

Navigating the evolving landscape of *financial crime*

March 2025

FOR PROFESSIONAL ADVISERS ONLY



Learning objectives



Understand the evolving landscape of cyber security



Recognise the risks AI poses for cybersecurity and financial crime



Understand the importance of third-party due diligence in protecting clients' assets

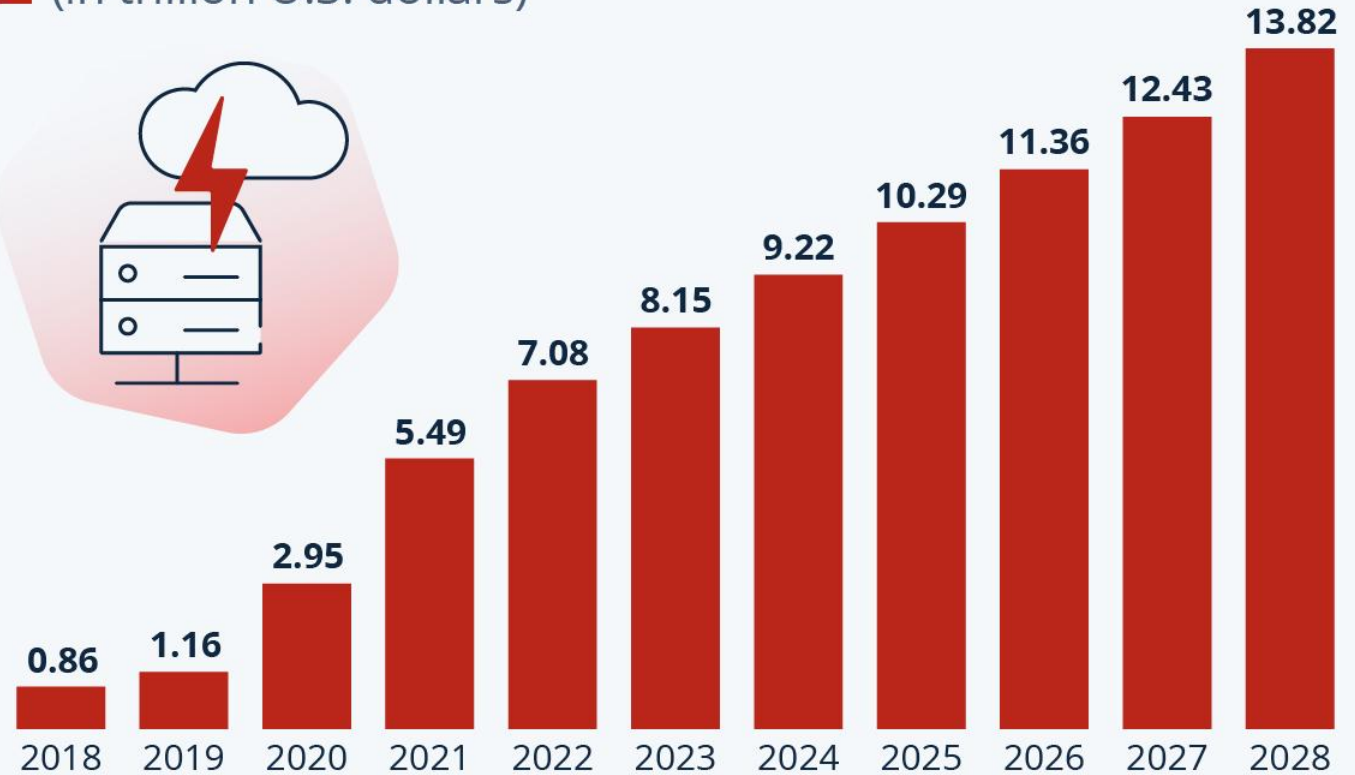
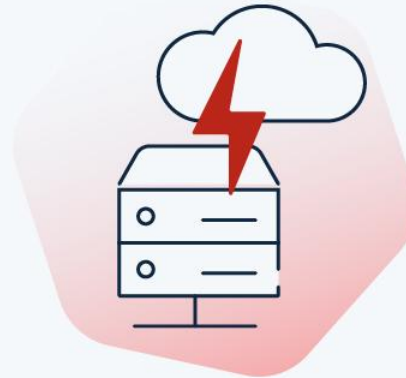
The evolving landscape of *cybersecurity*



Global cost of cyber crime

Cybercrime Expected To Skyrocket

Estimated annual cost of cybercrime worldwide (in trillion U.S. dollars)



As of Sep. 2023. Data shown is using current exchange rates.

Source: Statista Market Insights



Cyber threat landscape

1.5M

Business in the UK were hit with Cyber Crime in 2023 ⁽¹⁾

85%

of Cyber Security professionals attribute the rise in Cyber Attacks to bad actors using generative AI ⁽²⁾

94%

of malware is delivered via email ⁽³⁾

50%

of businesses identified a Cyber Breach or Cyber Attack in the UK. ⁽⁴⁾

95%

of Cyber Security incidents are a result of human error ⁽⁵⁾

86%

of Cyber Attacks use stolen credentials. ⁽⁶⁾

Source:

1. <https://www.infosecurity-magazine.com/news/uk-businesses-31bn-security/>
2. <https://www.cfo.com/news/cybersecurity-attacks-generative-ai-security-ransom/692176>
3. <https://www.guardsite.com/datasheets/Email-Protection.pdf>
4. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024>
5. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
6. <https://nordpass.com/passkeys/>

Investment fraud



The screenshot shows a news article from the City of London Police website. The header features the City of London Police logo and navigation icons. The article title is 'City of London Police reveals more than £612 million was lost to investment fraud in the UK last year'. Below the title, it is categorized as 'Fraud' and 'Press releases', with a publication date of 08/04/2024. The main text states that people aged 55 or over are more likely to be targeted by investment fraud, and that the data from Action Fraud shows a reported £612,208,663 in losses.

CITY OF LONDON POLICE

🏠 > News

City of London Police reveals more than £612 million was lost to investment fraud in the UK last year

Fraud
Press releases

🕒 Published: 09:24 08/04/2024

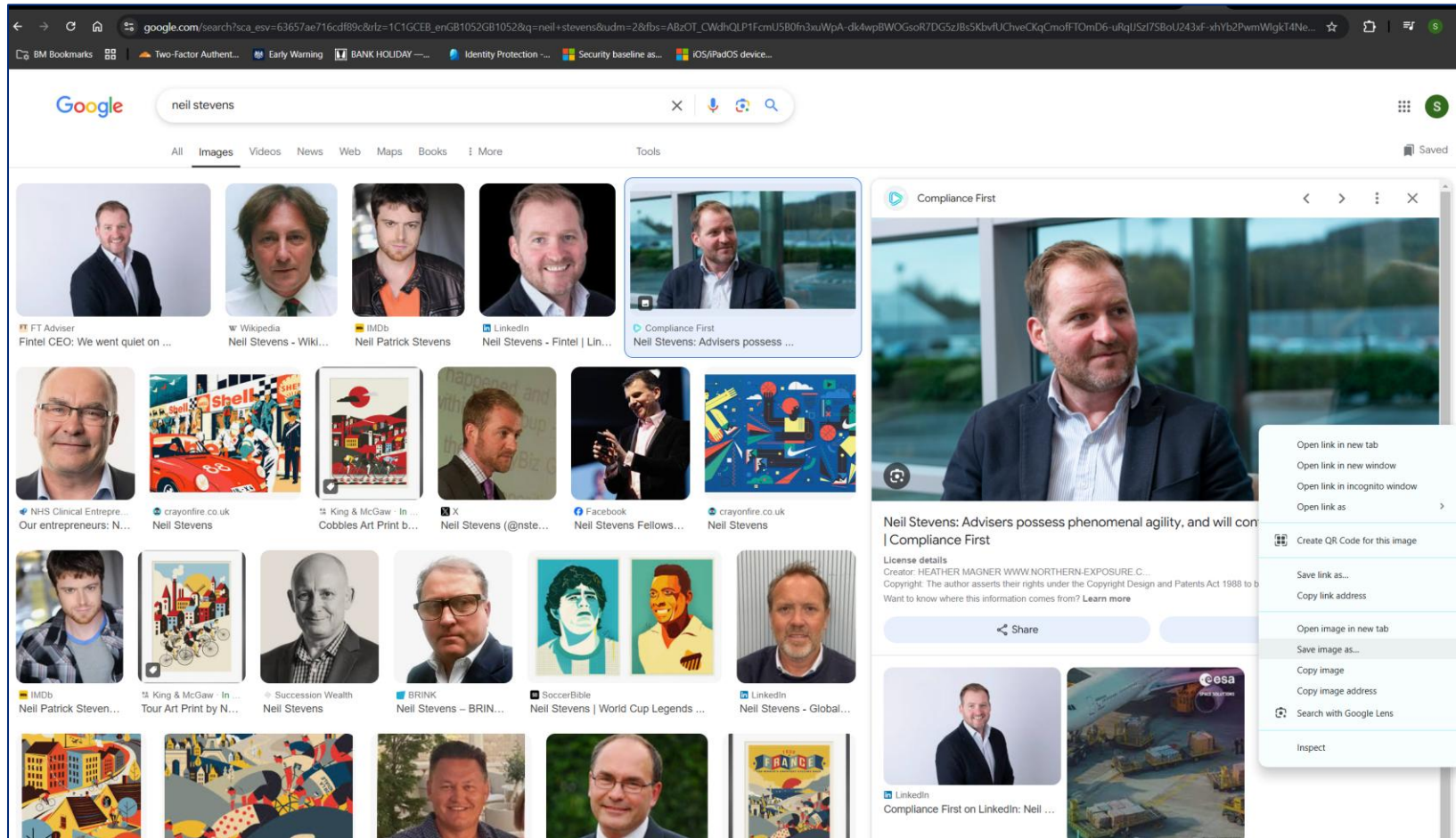
People aged 55 or over are more likely to be targeted by investment fraud, new figures show.

