INSIGHT REPORT

HOW DIGITAL IDENTITY CAN PROTECT AGAINST MISUSE OF AI

Version 2.1 | 30/06/2023 | Copyright © 2023 OneID Limited

AI IS REALISING ITS POTENTIAL

The concept of Artificial Intelligence (AI) has been around since the early days of computing. But it had not achieved widespread application until this year, with the new 'generative AI' models that have delivered a step-change in AI capabilities, triggering both fear and excitement.

'Good AI' has the potential to be a powerful force for good, enabling improved productivity in writing, music, video, photography, information analysis and problem-solving. Combined with human oversight and control, AI has the potential to enhance our work and increase our leisure time.

However, there are new challenges, particularly in synthetic identity and auto-generated content, which can increase the risk of fraud, misinformation and abuse on social media when AI is misused. This paper argues that strengthening the verification of digital identity is a key deterrent against the risks that 'bad AI' is generating.

CONTENTS

AI IS FACILITATING SYNTHETIC IDENTITY AND HARMFUL AUTO-GENERATED CONTENT

'Bad AI' is being used to create fictitious humans ('synthetic identities') to open online accounts and also being used to generate the harmful content that those accounts then publish.

Synthetic identities are created using a combination of real and fake personal information, to open accounts with the intention of doing harm. Traditionally, this meant merging textual data, for example, a real address with a fictitious name, but increasingly, AI is generating images and videos that make detection harder. Together, these new practices raise serious concerns about trust in identity on the internet and the authenticity and accountability for content.

Online platforms and businesses are using 'good AI' to filter and identify harmful content, but this is only part of the solution; as soon as content is removed and the account closed, another account is opened.

This paper describes how digital identity can be an additional effective tool in the fight against synthetic identities and auto-generated content. By adopting robust digital identity solutions, we can strengthen trust, ensure accountability and provide greater security in an increasingly AI-driven world.

To avoid the erosion of trust online, we need to be able to answer two key questions:

- **Is the content author a real human and who they claim to be?**
- **Is what they are telling or showing me true?**

FRAUDSTERS ARE USING AI TO ENABLE ENHANCED ID THEFT AND FRAUD

The ease with which AI can create synthetic identities is driving a rapid growth in identity theft and fraud. Fraudsters are exploiting these identities for various malicious activities, such as financial fraud, data breaches, illegal transactions and online abuse; we can no longer be certain who we are interacting with online, as most platforms perform little or no identity verification on account creation.

Fraudsters who use impersonation and social engineering are deploying AI technology in phishing scams. Generative AI tools are capable of creating convincing content, including documents, videos, images and audio. Deepfake videos or audio recordings can be manipulated to make it appear that someone is saying or doing something which never happened. Deepfakes can be used to spread misinformation, damage reputations, or even incite violence. Individuals, governments and businesses are increasingly vulnerable to scams.

Historically, cyber-fraudsters needed technical skills to produce fake documents or websites. But today, bad actors with no knowledge of coding can quickly create malware and chatbots to trap victims, using tools that are readily available.

JUST HOW EASILY CAN AI DECEIVE US?

Imagine a scenario where AI creates a synthetic identity and finds a platform with weak or very basic identity checks on new accounts. AI creates an account and posts a listing for a new property to rent, with enticing pictures and pricing.

To support this advert, AI creates top reviews from other fraudulent accounts. AI then '"chats'" with prospective customers answering queries, taking bookings and receiving payment in advance. AI quickly moves the money to an offshore account, deletes the listing account and disappears… until next time, when the scam can be repeated at scale and before the fraud is detected. It is easy to be duped now.

Online Fraud is now a "national crisis" and needs urgent action.

GOVERNMENT AND BUSINESSES NEED BETTER TOOLS TO PROTECT AGAINST "BAD AI"

As AI becomes weaponised by fraudsters, organisations need to keep pace by using multiple layers of protection to ensure that they know who they are dealing with, to protect themselves and their customers. Our new national fraud strategy calls for better tools to block fraudsters.

Digital identity verification solutions have emerged as a valuable tool in the fight against fraud. The first generation of these involved taking photos of official documents such as passports and driving licenses, and matching the picture from the document with a selfie. These solutions cause too much friction in the process of setting up many account types.

A second generation, reusable digital identity solution is now available in the UK, that leverages the identity checks that banks have already done on their customers, and benefits from the security technologies that the banks have already invested in.

Bank-verified identity checking is widely used in other countries to successfully reduce fraud, and can now be used in the UK to verify individuals in a few seconds, making it a very low friction addition to the account setup process.

ACCOUNT AUTHENTICATION ENABLES TRACEABILITY AND ACCOUNTABILITY FOR ONLINE CONTENT

New digital identity solutions can enable content creators to authenticate their work, which in turn strengthens trust. Digital signatures (or watermarks) linked to verified identities can demonstrate the authenticity and integrity of content.

We can place greater reliance on content whose source or provenance can be traced. In this way, digital identity solutions strengthen trust and security online by providing a robust authentication mechanism to quickly establish who is responsible for content.

Digital identity solutions can be used to enable the attribution of AI-generated content to specific individuals or entities. By linking content to verified digital identities, it becomes, and they can therefore be held easier to hold individuals accountable for the information they generate or share.

