RESEARCH
FOR THE WORLD

How do the cybercriminals behind business email compromise (BEC) fraud operate?

Published January 2025

Dr Suleman Lazarus, Visiting Fellow, Mannheim Centre for Criminology, LSE

Business email compromise schemes "earn" cybercriminals billions of dollars a year. **Suleman Lazarus** explains how a major organisation behind many of these scams operates – and why law enforcement needs to change its mindset if it is to achieve greater success in combatting this transatlantic crime.

Who, in this day and age, has not spent time considering whether an email link is safe before clicking? Yet despite increasingly sophisticated cybersecurity software and a rise in general knowledge about the potentials of cybercrime, business email compromise (BEC) schemes remain one of the "**most financially damaging online crimes**". While many phishing attacks and social engineering attempts fail, enough are getting through to "earn" cybercriminals **billions of dollars a year**.

Despite being a transatlantic crime, some of these BEC schemes are still too often viewed as "African" crimes – piquing the interest of the academic and media worlds only once Western victims are identified. Perhaps because of this, detailed knowledge of the hierarchies of the criminal gangs operating in this area is limited, making convictions even harder to obtain.

New research by **Dr Suleman Lazarus**, Visiting Fellow at the Mannheim Centre for Criminology at LSE, however, extends our knowledge about the way one of the world's major cybercriminal organisations operates in this field, throwing some common assumptions into question. Serving as an expert witness in a case against an alleged leader of a cybercriminal syndicate, he gained rare access to interview the defendant multiple times. The accused was also a member of the Black Axe Confraternity, one of Nigeria's "most notorious transnational criminal organisations," and faced numerous charges related to BEC offences.

> Once offenders gain access, they often do not act immediately. They discreetly take control of the email account, avoiding detection while conducting thorough research.

What is business email compromise?

In business email compromise (BEC) schemes, **fraudsters compromise organisational email accounts**, impersonating trusted entities such as executives or business partners to obtain sensitive information for potential extortion or to defraud businesses of money directly.

The scheme relies on a network of compromised machines from which fraudsters will glean important information – from the style of writing to the key players in each business. Whether a CEO or a university student, we are all vulnerable to organised criminals – students' bank accounts are often used for money laundering, while CEOs' emails are prime targets for manipulating colleagues. All it takes is one click.

What can appear on the surface to be a simple spamming attempt might, in reality, be the work of time spent planning and surveillance. "For these schemes to work, these organisations will need to make a phone call or write a cloned email with the same language and tone," explains Dr Lazarus. "Once offenders gain access, they often do not act immediately. Instead, they discreetly take control of the email account, avoiding detection while conducting thorough research to identify key relationships, access points to sensitive information, and their targets' linguistic and communication culture within the compromised organisation. They meticulously map out the organisation, or 'case the joint', strengthening their networks if needed by enlisting money mules, often university students, to facilitate the movement of funds across multiple bank accounts."

Who are the Black Axe Confraternity?

Originating as a university student fraternity in Nigeria, Black Axe has grown into a **ruthless criminal enterprise with global reach**. "The university environment in Nigeria is a breeding ground for cybercriminals, and because the Black Axe organisation also emerged from a university setting, the marriage between Black Axe organisation and cybercriminality is not as far-fetched as it might appear. And many students remain active in these networks even after graduation, perpetuating the cycle," says Dr Lazarus.

Having published on cybercrime and online fraud, Dr Lazarus was invited by a legal team in a Western nation's criminal justice system (undisclosed for confidentiality reasons) to serve as an expert witness. His role included interpreting obscure data and interviewing a high-ranking cybercriminal - a member of the Black Axe, who had been arrested. Initially unwilling to speak, the defendant eventually opened up, but only after Dr Lazarus established his "credentials" as an interviewer. Originally unwilling to speak, the gang member eventually opened up, but only once Dr Lazarus had set out his "credentials" as an interviewer.

"At first, when I asked a question, he would give me an answer that he would give to the criminal justice system representatives and his legal team," he says. "So, I analysed what happened to him – this is what happened, and you were arrested because you did not follow certain 'business' codes that you needed to follow, etc. And because I was able to identify this, and also the particularities of his identity, invisible in his official documents, he opened up, and we then had a more open and engaged conversation. I must also emphasise that adopting an approach of '**neither condemning nor ridiculing, but seeking to understand**' intrinsically motivated my dual role as both researcher and expert witness."

> Leadership within the group shifts based on individual expertise ... Because of this flexibility ... these criminals are more likely to succeed.

Access to this accused "leader" of a cybercrime syndicate in that Western nation, a Black Axe member, was crucial to developing Dr Lazarus's understanding of the organisation. His findings, drawn from a series of four-hour interviews and an analysis of tapped phone records monitored by the law enforcement agency, are presented in Dr Lazarus's paper: "***Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the "Black Axe" Confraternity***". This study provides the first empirical documentation of direct testimonies from a prominent BEC offender connected to the elusive Black Axe network.

'Academically, there hasn't been any empirical research on the topic of business email compromise schemes and the Black Axe – we have just had theoretical speculation or sensational media coverage – so this was a very rare opportunity. Having the opportunity to engage in a series of 'long-haul conversations' with a high-profile Black Axe member from an academic perspective was highly significant. These individuals have rarely been studied outside the context of police investigations, arrests, and so on. Without direct interviews to gain insight into their operations, we are left to speculate about how they truly function. "

Researching criminal organisations like the Black Axe Confraternity requires sensitivity, and so Dr Lazarus is careful over what details he shares. His findings, however, are clear, revealing, for the first time, the dynamics of the organisation as it operates these BEC scams, as well as highlighting one of the reasons law enforcement is struggling to combat this particular crime.