The data from Action Fraud, the national fraud and cyber crime reporting service, revealed the soaring rate of investment fraud in the last year, with a reported £612,208,663 in losses.

- People aged 55+ more likely to be targeted
- Investment fraud is when criminals contact people out of the blue and convince them to invest in schemes or products that are worthless or do not exist. E.g. foreign exchange, gold and valuable metals, time-shares overseas and cryptocurrency.
- **30,130 reports of UK investment fraud in 2023 £25,110 average loss per victim**
- One victim lost **£11.9 million.**
- As the victim's age increases, so does the loss amount. In the 55-64 age range alone, over **£133 million** in losses was recorded

It's never been easier to create deepfake videos

All you need is a photo of the target...



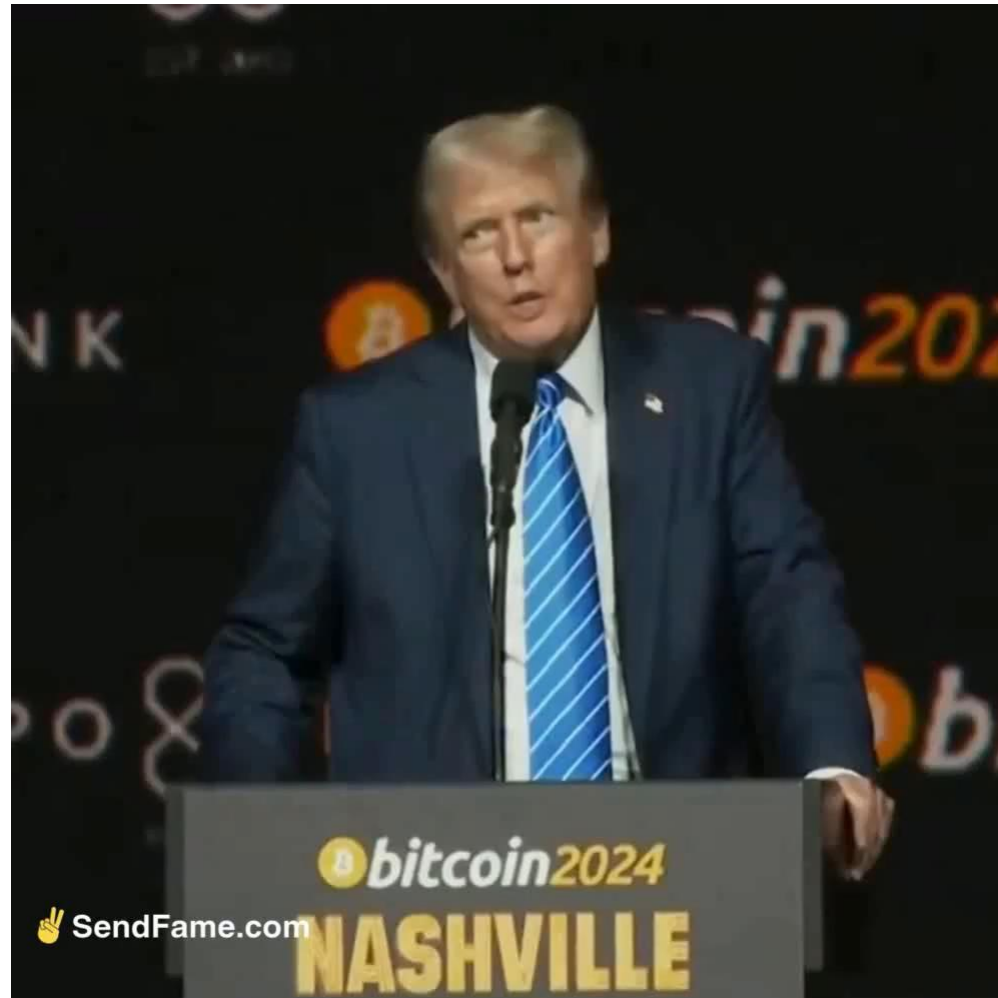
A word from Neil Stevens

Free tools are enabling the possibilities of deep fakes



A word from Donald Trump

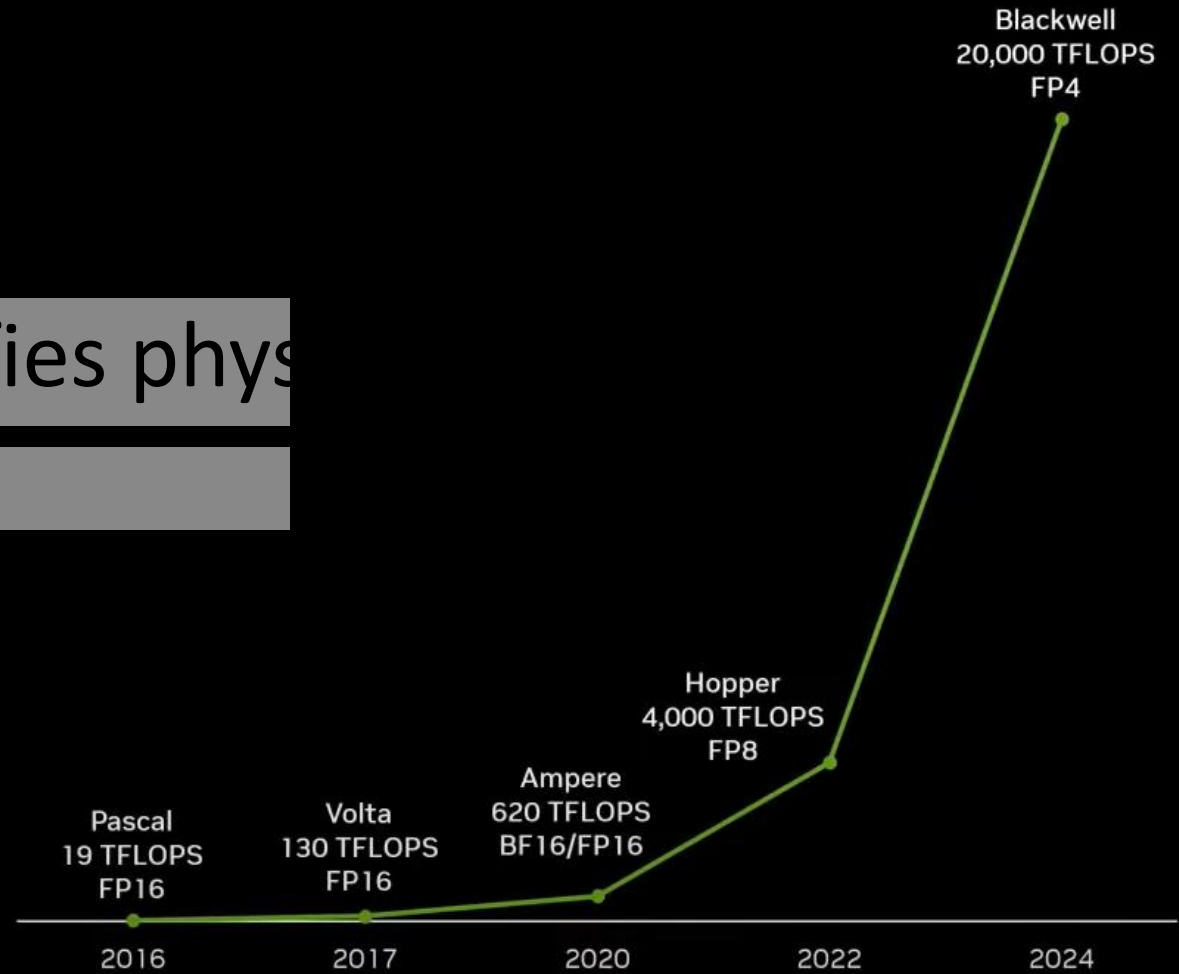
Free tools are enabling the possibilities of deep fakes



1000X AI Compute in 8 Years

Nvidia's breakthrough AI chip defies physics

1,000x AI compute in 8 years



The end of voice authentication?

- Phasing out as a security measure for accessing bank accounts and other sensitive information.
- Minimising the risk of damaging misinformation.

