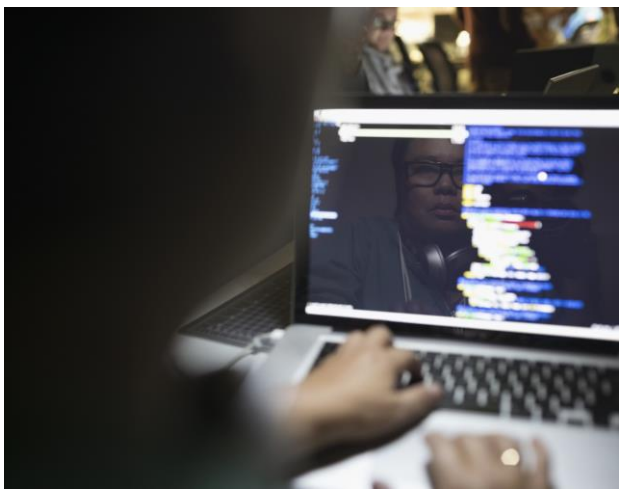
The new face of fraud – combating impersonation and deepfake threat

Imagine a significant amount of money was transferred from your company bank account, authorised by a senior executive in your organisation. Later, however, you discover your company has been a victim of fraud.

Unfortunately, this scenario is becoming more and more common. At PwC, we are seeing this as a growing global trend—and Nigeria is no exception, with companies across several industry sectors falling victim.

A 2024 report by Sumsub, a global identity verification service, revealed a surge in global fraud rates from 2023 to 2024, with Africa experiencing the steepest increase at 167%. Nigeria stands out with the second-highest fraud rate worldwide, reaching 5.91% - double the previous year's rate of 2.95%. Furthermore, Africa has seen a staggering 393% surge in deepfakes.



What is impersonation fraud?

Impersonation fraud is a growing threat in our digital world. Criminals imitate legitimate representatives of companies to steal sensitive information or money. They do this through any or a combination of the following:

1. **Phishing:** Fraudsters send deceptive emails pretending to be trustworthy individuals or organisations to trick people into providing sensitive information.
2. **Business email compromise:** Cyber criminals use email-based social engineering to defraud businesses by impersonating executives or employees.
3. **Deepfakes:** This involves the use of deepfake technology to mimic the voices or appearances of executives, often targeting junior staff or those less familiar with these individuals.

These techniques have become more sophisticated with AI and deepfake technology, making it increasingly difficult to distinguish between genuine communications and fraudulent attempts. Impersonation fraud can target individuals, businesses or government entities, often leading to significant financial losses or data breaches.

Deepfakes and insider threats: A dual challenge for organisations

A series of sophisticated impersonation frauds rocked multiple industries worldwide, showcasing the alarming capabilities of advanced deepfake technology and social engineering tactics.

Additionally, it is crucial to acknowledge that organisational scams can often originate from within, perpetrated by individuals with authorised access.

This insider threat is particularly evident in Nigeria's banking sector where FITC's Q2 2024 reports indicate a 23.4% rise in staff involvement in fraudulent activities, compared to the previous quarter.

Impersonation fraud powered by deepfakes typically involve this approach:

1. **Preparation and intelligence gathering:** Fraudsters meticulously gather publicly available information about the company's senior executives e.g. CEO and CFO. This includes video footage from interviews, voice recordings from earlier calls and personal details from the company's website and the senior executives' social media profiles.
2. **Technology preparation:** Using the collected data, criminals employ advanced AI algorithms to create convincing deepfake videos and voice clones of these senior executives. They also develop fake email accounts and messaging profiles that closely mimic those of the executive team.
3. **Trust building:** Scammers send an email to a mid-level finance manager, seemingly from the senior executive's assistant. This mentions an upcoming confidential project and is loosely based on current events within the organisation. This initial contact is designed to establish credibility without raising immediate suspicion and is usually followed by a request to sign a non-disclosure agreement. Over the next few days, the fraudsters exchange several emails with the finance manager, providing believable details about the supposed project and gradually building trust. Bad actors also pretend to be real consultants or external lawyers from reputable firms, which adds to credibility of the storyline.
4. **Voice cloning:** Once a foundation of trust is established, the scammers arrange a voice call between the finance manager and the "senior executive" using their AI-generated voice clone. During this call, the fake senior executive discuss the urgency of a highly confidential acquisition.
5. **Video conference deception:** The fraudsters hold a fake video call, pretending to be the senior executive to discuss the secret deal and stress the need for non-disclosure.
6. **Fund transfer request:** With trust and urgency in place, the fraudsters request the transfer of a substantial sum to a specified account, ostensibly to secure the acquisition deal

After deep fake cases, professionals are left puzzled over how this fraud could have occurred despite all the controls and safeguards in place. Reports of deepfake-related impersonation scams—such as the $25 million fraud involving a fake CFO on a video call as reported by CNN—underscore a hard truth: these attacks are happening despite existing controls, and organisations are learning the hard way.

Next steps for victims of impersonation fraud

You need to act fast. In the event of falling victim to impersonation fraud, organisations should ask themselves questions which includes:

- How did the fraudster obtain confidential information that was used to defraud the company?
- Which security measures failed and how can the company ensure this type of fraud does not happen again?
- Was anyone within the company involved in the fraud?

How to protect your organisation from impersonation fraud

Impersonation risk assessment

- Conduct thorough analysis of past incidents, industry trends and potential threat actors.
- Evaluate the likelihood of impersonation attempts by reviewing access points, communication channels, and user interfaces that could be exploited.
- Comprehensively review your organisation's systems, processes and controls to identify any potential weaknesses.
- Perform data due diligence by reviewing publicly available information on the key management and the company (particularly audio/voice data).

Cybersecurity crisis readiness and management

- Review your organisation's procedures for incident response & crisis management, conduct readiness assessment to ensure safe practice.
- Activate the prepared plans, gain control of the incident to contain damage and proceed to eradicate threats, returning to normal in a resilient way.

Awareness training

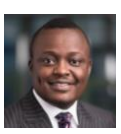
Awareness training/workshops on deepfake technologies can be organised as part of in-house training or conferences.

Employees should be trained:

- to recognise that media content can be manipulated or faked,
- how deepfakes are made,
- and how to recognise deepfakes.

Contact us

Habeeb Jaiyeola
Partner, PwC Nigeria
habeeb.jaiyeola@pwc.com



Adeola Adekunle
Associate Director, Forensics Services, PwC Nigeria
adeola.adekunle@pwc.com