WE NEED TO BE ABLE TO FILTER OUT UNWANTED NOISE FROM UNVERIFIED

We need to be able to turn off AI-generated misinformation, and focus our precious time on authenticated, genuine content. If platforms gave users the ability to turn off content from unverified accounts, content tagged with a verified digital ID could be prioritised to pass through an individual's filters, while unverified AI-generated content would be filtered into the 'noise' feed. This would create a safer and more pleasant online user experience.

WHY BANKS PLAY A KEY ROLE IN PROVIDING DIGITAL IDENTITY

Banks enjoy a strong position of trust. We all trust banks with our savings and payments. Banking regulation requires that banks apply rigorous Know Your Customer (KYC) and Anti-Money Laundering (AML) checks to verify the identity of their customers and ensure they are not criminals, terrorists or engaged in money-laundering. It is thanks to this comprehensive level of checking that banks are ideally placed to support digital identity verification.

Banks are also under constant attack by cyber-criminals and must maintain a higher IT security spend than any other sector to protect against illicit access to bank accounts. Banks have a better track record than other industries in protecting their customers' personal data.

Banks are continually introducing new techniques to protect against fraud; examples such as 'Strong Customer Authentication' to check the right person is present, and 'Confirmation of Payee' to enable the person sending money to check the receiver's details match what they expect. Digital identity verification is another tool to fight fraud.

NEW REGULATION AND MARKET INFRASTRUCTURE UNDERPIN DIGITAL ID VERIFICATION

The UK government has modernised the UK identity landscape by introducing a framework for certified digital IDs. UK banks have also, via Open Banking, developed an infrastructure which enables individuals to securely authorise their bank to exchange account data with suitably regulated parties.

The combination of the identity framework and modern bank data-sharing platform have enabled new secure, regulated and certified identity services. Different data sets can be shared with a business, government entity or indeed another bank, depending on the type of verification that is required; this could be name, address and date of birth, contact information, or indeed just that 'I am a human' or 'I am over 18'. And all of this is under the control of the individual who sees and consents to the data being shared each time.

DIGITAL IDENTITY'S POWERFUL REACH AND EASE OF USE

A bank-based digital identity solution allows any business or government entity to immediately verify the identity of anyone with an online bank account in the UK, which equates to nearly 50 million individuals.

Government and businesses can enable prospective and existing customers to quickly provide consent to their bank to verify their identity, with just a few clicks and in real time. Users do not need to download an app, nor upload documents or photos to a new website. Instead, they simply use their banking app to consent to their bank sharing ID data with any specified organisation which has activated this service.

BANK-VERIFIED ID IS FASTER AND MORE SECURE THAN DOCUMENT SCANNING

The conventional process of checking identity by uploading documents and taking selfies can be a slow and clunky experience which is prone to errors. This is turn can lead to consumers users abandoning their attempts to access a particular product or service. The proliferation of AI-created fake documents and photos also makes it challenging to filter out synthetic identities.

BANK-VERIFIED DIGITAL ID IS WELL POSITIONED TO CUT AI-DRIVEN FRAUD AND DEEPFAKES

Individuals can now easily and securely use their bank-checked and bank-protected personal data to provide real time digital ID verification. Digital identity is a powerful new tool in the fight against fraud, misinformation and online abuse.

Bank-led digital ID services are already widely used in the Nordics, with a solution known as BankID. In Norway, the cost of fraud has been reduced to a tiny fraction as a result of widespread use of BankID.

The UK needs to catch up with these market leaders, especially if it is to fulfil its aspiration to be a technical superpower. In Norway, with widespread use of BankID, fraudulent payment transactions have reduced from 1% of all transactions to 0.00042%.

The UK also aspires to be a world centre for AI regulation and ethics. Digital identity is an enabler for more ethical AI; it brings accountability. By enabling bank-verified digital identity services, there is now a viable way for government, businesses and banks to protect their customers from the threats brought by AI, whilst enabling us all to safely enjoy the benefits of productivity and creativity that AI brings.

ABOUT THE AUTHOR

This paper was produced by OneID®; the only provider of truly digital, real-time identity services that create absolute certainty between a business and a customer, in the fastest, cheapest and safest way.

It is the only UK identity service with access that leverages bank-verified data to ensure that every transaction is protected by the most advanced counter-fraud measures.

About OneID®

OneID® is the only provider of truly digital, real-time identity services that create absolute certainty between a business and a customer, in the fastest, cheapest and safest way.

Our digital ID services use the most advanced counter-fraud measures to help protect banks, businesses and consumers from online identity fraud. By streamlining existing ID processes, including payments, direct debits, onboarding and more, we help businesses reduce operational costs, increase sales and improve customer engagement. As the only UK Identity Service with access to bank-verified data, 40m UK adults are already set up to use OneID®, for real-time verification. OneID® is government certified, regulated by the FCA and is a BCorp business.

Headquartered in the UK, we have brought together the best people in Digital Identity, Payments, Banking, Technology and Government to ensure we make the world a safer place.

To learn more visit **www.oneid.uk**.

FOR MORE INFORMATION
Contact Keith Mabbitt,
07790 494 836

© Copyright Digital Identity Net UK Limited 2023