OpenAI deems its voice cloning tool too risky for general release

Delaying the Voice Engine technology rollout minimises the potential for misinformation in an important global election year

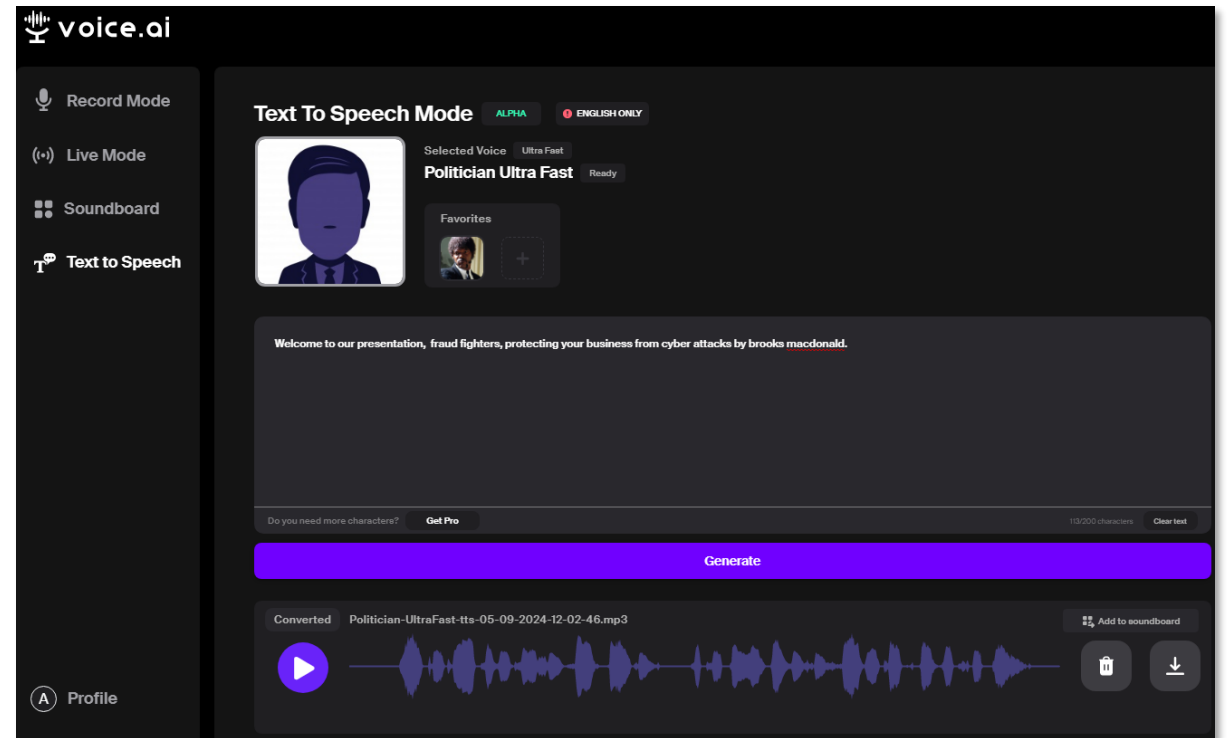
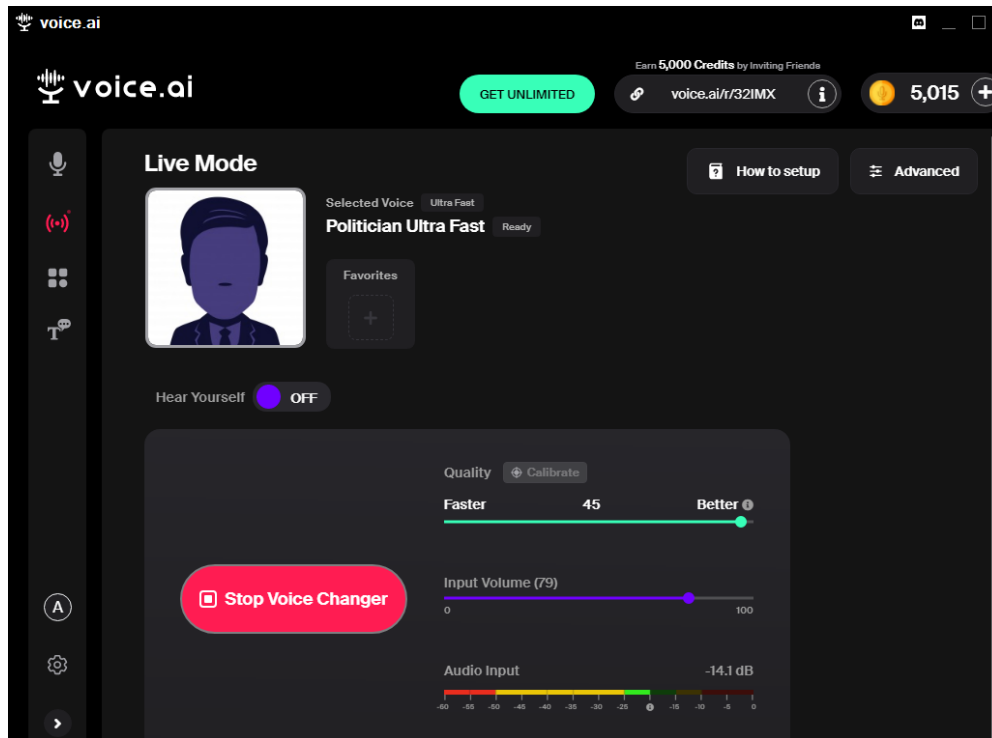


📹 The company says it will 'make a more informed decision' about deploying its Voice Engine technology at scale after further testing. Photograph: Costfoto/NurPhoto/Rex/Shutterstock

A new tool from [OpenAI](#) that can generate a convincing clone of anyone's voice using just 15 seconds of recorded audio has been deemed too risky for general release, as the AI lab seeks to minimise the threat of damaging misinformation in a global year of elections.

Greater power in voice AI tools

Ability to clone anyone's voice in 15 seconds



Apps Supported By Voice AI

Integration with
everyday
applications



Discord



Skype



Whatsapp



Zoom



World of Warcraft



Fortnite



PUBG



League of Legends



Google Meet



Among Us



Minecraft



Viber



TeamSpeak



Twitch



OBS Studio



Messenger



The risks AI poses
*for cybersecurity
and financial crime*



Chat



GPT

Implications of AI on cybersecurity

AI will make scam emails look genuine, UK cybersecurity agency warns

NCSC says generative AI tools will soon allow amateur cybercriminals to launch sophisticated phishing attacks



A report from the National Cyber Security Centre says the overall volume of online attacks is also likely to increase. Photograph: Andrew Brookes/Getty Images/Image Source

MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV INV

TECHNOLOGY EXECUTIVE COUNCIL

AI tools such as ChatGPT are generating a mammoth increase in malicious phishing emails

PUBLISHED TUE, NOV 28 2023-10:39 AM EST

Bob Violino

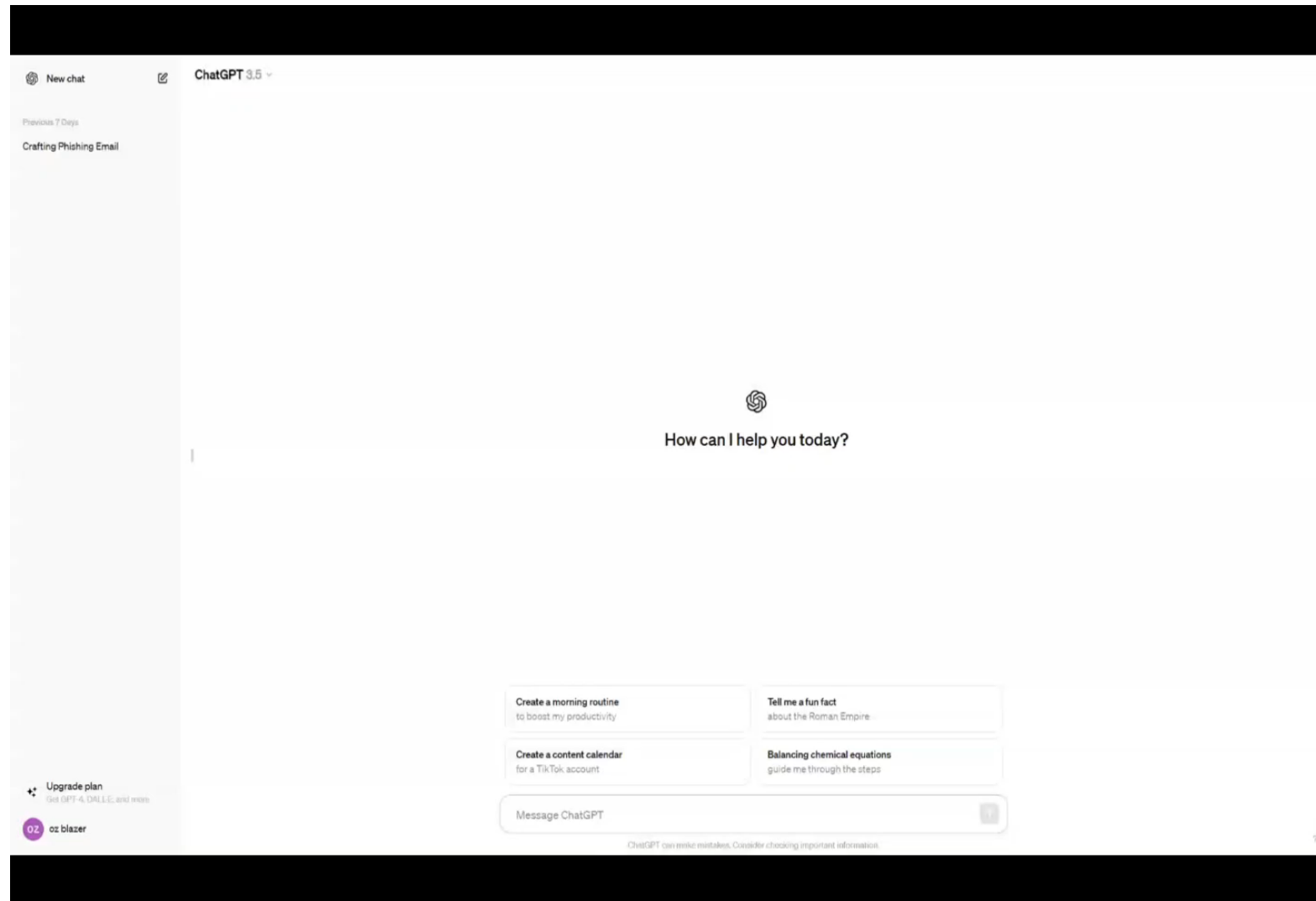
SHARE [f](#) [X](#) [in](#) [✉](#)

