

Generative AI from a Hacker's Perspective: An opportunity for bad actors

Alex Wood

CEO and Author, Reform Courses

in **DigiGov Expo**

 **DIGIGOVEXPO**

ALEX WOOD

CYBERCRIME, AI, SOCIAL ENGINEERING & COUNTER FRAUD SPEAKER

Alex's early career was in the music industry. Aged 13 he began to tour the world as a violin soloist and performed under the greatest conductors of the modern era. He was awarded prestigious scholarships to attend the Purcell School, the Royal Academy of Music and the Royal College of Music, won an array of prizes along the way and became a regular guest at Buckingham Palace and Windsor Castle.

Aged 24 his career was abruptly halted by the onset of repetitive strain injury (RSI) in his right hand and faced with mounting debts and no source of income, his criminal career began. His life spiralled out of control, culminating in several years spent in prison for a number of dishonesty offences - everything from impersonating the 13th Duke of Marlborough to committing multi-million pound cyber-crime.

Since his release from jail in early 2022 Alex has turned his life around and become an immensely powerful force in the Counter Fraud profession. He is a sought after Keynote speaker and commentator across mainstream media.

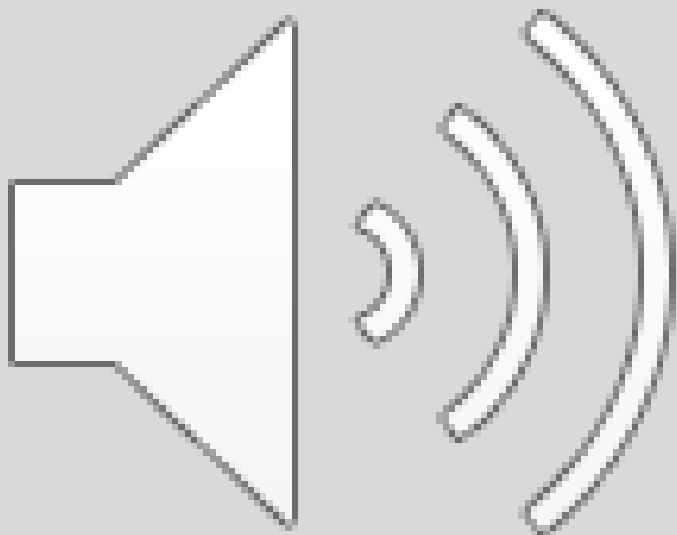
Alex consults for leading global financial institutions (including Tier 1 banks, insurance providers, law firms and risk experts) so as to enable a deep understanding of the 'Fraud Mindset' as well as sophisticated 'Social Engineering' techniques and the threat of emerging tech (including AI).

Alex is working on a national strategy, in partnership with banks, lawyers, Police forces and Government in order to educate children about the risks of involvement in mule activity.

While in prison, Alex was signed by the world-leading literary agent Andrew Lownie. His story is now the subject of a major documentary (in production) by the renowned filmmakers Chris Atkins and Louis Theroux (Mindhouse Productions).

Alex is exclusively represented by Sara Butler at SCAMP Speakers.





SPEAKER QUALIFICATIONS

BBC NEWS

Home UK World Business Poli

'Fake duke' Alex Wood jailed for London hotels fraud

9 December 2015



GETTY/VIMEO

The Duke of Marlborough (left) is more than 25 years older than Alexander Wood

Daily Mail MORE STORIES

Cyber fraudster jailed for pretending to be the Duke of Marlborough is sent back to prison over a £2million scam

By Rebecca Camber Crime Correspondent For The Daily Mail
02:10 21 Jul 2018, updated 02:17 21 Jul 2018



