Nexia
Agbo Abel & Co

The Dark Web's Role in Cybercrimes in Nigeria: Challenges and Cybersecurity Solutions

Content

The Dark Web's Role in Cybercrimes in Nigeria: Challenges and Cybersecurity Solutions

The deep web is a breeding ground for cybercrime in Nigeria. This anonymous online space allows criminals to steal financial information, exploit people, and traffic illegal goods. The economic impact is significant, with billions lost annually.

Nigeria faces challenges due to a lack of cybersecurity awareness, outdated infrastructure, and poverty. The country is fighting back with public awareness campaigns, legal reforms, and efforts to build a skilled cybersecurity workforce.

The internet has revolutionized various aspects of modern life, providing unprecedented access to information, connectivity, and commercial opportunities. Yet, under its surface lies the dark web, a shadowy realm facilitating numerous illicit activities, including cybercrimes. Nigeria, a rapidly evolving nation in terms of digital transformation, faces significant challenges due to deep web facilitated cybercrimes that disrupt economic activities and personal security. This article explores these challenges and presents potential cybersecurity solutions to combat the detrimental effects of the dark web in Nigeria. It also looks at the National response so far.

1. Understanding Deep-Web Related Cybercrime

Deep-web related cybercrime encompasses a broad spectrum of illegal activities mediated via the deep web. This shadowy segment of the internet hosts sophisticated software, malicious tools, and platforms used by cybercriminals to exploit vulnerabilities in information systems and networks. Often referred to as 'virtual crime,' 'hi-tech crime,' 'net-crime,' or 'computer e-crimes,' these offenses leverage advanced technologies to target and manipulate critical systems, compromising data integrity and leading to severe economic repercussions.

2. The Impact of Deep-Web Enabled Cybercrimes

The economic cost of dark web facilitated cyber-attacks is steep, manifesting in reputation damage, legal proceedings, psychological distress, financial losses, and disrupted social connections. These cyber threats target both individuals and organizations, leading to compromised accounts, stolen data, and significant financial harm. In Nigeria, the transition from analog to digital systems exposes corporate entities to heightened vulnerability, exacerbated by factors such as corruption, lack of standards, inadequate ICT education, high unemployment, insufficient infrastructure, and ineffective law enforcement. In its report, the Nigerian Communications Commission had claimed in 2023 that Nigeria "is losing $500 million annually to all forms of cybercrime including hacking, identity theft, cyber terrorism, harassment and internet fraud." This was confirmed by the chairman of the economic and financial crimes commission Mr. Abdulrasheed Bawa, in 2023 budget defense when he stated that 2,847 persons have been convicted of cybercrimes across the country as of date.

3. Types of Cybercrimes Facilitated by the Deep-Web

Types of cybercrimes that are facilitated by the deep web include a range of illicit activities that exploit the anonymity and untracked nature of the dark corners of the internet. These include intellectual property

The Dark Web's Role in Cybercrimes in Nigeria: Challenges and Cybersecurity Solutions

theft, financial or fintech crimes, identity theft and phishing, cyber-terrorism, child exploitation/sex trafficking and pornography, human trafficking, and drug trafficking.

- Intellectual Property Theft is a prevalent crime, involving the unauthorized reproduction and distribution of copyrighted content such as movies, music, software, and games.
- Financial Crimes encompass a broad spectrum of illegal actions, from industrial espionage and sabotage to extortion, product counterfeiting, and different forms of financial fraud, often causing significant monetary losses.
- Identity Theft and Phishing are tactics used by malicious individuals to steal personal information and credentials for financial gains, leading to scams, unauthorized transactions, and potential long-term damage to victims' financial wellbeing.
- Cyber-Terrorism involves attacks on critical national digital and physical infrastructure, security systems, and even human lives, demonstrating the profound impact deep-web cybercrimes can have on society and security.
- Child Exploitation, Human Trafficking, and Drug Trafficking are despicable acts that find fertile ground on the dark web, enabling the distribution of child pornography, exploitation of vulnerable individuals, and illegal drug trade in an underground environment.
- Given the increasingly sophisticated nature of these crimes, detecting and preventing them poses significant challenges. The unique socio-economic landscape of Nigeria further complicates the cybersecurity scenario, underscoring the pressing need for robust and effective countermeasures to combat deep-web cybercrimes and protect individuals and institutions from its harmful effects.

4. Deep-Web Related Cybertheft and Financial Fraud in Nigeria

Deep-Web Related Cybertheft and Financial Fraud in Nigeria present serious challenges for the banking and e-commerce sectors in the country. Scams related to Bank Verification Numbers (BVNs), phishing attacks, and digital intrusions are prevalent issues. Cybercriminals exploit vulnerabilities in the systems to illicitly access personal and financial information, enabling them to steal funds or create false identities for illegal purposes.

Moreover, counterfeit and deceptive sales pose a significant risk, as fraudulent transactions target unsuspecting consumers through popular online platforms, resulting in financial losses and a decline in trust. Additionally, ATM and card theft are common tactics used by cybercriminals, who use stolen or cloned BVNs and bank cards to unlawfully withdraw funds. Furthermore, phishing schemes are rampant, with cybercriminals employing fake and cloned websites or deceptive emails to trick individuals into divulging sensitive information.