KEY POINTS

- Since the fourth quarter of 2022, there's been a 1,265% increase in malicious phishing emails, and a 967% rise in credential phishing in particular, according to a new report by cybersecurity firm SlashNext.
- Cybercriminals are using generative artificial intelligence tools such as ChatGPT to help write sophisticated, targeted business email compromise (BEC) and other phishing messages.
- The report findings highlight just how rapidly AI-based threats are growing, especially in their speed, volume and sophistication.

Source: The Guardian (<https://www.theguardian.com/technology/2024/jan/24/ai-scam-emails-uk-cybersecurity-agency-phishing>, <https://www.theguardian.com/world/2024/feb/05/hong-kong-company-deepfake-video-conference-call-scam>)

Using Chat GPT for malicious purposes



Intel gathering phishing emails

An attempt to start conversation with employees



CITYWIRE
WEALTH
MANAGER

FRAUD | 11 JUN, 2024

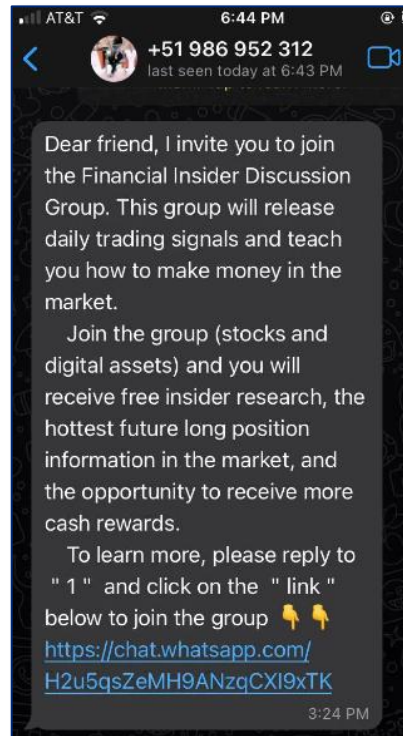
Lindsell Train targeted by bogus WhatsApp group

Fraudsters are masquerading as fund manager Nick Train.

BY **JOHN SCHAFER**

EQUITIES SPONSORED BY
CONTRARIUS

I'm unable to speak over the phone due to a serious throat pain caused by laryngitis. Hope this finds you well. Please let me know when you get this, I'd like to ask you for a favour.



Happy to hear from you. I am sorry for bothering you with this mail, I need to get an Apple gift card for my friend, it's her birthday today and I promised to get it for her, but I can't do this now because I'm currently in the hospital. I have Arthritis in the knee and ankle and all my effort purchasing it online proved aborted.

Can you please get it from any store around you or online?. Kindly let me know if you can handle this.

Kind regards
Peter

Hello Daniel,

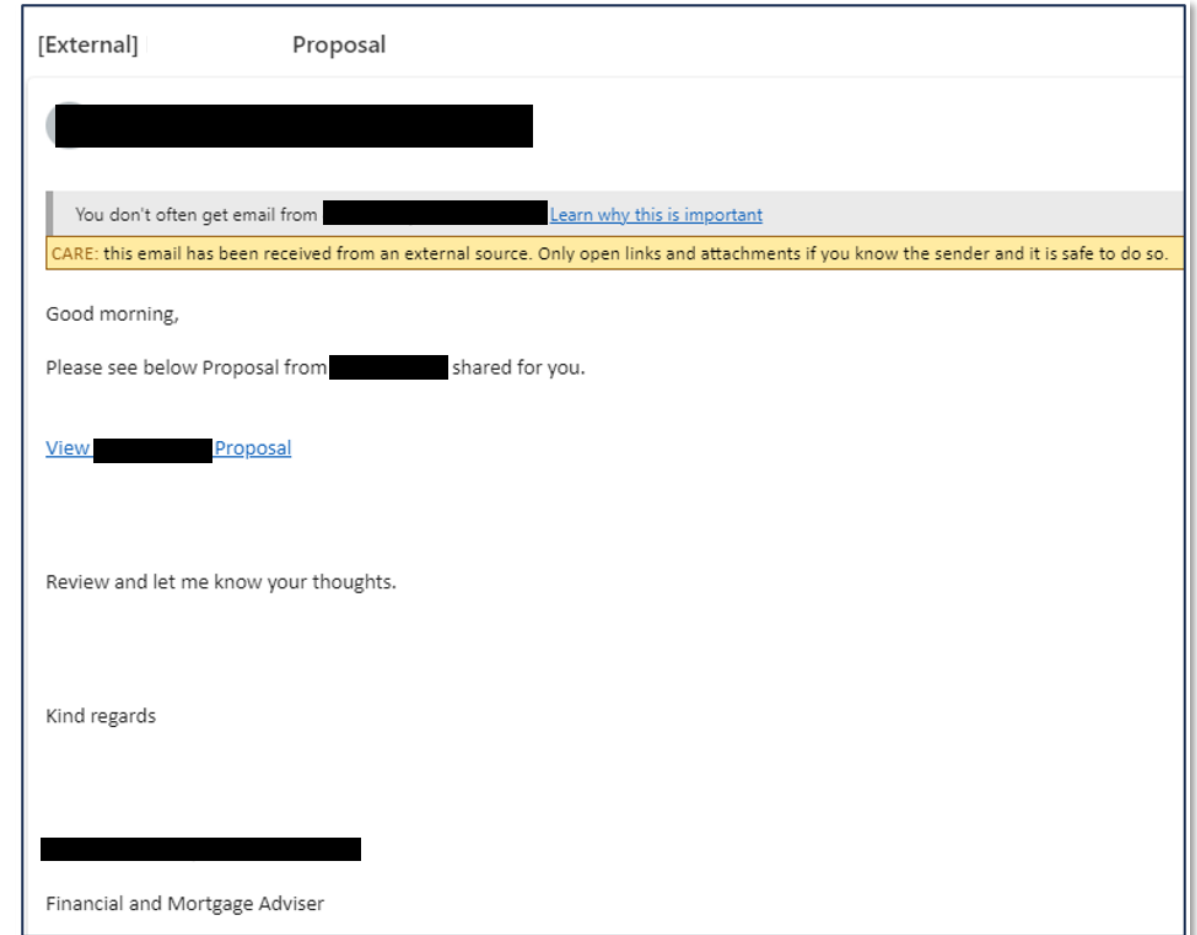
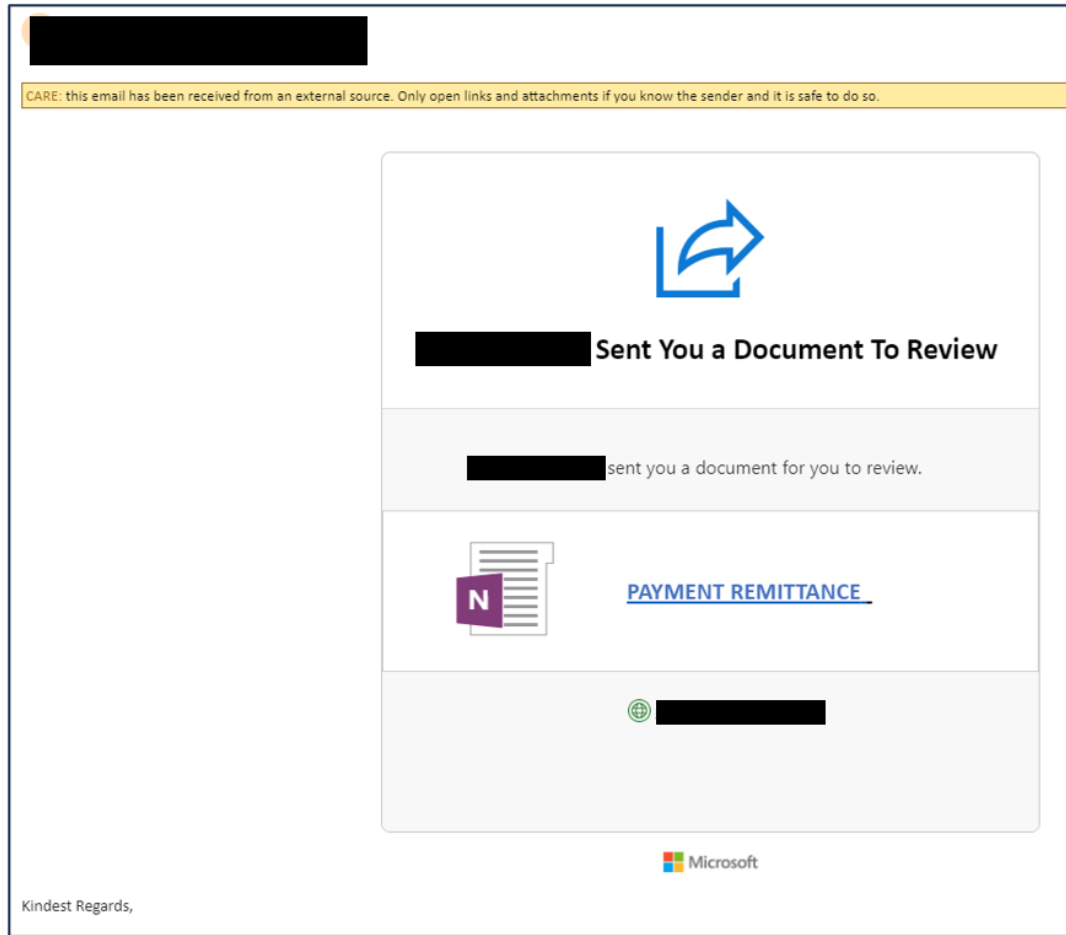
I would like you to perform a confidential task for me urgently, send me your WhatsApp number .