Why a non-hierarchical structure is helping the Black Axe evade law enforcement

Unlike the mafia or more typical street gangs, the Black Axe Confraternity's cybercriminal network, particularly those involved in BEC schemes, does not operate hierarchically, he finds. Instead of a main "boss" with a series of lower-level "lieutenants", it has a flat structure, allowing for those with the most relevant technical knowledge for each particular scheme to take the lead.

"I saw no evidence for any hierarchical structure," says Dr Lazarus. "What I discovered is that leadership within the group shifts based on individual expertise. The person whose skills are most relevant at a given moment assumes the role of lead operator, while others take on subordinate roles. This dynamic changes with each transaction, and job titles rarely align with conventional hierarchies, adding to the complexity.

"Because of this flexibility, adaptability and manoeuvrability, these criminals are more likely to succeed, as it makes it very difficult for law enforcement to pinpoint precisely who the leader, conduit, recruiter or manager is at any given time."

As a result, tracking members of the gang becomes far more difficult, particularly if law enforcement does not recognise how the organisation operates. "Law enforcement often struggles with accuracy in their operations because they broadly approach business email compromise schemes through the lens of traditional organised crime models. They attempt to fit these schemes into longstanding frameworks that help them make sense of the situation, relying heavily on established models and prevailing knowledge about organised crime. In doing so, they overlook critical nuances, remaining blind to what more flexible and adaptable observers can clearly see," Dr Lazarus says.

> “There has been a persistent tendency to trivialise these crimes as "African issues".”

Black Axe cybercrime is not a "Nigerian problem"

As **one phishing email could potentially cost a small business as much as $100,000**, combatting this crime is a policy imperative. With a clearer understanding of the realities on the ground, Dr Lazarus's findings should prove useful to law enforcement and policymakers looking to combat crimes like BEC schemes. At present, however, he argues that various forms of online fraud, such as BEC, involving West African criminal actors targeting victims worldwide, are still too often dismissed as a "local" African problem rather than recognised as the global issue they are.

Dr Lazarus, who recently **presented this research to policymakers**, is eager to challenge this perception. "There has been a persistent tendency to trivialise these crimes as 'African issues', not only in public policy but also in academia. Ironically, the media has been more forward-thinking in this regard. Research on West African cybercriminals is still frequently deemed less relevant to Western audiences. Perpetrators and victims are two sides of the same coin, yet when attention is given to these crimes, it disproportionately focuses on the victims, neglecting the broader systemic and societal factors at play," he says.

"There has to be a shift in attitudes. We have to stop siloing work in this area as of relevance just to one particular country or part of the world and start seeing it as the transatlantic problem it is."

From business email compromise scams to romance fraud

Another crime that often captures the interest of the media through the victim stories is romance fraud, an area Dr Lazarus has also been focused on. Dr Lazarus has built on his **research on online romance fraud** with a new paper, "***Examining 50 Cases of Convicted Online Romance Fraud Offenders***".

Building on his previous research, such as "**cryptocurrency fraudsters**" and the UK Home Office-funded "**interviews with active fraudsters in India, Ghana, Nigeria**", Dr Lazarus's analysis of "**case files of convicted romance scammers**" identifies key patterns in victim demographics, fraudsters' operational strategies and offenders' socioeconomic backgrounds.

As with BEC schemes, romance fraud reaches around the world, with most scammers operating from Nigeria – the country Dr Lazarus's paper focuses on – and targeting victims in the USA (56 per cent). And as with the Black Axe Confraternity, there is a university connection. "74 per cent of romance fraudsters are university students, with an additional 16 per cent being graduates, all of them male. Economic conditions in society shape university settings, turning them into fertile breeding grounds for romance scam offenders. "Unfortunately, for most of these offenders, establishing 'scamming industries' becomes an adaptive and innovative response to their socioeconomic challenges," says Dr Lazarus.

Dr Lazarus's paper also reveals more about the cover stories romance fraudsters tend to opt for, with the majority presenting as a Caucasian American male (46 per cent) and 12 per cent presenting as a military officer. Only six per cent used a female cover story.

"The military cover is attractive as they [fraudsters] can find military officers on Facebook, which gives them a believable, real-life script. It also gives them excuses – being busy because of some military posting, or not being able to talk for some time because of being away for a special operation, etc."

Whether the scam is an **impersonal business-focused** or a more personal, **romance-focused scheme**, it is clear the criminals operating in the shadowy world of the internet currently have the upper hand. While a clearer understanding of how they operate may provide some legal support, Dr Lazarus stresses that these online schemes will only be reduced when prevention strategies address the underlying socioeconomic and political issues that are turning so many university students and graduates towards a career in cybercrime. ■

"**Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the "Black Axe" Confraternity**" by Dr Suleman Lazarus was published in *Deviant Behavior*.

"**Examining Fifty Cases of Convicted Online Romance Fraud Offenders**" by Adebayo Benedict Soares and Dr Suleman Lazarus is published in *Criminal Justice Studies*.

Dr Suleman Lazarus was speaking to Jess Winterstein, Deputy Head of Media Relations at LSE.

Subscribe to receive articles from LSE's online social science magazine

lse.ac.uk/rftw