Support us →

The Guardian
News website of the year

News Opinion Sport Culture Lifestyle



UK news

Fraudster who posed as aristocrat to stay in top London hotels is jailed

Ham&High Subscribe

News Sport Things to do More


News > Crime Traffic & Travel Local Council

Find words! Category: Self-Care

Jailed: Conman who defrauded businesses of £2m

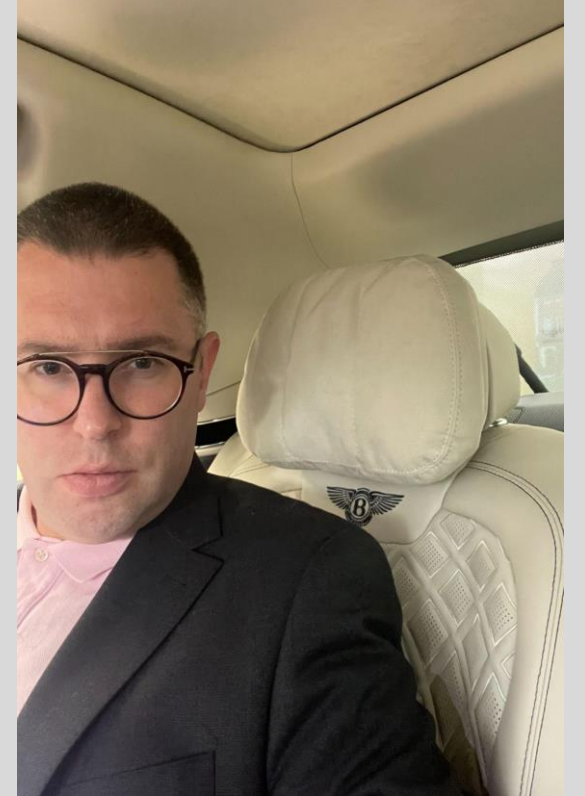
13th July 2018

CRIME



Alexander Wood and Muhammed Azhar. Picture: Metropolitan Police (Image: Archant)

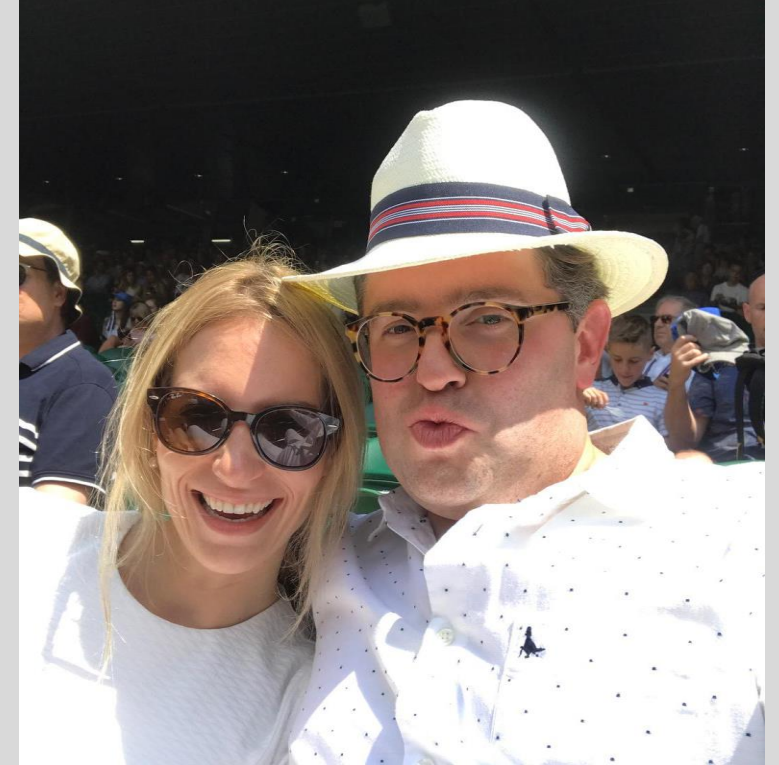
SPEAKER QUALIFICATIONS



SPEAKER QUALIFICATIONS



SPEAKER QUALIFICATIONS



SPEAKER QUALIFICATIONS



SPEAKER QUALIFICATIONS



ANATOMY OF A CYBER FRAUD

- Utilised social engineering techniques
- Target company
- Number spoofing
- Voice manipulation / mirroring

ANATOMY OF A CYBER FRAUD

- Lay false trail (geolocation)
- “Suspend” gateway (suspicious emails / system lagging)
- Possibility of virus (seeds of doubt)



ANATOMY OF A CYBER FRAUD

- Test session (inbound / outbound transactions “frozen”)
- Opportunity to opt-out (can visit branch with CPU / server unit).....a far more inconvenient alternative to opting-in
- Psychological pact to proceed



to be described
point of view
Fraud
to deceive;
cheating inter
liberately r

ANATOMY OF A CYBER FRAUD

- Test session (no money in / out)
- Carefully log in (**do not divulge PINs / codes - further reinforcing banks' messaging**)
- Padlock diversion

ANATOMY OF A CYBER FRAUD

- ‘Sync’ with balances (last 4) - knowledge of values available to steal
- Acquire corresponding mules from the ML team
- Direct to seldom used areas of portal (‘vulnerable to virus’)

ANATOMY OF A CYBER FRAUD

- Inputting of data / generation of 'random' details / authorisation. Innocuous payment references. Are all fields filled (further social engineering)?
- Reverse / repeat
- Counteracting the banks' response (e.g. management of pop-ups / varying of payment references)

GENERATIVE A.I.

“Generative AI” refers to deep-learning models that can generate high-quality text, images, and other content based on the data they were trained on.