Kind Regards.

Martin

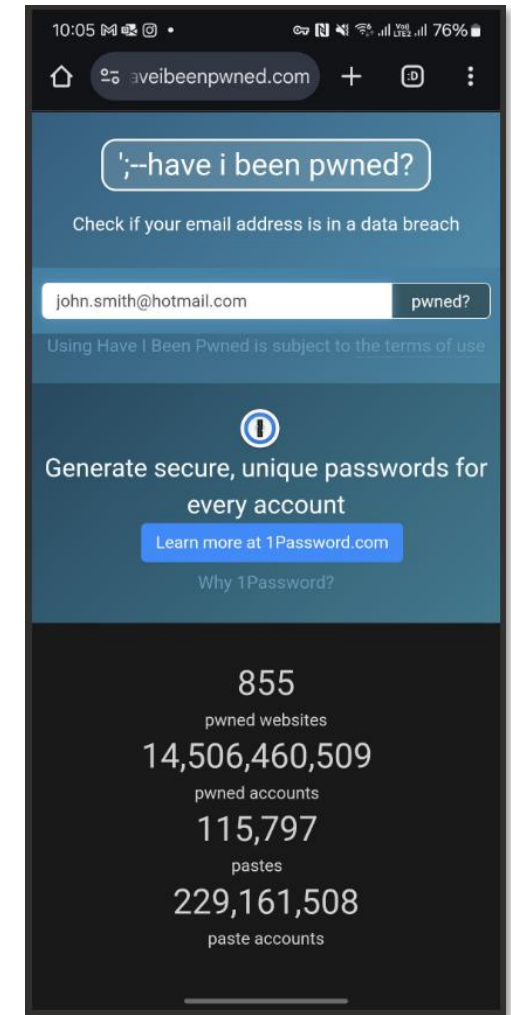
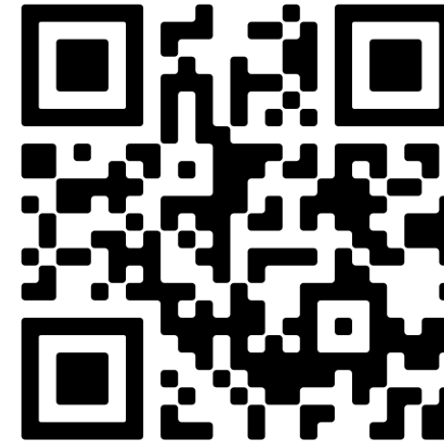
Financial advisers are no exception

Emails we've seen from hacked advisers

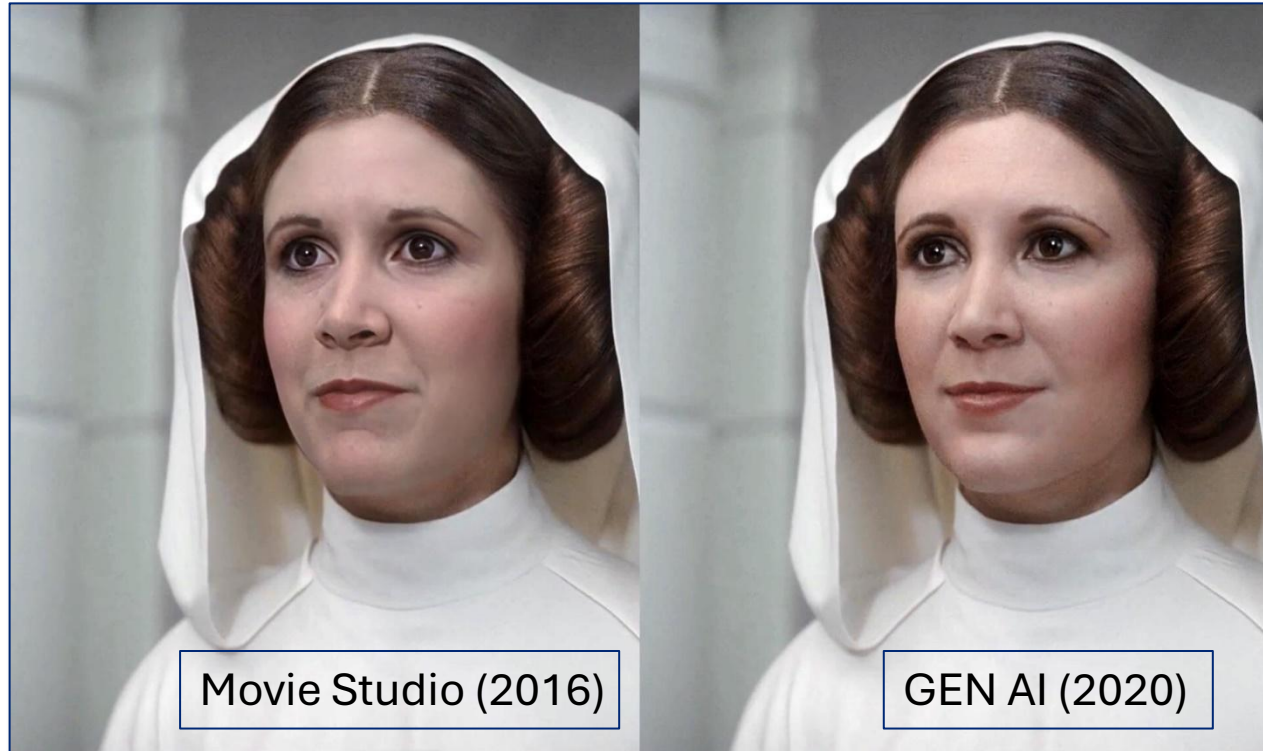


Is your data in breach?

- Have you ever checked to see if your email address has been in a data breach?
- Scan the QR code to check for yourself...



Increase in home PC power



UK engineering firm Arup falls victim to £20m deepfake scam

Hong Kong employee was duped into sending cash to criminals by AI-generated video call

● [Business live - latest updates](#)



Arup confirmed that fake voices and images were used in the fraud. Photograph: Andrew Brookes/Getty Images/Image Source

Deepfake in audio in politics

POLITICO

UK general election | War in Ukraine | Israel-Hamas war | Newsletters | Podcasts | Poll of Polls | Policy news | Events


NEWS > TECHNOLOGY UK

Keir Starmer suffers UK politics' first deepfake moment. It won't be the last

Deepfake of opposition leader is still racking up views, as experts warn UK response to AI-generated fake content barely scratches the surface.

▶ LISTEN ◻ SHARE

POLITICO PRO Free article usually reserved for subscribers



0:00 / 0:24 Have you got it?

An audio clip appearing to show UK opposition leader Keir Starmer swearing at staffers went viral | Leon Neal/Getty Images

Slovakia's Election Deepfakes Show AI Is a Danger to Democracy

Fact-checkers scrambled to deal with faked audio recordings released days before a tight election, in a warning for other countries with looming votes.



