consensual pornography. The technology can be used to create fake adult content without the consent of the individuals involved, leading to humiliation, shame, and emotional distress for the victims of these fake videos.

3. Evidentiary Issues

Videos and images which are admissible as evidence in court will face issues in the future due to falsified ultra-realistic multimedia by deepfake technology. In future videos and images may be used to create false evidence which could lead to wrongful convictions and undermine trust in the justice system.

4. Loss of Trust

The proliferation of deepfakes can lead to a loss of trust in video content, as people may become sceptical of any video they see online. This can make it difficult for people to discern what is real and what is fake and undermine public trust in the media.

Conclusion

The ill-effects of deepfake technology cannot be overlooked, as it poses significant risks to society. However, it is also important to acknowledge the potential benefits that this technology can offer.

Read the full article : https://zyberglobal.com/blog

Zyber News Roundup

Ferrari Hacked & Ransom Demanded

The famous Italian sports car maker Ferrari has said it has been a victim of a cyber-attack targeting confidential information about its customers but said it had refused a demand for ransom money.
In a statement the firm said "We regret to inform you of a cyber incident at Ferrari, where a threat actor was able to access a limited number of systems in our IT environment," and we are working to reinforce the security of its systems, adding that there was "no impact on the operational functions of our company... Ferrari was recently contacted by a threat actor with a ransom demand related to certain client contact details," it said.

The hackers "had access to certain customer data such as names, addresses, email addresses and telephone numbers, but not bank details", a spokesman.
After it received an unspecified demand for ransom, Ferrari said it began an investigation with the help of a cyber security firm and informed the authorities.
Chief executive Benedetto Vigna has written to clients to inform them of the incident. "Ferrari takes the confidentiality of our clients very seriously and understands the significance of this incident. As a policy, Ferrari will not be held to ransom as paying such demands funds criminal activity and enables threat actors to perpetuate their attacks." the firm said.

Read more:
https://www.cybersecurityintelligence.com/blog/ferrari-hacked-and-ransom-demanded-6852.html

China's Nuclear Energy Sector Targeted in Cyberespionage Campaign

A South Asian advanced persistent threat (APT) actor has been targeting the nuclear energy sector in China in a recent cyberespionage campaign, Intezer reports.
Dubbed 'Bitter' and active since at least 2021, the group is known for the targeting of energy and government organizations in Bangladesh, China, Pakistan, and Saudi Arabia, and is characterized using Excel exploits, and Microsoft Compiled HTML Help (CHM) and Windows Installer (MSI) files.

The Bitter APT targeted recipients in China's nuclear energy industry with at least seven phishing emails impersonating the embassy of Kyrgyzstan in China, inviting them to join conferences on relevant subjects. The recipients were lured into downloading and opening an attached RAR archive containing CHM or Excel payloads. "Bitter APT do not appear to change their tactics too much, therefore we can assume that the payloads will be similar to those observed in 2021, executing a downloader module that can be served with plugins such as a keylogger, remote access tool, file stealer, or browser credential stealer," Intezer notes.

Read more:
https://www.securityweek.com/chinas-nuclear-energy-sector-targeted-in-cyberespionage-campaign/

Netherlands: Eight Arrested in Bank Help Desk Scam after 150 People Lost €1.6 million

The Limburg police arrested eight suspects of bank helpdesk fraud in the past months. The suspects are four men and four women, mostly from the Amsterdam region. According to the police, they stole a total of 1.6 million euros from 150 people, scamming the victims into thinking they were calling from their bank.

The Limburg police's Cybercrime Team launched this investigation into bank helpdesk fraud in March 2022. Months of inquiry led them to arrest four women in October last year and four men last week.

According to the police, the scammers called victims with a fake number, making it look like they were calling from the victim's bank. Posing as bank employees, they told the victims that there were suspicious transactions on their bank accounts, showing the accounts had been hacked. They convinced the victims to transfer their account balance into a "vault account" or a "safe account," which were the suspects' accounts.

Read more:

https://nltimes.nl/2023/03/31/eight-arrested-bank-help-desk-scam-150-people-lost-eu16-million

Fake Trump arrest photos: How to spot an AI-generated image

Fake images created by artificial intelligence (AI) tools depicting Donald Trump have appeared on social media over the past week. Many falsely showed the arrest of the former president, who may face indictment over payment of hush money to a woman he allegedly had an affair with. He has not yet been charged with a crime.
Many of those sharing the images pointed out they were fake, and they did not appear to fool lots of people - but a few did seem to be tricked.
On Thursday, Mr Trump also shared an AI-generated image on his own social media platform Truth Social. It showed him kneeling in prayer.
What are some of the tell-tale signs of AI-generated imagery? And how can you distinguish a real from a fake?

Read more:
https://www.bbc.co.uk/news/world-us-canada-65069316

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

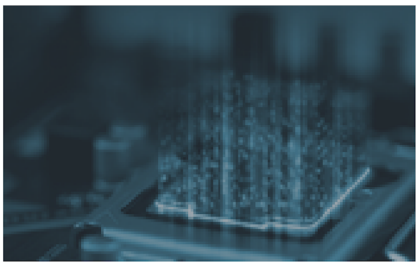
UK Cyber-week Expo and Conference **Business Design Centre London, UK** 4 **- 5 April 2023**	**CYBERUK 2023** **ICC Belfast, Northern Ireland** **18– 20 April 2023**	**RSA Conference** **San Francisco, USA** **24 - 27 April 2023**
We are all in this together, but we believe there is a knowledge gap between the expertise of the cyber community and UK businesses leaders. We want to close that gap. Everyone has their part to play – policymakers, businesses, cyber professionals, IT departments, cyber vendors, software developers, law enforcement, media and educators. Join the community fighting back at UK Cyber Week. We are bringing everyone together to level up UK cyber security, demystify jargon, share the latest thinking and learn from truly world-class experts. Our promise is that everyone, no matter how much or how little expertise they have, leaves knowing more and is better equipped. UK Cyber Week's live flagship event is completely free to attend.	CYBERUK 2023 will examine how today's cyber ecosystem must adapt in order to keep the UK the safest place to live and work online. It will explore new ways that the sector - worth £10 billion to the UK economy - can join together: to innovate and to strengthen, to resist new threats and to be ready for opportunities. CYBERUK has a reputation for its energy, packed with world-class content, engaging speakers and opportunities to connect.	One of the largest and most well-known cybersecurity conferences in the US and Asia is celebrating 30 years in the industry. As always, they have a busy lineup of cybersecurity experts, panel discussions, and interesting guest speakers. This year's agenda includes a cloud security summit, OWASP seminar, FIDO Alliance seminar, innovation sandbox, women's networking reception, and daily learning lab events. Plus, they are hosting both in-person and online marketplace expo options featuring hundreds of businesses, product specialists, and demos of the newest solution.
For further information **https://www.ukcyberweek.co.uk/why-should-i-attend**	**For further information** **https://www.cyberuk.uk/cyberuk/programme**	**For further information** **https://www.rsaconference.com/usa**

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