5. The Prevalence and Impact of Cybercrime in Nigeria

Nigeria's digital ecosystem is highly susceptible to cybercrime due to a combination of high poverty rates, limited cybersecurity awareness, widespread use of unregulated cybercafés, outdated/inadequate cybersecurity infrastructure, and rise of artificial intelligence

The Dark Web's Role in Cybercrimes in Nigeria: Challenges and Cybersecurity Solutions

(AI) & machine learning (ML). The financial toll is significant, with annual losses estimated in billions. According to the Kaspersky (www. Kaspersky.co.za) Digital Payment survey, 61% of respondents from Nigeria faced phishing scams when using online banking or mobile wallet services. 67% have personally encountered fake websites, and a staggering 82% experienced scams (via texts or calls) using social engineering. Notable cases, such as the MMM Ponzi scheme, highlight the profound socio-economic impact of deep-web facilitated scams. The country's youth, often driven by poverty and peer pressure, are increasingly engaged in cybercriminal activities, exploiting deep-web technologies to perpetrate financial fraud and identity theft.

6. Strategies for Combating Cybercrime in Nigeria

Strategies for combating cybercrime in Nigeria demand a thorough and structured approach encompassing distinct areas. The key measures involve advanced security intelligence, public awareness campaigns, robust infrastructure, legal reforms, and capacity building initiatives.

Firstly, enhancing security intelligence is imperative. This includes deploying sophisticated SIEM tools for gathering security information, utilizing network visibility tools, and implementing threat detection systems. Furthermore, organizations must focus on proactive Threat Lifecycle Management, which involves identifying and neutralizing potential threats through systematic measures like direction, collection, processing, analysis, dissemination, and feedback.

Secondly, raising public awareness is critical. Collaborative endeavors with NGOs, businesses, and governmental bodies are necessary to educate the masses about cyber threats and encourage deep-web and safe online practices. Incorporating cybersecurity modules into school curricula can foster a culture of cyber awareness from an early age, especially among vulnerable youth.

Thirdly, strengthening cybersecurity infrastructure is paramount. Establishing an Integrated National Cybersecurity Framework is essential, entailing resilient cybersecurity ecosystems supported by legal guidelines, skilled professionals, and technological resources. Collaborative strategies among financial institutions can also boost fraud monitoring and prevention mechanisms.

Implementing legal and regulatory reforms is the fourth crucial step. Enhancing existing legislation like the Cybercrime Act to encompass comprehensive national cybersecurity protocols and promote international collaboration is essential. Strengthening data protection laws to safeguard personal and corporate data is also imperative.

Lastly, building capacity through training and development is essential. Professional development programs offering scholarships, internships, certifications, and continuous training for IT professionals, to help them stay updated with evolving cybersecurity trends. Investing in cybersecurity talent is vital to creating a competent workforce that ensures a secure digital environment for all.

7. National Response

Nigeria has taken several steps to address

The Dark Web's Role in Cybercrimes in Nigeria: Challenges and Cybersecurity Solutions

cybersecurity crimes with various key initiatives implemented over the years. In April 2014, the National Computer Emergency Response Team (CERT) was created to serve as Nigeria's national cybersecurity incident response team, working in collaboration with different stakeholders to prevent, detect, and respond to cybersecurity incidents.

The Cybercrime Act of Nigeria was initially enacted in 2015 to define and penalize cyber-related offenses. Subsequently, in February 2024, the Act was amended to address emerging forms of cybercrimes like electronic fraud, data interception, and unauthorized system interference. The amended Act was designed to prosecute cybercriminals, enhance cybersecurity, combat terrorism and money laundering, improve international cooperation in cybercrime investigations, prevent cybercrimes, and adapt the legal framework to address evolving digital threats.

Following that, the Cyber Security Advisory Council was established in March 2016 by the Nigerian government. This council was set up to offer strategic guidance on cybersecurity matters and to coordinate cybersecurity activities across different sectors.

In October 2023, the government, in collaboration with industry stakeholders, conducted its 20th cybersecurity awareness campaign. This campaign focused on educating the public, especially the youth, about online threats, reporting cybercrimes, and practicing safe online behaviors. Various programs were put in place to raise awareness about cybersecurity threats and promote measures to safeguard individuals in the rapidly evolving digital landscape.

Despite these proactive efforts, cybersecurity continues to pose a significant ongoing challenge in Nigeria and other countries. Continuous vigilance, capacity building, and collaboration remain crucial in effectively addressing cybersecurity crimes.

Conclusion

Combating deep-web facilitated cybercrime in Nigeria demands an integrated approach encompassing technology, education, legal reforms, and collaborative efforts. By enhancing security intelligence, raising public awareness, strengthening cybersecurity infrastructure, enacting comprehensive laws, and developing a skilled workforce, Nigeria can build a resilient digital ecosystem capable of mitigating cyber threats. Addressing these challenges not only secures the nation's digital future but also fosters economic growth and stability in an increasingly connected world.