PHOTOGRAPH: ZUZANA EDOGVA/GETTY IMAGES

JUST TWO DAYS before Slovakia's elections, an audio recording was posted to Facebook. On it were two voices: allegedly, Michal Šimečka, who leads the liberal Progressive Slovakia party, and Monika Tódová from the daily newspaper Denník N. They appeared to be discussing how to rig the election, partly by buying votes from the country's marginalized Roma minority.



Official Men's Grooming Supplier

Source: The BBC (<https://www.bbc.co.uk/news/world-us-canada-68064247>) and Politico (<https://www.politico.eu/article/uk-keir-starmer-labour-party-deepfake-ai-politics-elections>)

Manipulated videos of global leaders

Use of deepfake for political gain



Manipulated videos of trusted individuals

Use of deepfake for monetary gain

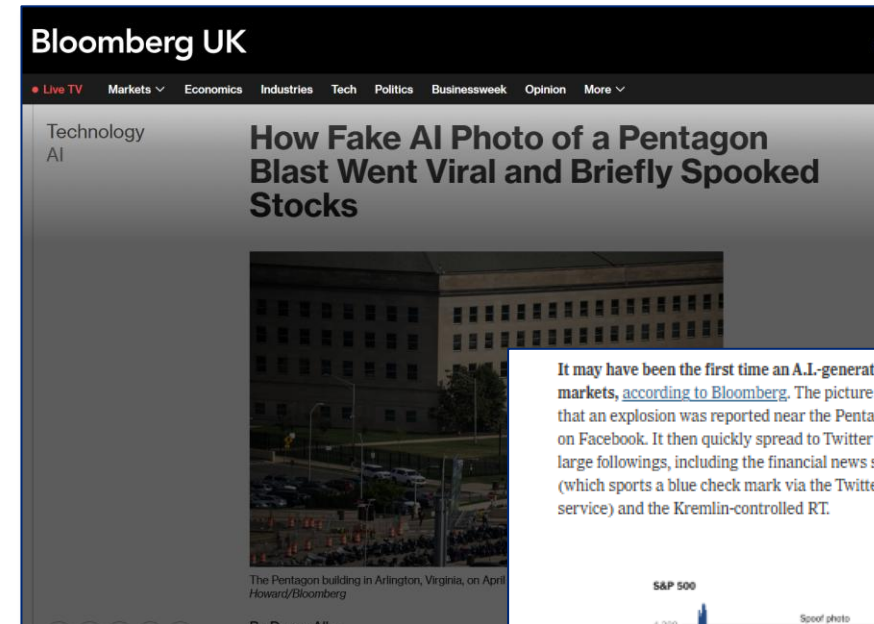


Source : Good Morning Britain, 2023

Impact of deepfakes on markets

Fake news, real market drop

- The potential for AI to exploit the “fragility” of the financial systems.
- The need for regulatory oversight to audit and, when necessary, restrict systems that go beyond a certain level of capability.



It may have been the first time an A.I.-generated image moved markets, according to Bloomberg. The picture — which claimed that an explosion was reported near the Pentagon — first appeared on Facebook. It then quickly spread to Twitter via accounts with large followings, including the financial news site ZeroHedge (which sports a blue check mark via the Twitter Blue subscription service) and the Kremlin-controlled RT.

Within minutes, internet sleuths began to debunk the image, and soon after ZeroHedge and RT deleted it from their accounts, while

Source: The BBC (<https://www.bbc.co.uk/news/world-us-canada-68064247>) and Politico (<https://www.politico.eu/article/uk-keir-starmmer-labour-party-deepfake-ai-politics-elections>)

Future of fraud forecast

5 emerging fraud risks for business and consumers

Generative AI
accelerates DIY
fraud

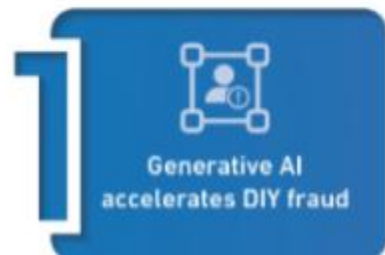
Branches are
cool again

Retailers hit
with empty
returns

Synthetic
identity fraud
will surge

Fraudsters
expand into
cause-related
and investment
deception

Experian suggests consumers and businesses watch out for these **five fraud threats in 2024**:



Source: Experian, 2024

The importance of
*third-party due
diligence* in
protecting client
assets



Why is third-party & vendor due diligence is crucial?

Morgan Stanley hit with \$60m penalty for failing to properly decommission old kit hosting 'wealth management' data

Banking giant rapped over management of two US bit barns

Matthew Hughes

Tue 13 Oct 2020 // 14:44 UTC

Banking giant Morgan Stanley has been ordered to pay a \$60m civil penalty over allegations it failed to properly decommission hardware from two of its US data centres in 2016.

Morgan Stanley

These included lapses in subcontracting the work to third parties, and a failure to keep an inventory of customer data stored on obsolete hardware.



The US Securities and Exchange Commission is launching its own investigation into the vulnerability in Progress Software's MOVEit transfer tool that exposed data from more than 2,000 organizations and 60 million individuals.

Tracked as CVE-2023-34362, the flaw was exploited as a zero-day by the notorious Russia-linked CIOp ransomware group to steal data from organizations using the MOVEit Transfer managed file transfer (MFT) software.

270,000 UK forces records thought to have been exposed to Chinese hackers

Payroll data at risk includes names, bank details and addresses of current and former force members, government sources suggest

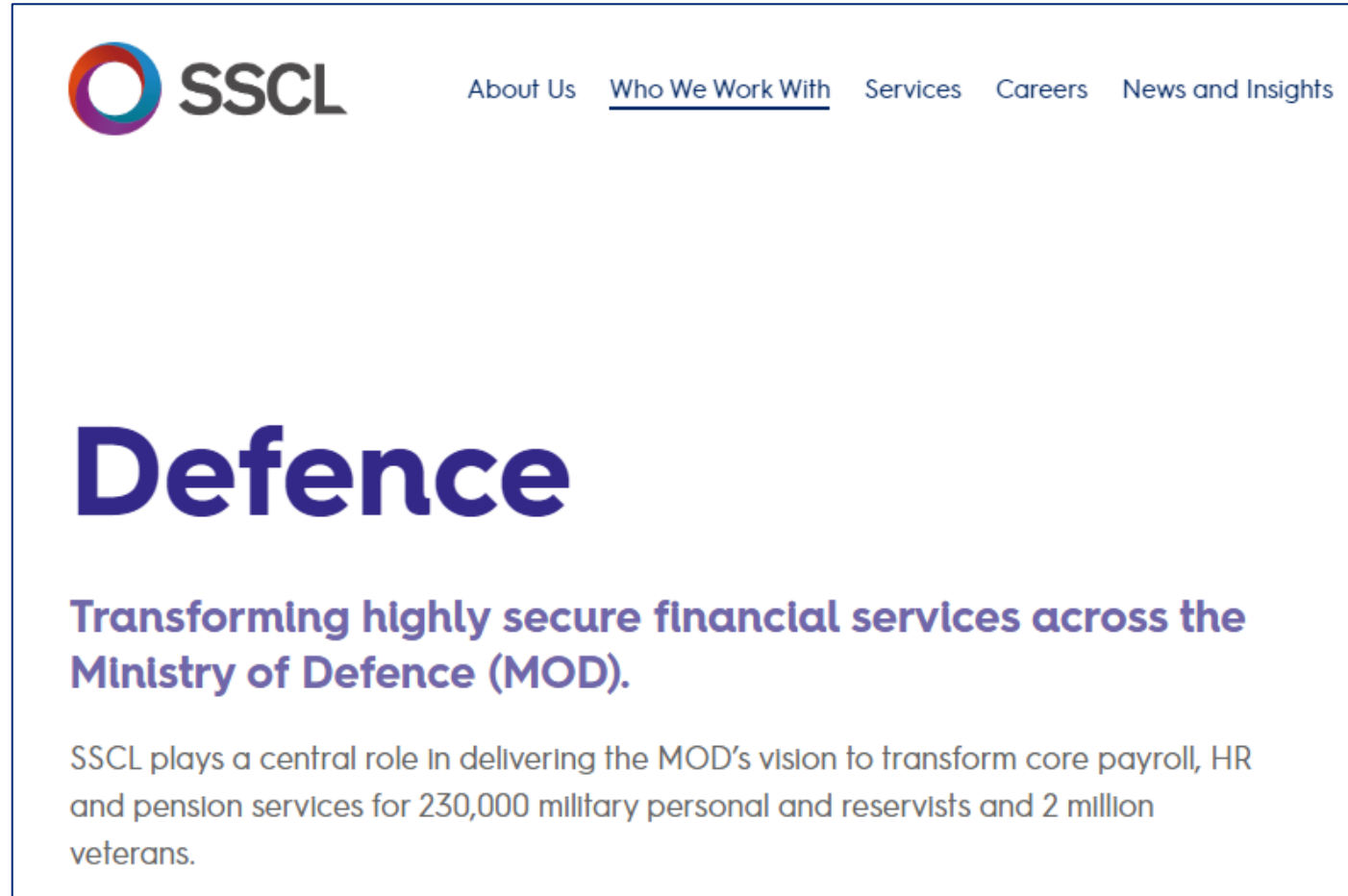


Ministry of Defence

The MoD building in London. The UK defence secretary, Grant Shapps, is expected to brief MPs on Tuesday afternoon. Photograph: Neil Hall/EPA

An estimated 270,000 payroll records belonging to nearly all members of Britain's armed forces have been exposed to Chinese hackers in a breach at a third-party contractor that was discovered a few days ago.