IBM Research

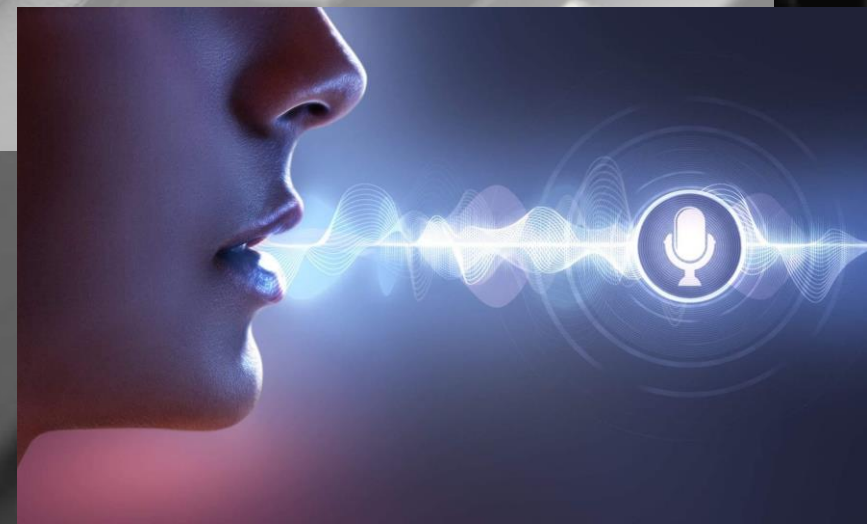
GENERATIVE A.I.

“Generative AI” refers to deep-learning models that can take raw data - say, all of Wikipedia or the collected works of Rembrandt - and “learn” to generate statistically probable outputs when prompted.

IBM Research

DEEP FAKE VOICE CLONING

- 3-minute voice sample
- 99% accurate clone



DEEP FAKE VOICE CLONING

www.fakeyou.com

www.resemble.ai

www.elevenlabs.io

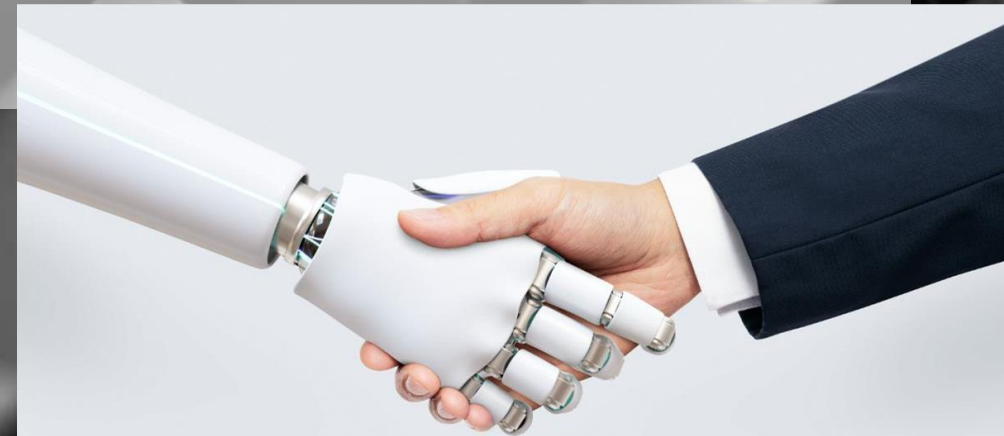
www.voice.ai



FRAUD AUTOMATION

Combining Generative A.I. / Chat GPT / Deep Fake:

- APP-style fraud can be automated from start to finish
- Zero-touch fraud
- Opportunity for one bad actor to commit multiple frauds simultaneously



FRAUD AUTOMATION



DEEPPFAKE (recent examples)

THE ECONOMIC TIMES | Industry Sign In
English Edition | Today's ePaper

Home BUDGET'24 ETPrime Markets News **Industry** Rise Politics Wealth Mutual Funds Tech Careers Opinion NRI Panache

Auto Banking/Finance Cons. Products Energy Renewables Ind'l Goods/Svs Healthcare/Biotech Services Media/Entertainment

Business News > Industry > Tech > Hong Kong MNC suffers \$25.6 million loss in deepfake scam

Hong Kong MNC suffers \$25.6 million loss in deepfake scam



A social media post featuring a deepfake of Elon Musk. The top part shows a video of a man speaking, with a caption that reads "LIVE MARTIN'S HOUSE" and "QUANTUM AI BRITISH MAKE A PROFIT WITH THIS ELON MUSK'S NEW PROJECT". To the right is a photo of Elon Musk in a tuxedo. Below the video is a large red "SCAM" warning with the text "Given the existing... ZaynorArt". On the right side, there are social media icons for likes (26), comments (10), and shares.