pwc

Forensics Digest

Noted increase in invoice fraud spoofing incidents in the Eastern Africa region

April 2024

In the course of our work advising clients on managing and responding to various fraud and cyber-crime risks, we have noted a common spoofing scheme, primarily affecting Non-Governmental Organisations and organisations with nascent finance functions. Spoofing is the disguising of communication by fraudulent actors to impersonate known/trusted sources. Common forms of spoofing involve fabrication of email addresses, websites and phone calls and with Artificial intelligence (AI) algorithms like generative adversarial networks (GANs) production of deceptive contents like “deepfakes” for impersonation.

The ascendance of technologies such as generative AI is only going to transform traditional spoofing and phishing attacks and make them more potent and believable, increasing these incidents. This is therefore a call for added vigilance for organisations and law enforcement networks within the Eastern African region.

“The ascendance of technologies such as generative AI is only going to transform traditional spoofing and phishing attacks and make them more potent and believable

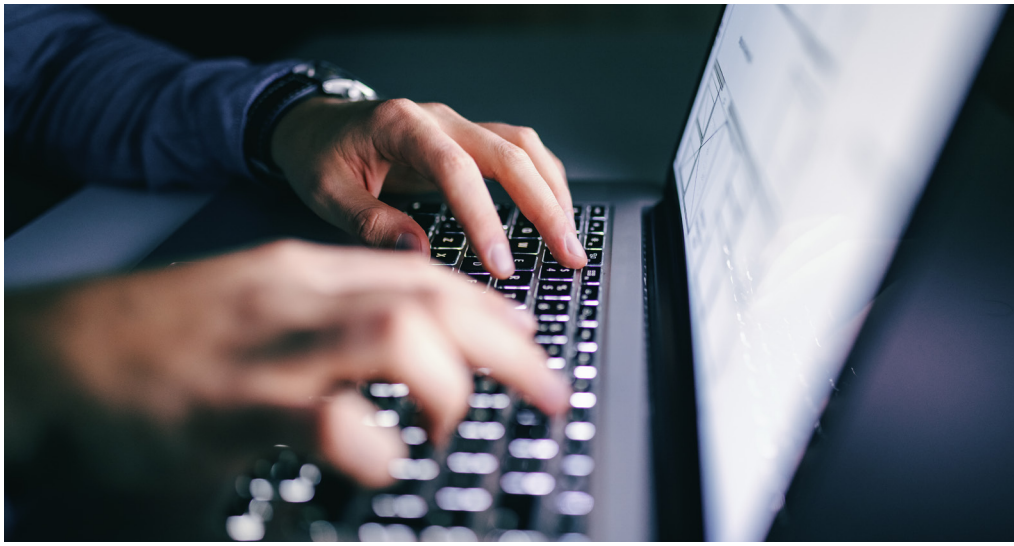
How the spoofing fraud is carried out

The fraudsters appear privy to information on pending or upcoming supplier payments at targeted organisations, pointing to the possibility of insider involvement. Through falsified email addresses similar to those of legitimate suppliers or partners, the fraudsters impersonate the suppliers then contact members of the Finance Department via email. In the emails, the impersonating fraudsters notify the organisation that the vendors have changed their banking details and provides new banking details for payment. Payment is then wired to the fraudsters’ accounts, which are typically offshore accounts.

The transnational nature of these crimes makes it difficult to recover the stolen funds unless it’s detected quickly or the beneficiary bank flags the fraud through their routine transactions monitoring processes. Where this doesn’t happen, the funds may be moved to various other accounts, further reducing the chances of recovery.

Steps organisations can take to protect themselves

1. Restricting access to systems and sensitive financial information on need-to-know basis.
2. Using encrypted and authenticated protocols to reduce the likelihood of a successful man in the middle attacks leading to spoofed phishing emails.
3. Training staff to be vigilant and to verify the authenticity of requests for sensitive data through alternative channels, especially when dealing with third parties.
4. Enhance change of financial information procedures by partners, vendors and other third parties. Ensuring change of details require verification through multiple channels and enforce segregation of duties for automated approval matrices.
5. Enhancing password requirements including complexity, frequency of change and multi factor authentications.
6. Enhancing whistleblower and hotline channels.
7. Third party risk management including clauses to protect the organizations from 3rd party-initiated risks.
8. Implement Email Authentication Protocols- to verify the authenticity of incoming emails and prevent spoofing.
9. Email Filtering and Anti-Spoofing Tools: that can detect suspicious email patterns,
10. Monitor Outbound Traffic: to identify emails sent to unfamiliar domains to detect information exfiltration.
11. Regular Security Audits and Penetration Testing:
12. Regular Updates and Patch Management:



Practical immediate actions to take in case of an attack

We set out below practical measures to take in immediate incident response:

- Alert your bank and through them alert the beneficiary bank. The bank-to-bank cooperation is critical to ensure the immediate freezing of associated accounts.
- Report the matter to law enforcement authorities to obtain relevant orders for support in freezing of the fraudsters' accounts.
- Secure payment information and records and suspend payment processes temporarily.
- Secure company-issued devices for key staff with access to compromised vendor data.
- Instruct staff to update their passwords.
- Carry out a digital forensics review to establish the facts of the incident.
- Immediately remediate vulnerabilities exploited to carry out the attack.

How PwC can support you respond to an attack

Cyber threats come without warning – both from outside and within. Having in place a team that can act quickly and effectively to secure your data, judiciously investigate and provide critical liaison with law enforcement can make all the difference. At PwC, our team of cyber-attack response specialists have extensive experience supporting and working with clients to investigate, secure evidence and identify exploited vulnerabilities to support remediation processes. Their expertise spans the following areas:

- Cyber fraud risk assessments
- Cyber-attack preparedness and cyber-response employee training
- Identification and investigation of computer and cyber related irregularities.
- Computer forensics tools and techniques to perform a wide range of analysis encompassing network, event log analysis, email analysis, external media connection, web analysis and mobile device analysis on company-owned electronic devices used by suspected individuals.
- Cyber fraud Evidence corroboration, triangulation, remediation design and planning
- Forensics Data analytics on structured and unstructured data for e-discovery and suspicious patterns identification.

Contact Us

For more information, please contact your usual PwC contact or any of our experts listed herein should you wish to discuss this further.

John Kamau
Associate Director
Forensics & Financial Crime Leader,
East Africa

john.kamau@pwc.com
+254 20 285 5000

Patrick Matu
Associate Director Forensics &
Financial Crime Leader,
PwC Uganda

patrick.k.matu@pwc.com
+254 20 285 5000

Chrisantus Khulabe
Senior Manager
Digital Forensics & Data Analytics,
East Africa

chrisantus.khulabe@pwc.com
+254 20 285 5000

Brenda Guchu
Manager
Forensics & Financial Crime,
East Africa

brenda.guchu@pwc.com
+254 20 285 5000