Is advertising that you process sensitive data a good idea?



The screenshot shows the SSCL website header with navigation links: About Us, Who We Work With, Services, Careers, and News and Insights. The main heading is 'Defence' in a large, bold, dark blue font. Below it is a sub-heading: 'Transforming highly secure financial services across the Ministry of Defence (MOD)'. The text below describes SSCL's role in delivering the MOD's vision to transform core payroll, HR, and pension services for 230,000 military personnel and reservists and 2 million veterans.

SSCL About Us Who We Work With Services Careers News and Insights

Defence





Transforming highly secure financial services across the Ministry of Defence (MOD).

SSCL plays a central role in delivering the MOD's vision to transform core payroll, HR and pension services for 230,000 military personal and reservists and 2 million veterans.

Reporting fraud



Drivers of vulnerability

Health 	Life events 	Resilience 	Capability 
<ul style="list-style-type: none">• Physical disability• Severe or long-term illness• Poor mental health• Addiction• Low mental capacity or cognitive impairment	<ul style="list-style-type: none">• Caring responsibilities• Bereavement• Relationship breakdown• Domestic abuse• People with non-standard requirements such as people with convictions, care leavers, refugees• Retirement	<ul style="list-style-type: none">• Low or erratic income• Over indebtedness• Low emotional resilience	<ul style="list-style-type: none">• Low knowledge or confidence in managing finances• Poor literacy or numeracy skills• Poor or non-existent digital skills• Learning impairments• No or low access to help or support

Your role in this...

Complete DD on the firms
that you're working with

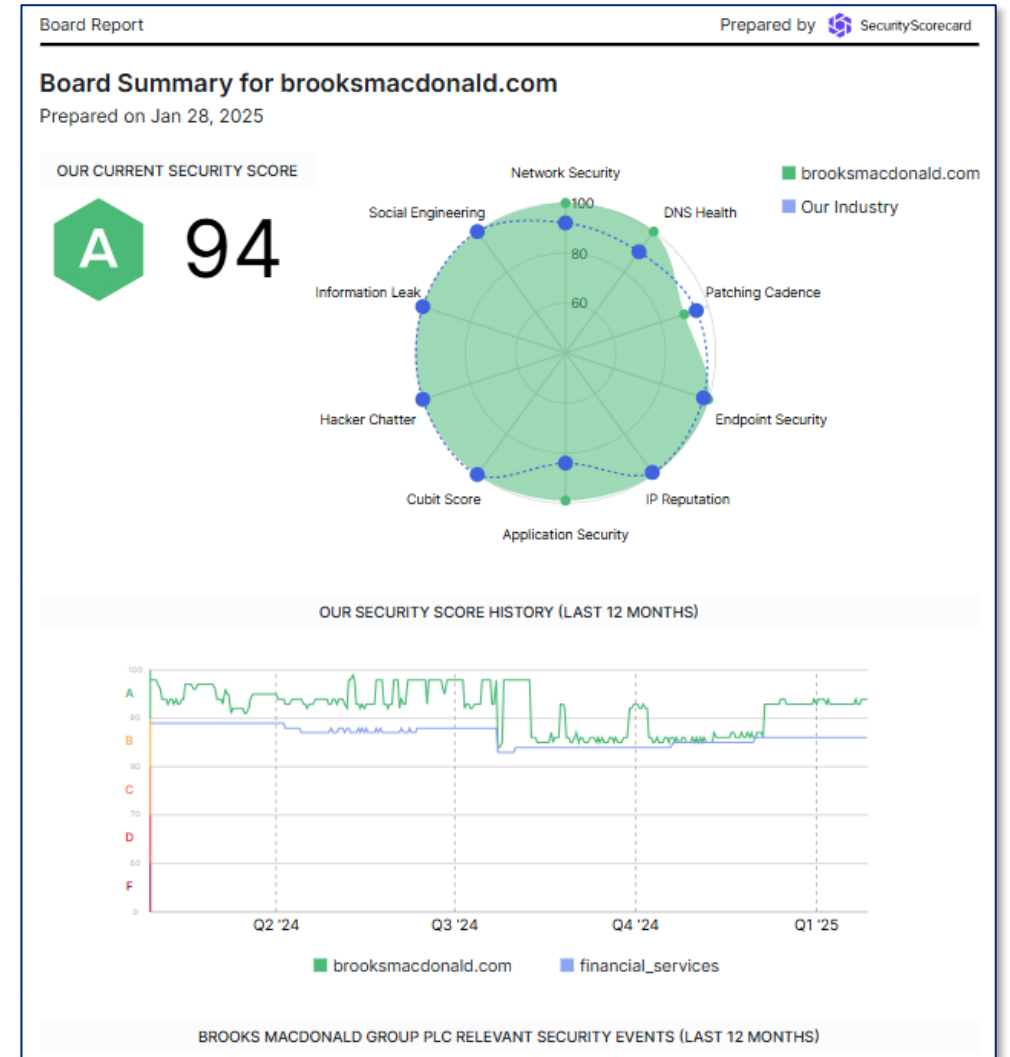
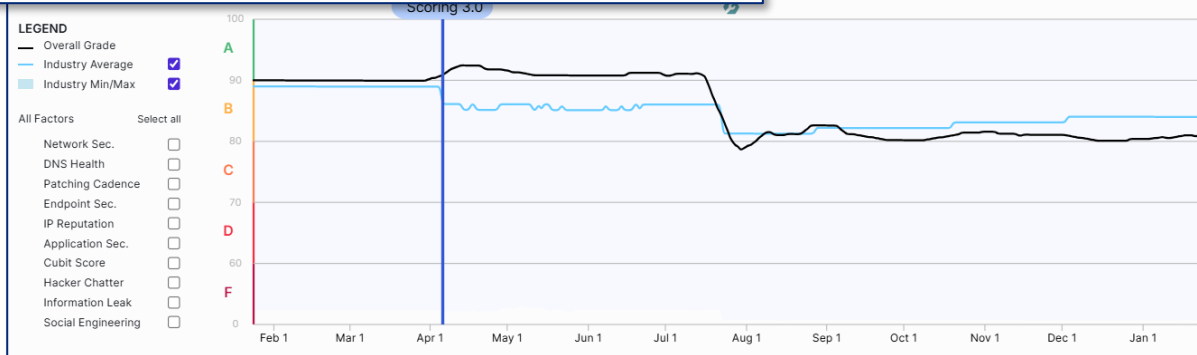
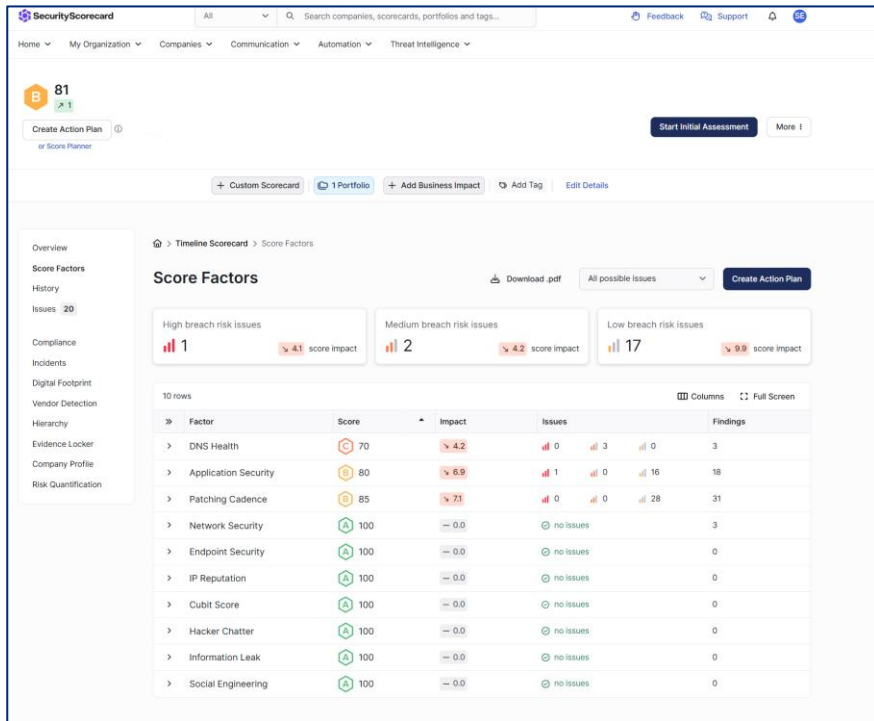
Reliance on others –
Client data, security

Agent as client –
platform due diligence
PI /business risk

Document
process –
governance and oversight

Immediately
report
suspicious emails

Cybersecurity and due diligence



Trust in your partners and providers



CYBER ESSENTIALS

CERTIFICATE OF ASSURANCE

BROOKS MACDONALD GROUP PLC
21 Lombard Street London EC3V 9AH
COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS SCHEME

NAME OF ASSESSOR : Glen Patrick
CERTIFICATE NUMBER : 32bf1112-d00a-4331-b861-1c840d1d3138 DATE OF CERTIFICATION : 2024-05-03
PROFILE VERSION : 3.1 (Montpellier) RECERTIFICATION DUE : 2025-05-03
SCOPE : Whole Organisation

SCAN QR CODE TO VERIFY THE AUTHENTICITY OF THIS CERTIFICATE

CERTIFICATION MARK:  CERTIFICATION BODY:  CYBER ESSENTIALS PARTNER: 

The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials implementation profile and thus that, at the time of testing, the organisations ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisations defences will remain satisfactory against a cyber attack.



CYBER ESSENTIALS PLUS

CERTIFICATE OF ASSURANCE

BROOKS MACDONALD GROUP PLC
21 Lombard Street London EC3V 9AH
COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS PLUS SCHEME

NAME OF ASSESSOR : Brynmor Trotter
CERTIFICATE NUMBER : bb3c247e-72cc-4b1f80f8-5befb363c6e5 DATE OF CERTIFICATION : 2024-07-15
PROFILE VERSION : 3.1 (Montpellier) RECERTIFICATION DUE : 2025-07-15
SCOPE Whole organisation

SCAN QR CODE TO VERIFY THE AUTHENTICITY OF THIS CERTIFICATE

CERTIFICATION MARK:  CERTIFICATION BODY:  CYBER ESSENTIALS PARTNER: 

The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials Plus implementation profile and thus that, at the time of testing, the organisations ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisations defences will remain satisfactory against a cyber attack.

Why this matters?

Consequences of a successful attack

REPUTATIONAL DAMAGE

OPERATIONAL DISRUPTION

FINANCIAL LOSSES

LEGAL AND REGULATORY PROBLEMS

CUSTOMER LOSS/DISTRUST

CLEANUP COSTS

Learning outcomes



Understand the evolving landscape of cyber security



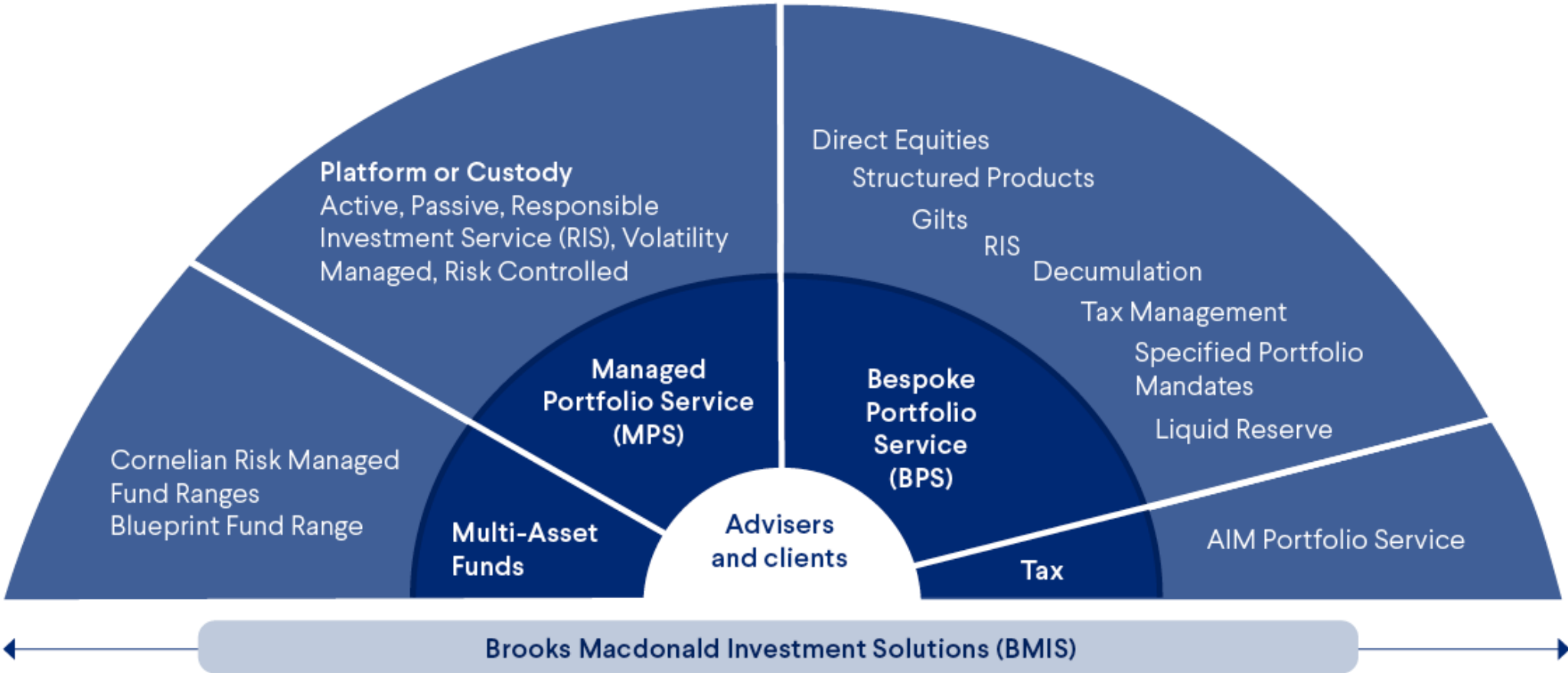
Recognise the risks AI poses for cybersecurity and financial crime



Understand the importance of third-party due diligence in protecting clients' assets

Depth and breadth

Compelling solutions built from demonstrable expertise



BM BROOKS MACDONALD

FOR PROFESSIONAL ADVISERS ONLY

Brooks Macdonald: *Your Partner in Wealth Management*

*Realising Ambitions.
Securing Futures.
We are Brooks Macdonald.*

Our CIP involves research, the assessment, and repeatable and discernible process with explicit outcomes. Here is an outline of its key processes:

- Internal Research
- External Research
- Asset Allocation
- Investment Construction

What sets our CIP apart

The CIP aims to provide a consistent strategy across Brooks Macdonald, the investment manager, on the location solution you choose. Our investment takes an active role in the world, making us can truly represent our

Minimum investment

Level of personalisation: AIM, BPS, BMIS, MFS, FMFS, Multi-Asset, SVS Composites

Collage of lifestyle images: a man in a suit, a family, a woman with a child, a man with a soccer ball, a woman on a phone, a man with an elderly woman, a woman with a child, a woman with a dog, a man with a woman, a man with a woman, a man with a woman, a man with a woman.

- Adviser led
- Independent, financial strength
- Market leadership pioneering solutions for advisers

Important information

All data provided by Brooks Macdonald accessed as at 31 December 2024, unless otherwise stated. This document is intended for professional advisers only and should not be relied upon by any persons who do not have professional experience in matters relating to investments.

Investors should be aware that the value of investments and the income from them may go down as well as up and neither is guaranteed. Investors could get back less than they invested. Past performance is not a reliable indicator of future results.

Please be aware that this service utilises structured products as part of the portfolio construction/strategy which comes with specific risks. Should the counterparty fail, you may not have access to the Financial Services Compensation Scheme (FSCS). Investors should speak to their advisers for further information and to ensure they understand the risk and return factors applicable in their case.

Important information continued

The MSCI information may only be used for your internal use, may not be reproduced or re-disseminated in any form and may not be used as a basis for or a component of any financial instruments or products or indices. None of the MSCI information is intended to constitute investment advice or a recommendation to make (or refrain from making) any kind of investment decision and may not be relied on as such. Historical data and analysis should not be taken as an indication or guarantee of any future performance analysis, forecast or prediction. The MSCI information is provided on an “as is” basis and the user of this information assumes the entire risk of any use made of this information. MSCI, each of its affiliates and each other person involved in or related to compiling, computing or creating any MSCI information (collectively, the “MSCI Parties”) expressly disclaims all warranties (including, without limitation, any warranties of originality, accuracy, completeness, timeliness, non-infringement, merchantability and fitness for a particular purpose) with respect to this information. Without limiting any of the foregoing, in no event shall any MSCI Party have any liability for any direct, indirect, special, incidental, punitive, consequential (including, without limitation, lost profits) or any other damages. (www.msci.com).

Brooks Macdonald is a trading name of Brooks Macdonald Asset Management Limited used by various other companies in the Brooks Macdonald group of companies.

Brooks Macdonald Asset Management Limited is authorised and regulated by the Financial Conduct Authority. Registered in England No 03417519. Registered office: 21 Lombard Street London EC3V 9AH.

More information about the Brooks Macdonald Group can be found at brooksmacdonald.com.