Criminals are using AI to create fake documents to trick businesses

Opinion By Francisco Rodrigues, Adam Maurer published 22 hours ago

Document forgery requires tech solutions - here's what you need to know

(Image credit: Shutterstock)

We may not think much about it, but businesses need to rely on digital and physical documents every day. Decisions, purchases, and deals worth millions hinge on information in official documents being trustworthy. In the new world that AI has brought about, forged or altered documents are becoming not only very convincing, but also available to anyone with basic AI tools.

The news cycle has been replete with cases of AI being used to fake crucial documents like IDs – and these only scratch the surface. AI has given fraudsters the tools for fabricating invoices, tax forms, investment contracts, risk assessments, financial audits, and procurement documents among others.

A report on AI-assisted fraud found that digital document forgeries increased 244% between 2023 and 2024 making it one of the fastest growing categories of business-related fraud going into 2025. For businesses operating into the next decade, the possibility that they cannot trust their own internal documents is becoming a problem that is impossible to ignore.

Adam Maurer, Francisco Rodrigues

COO and Product Manager for Truth Enforcer at Connecting Software respectively.

Faked documents do real harm to businesses

While cases of significant fraud will be rare given the layers of internal security and regulations that prevent decision making being centered on one person or one document, the real damage this will do will be to trust. Without a reliable and quick way to authenticate documents businesses may have to add hours into processes of checking and re-verifying documents, even when they are perfectly legitimate.

At best, this will add a significant inefficiency to many businesses, wasting time and effort – but at worst, it can grind operations almost to a standstill – costing businesses the critical advantage of time against their competitors.

This creates a need to counter this by creating systems that distinguish authentic documents from tampered ones.

How tech restores trust

Responding to this critical problem, new technologies focused on document verification have developed quickly. Principally, the solutions that exist fall into four main categories blockchain-based solutions, AI detection, Identity Verification Technology (IDVT), and Public Key Infrastructure (PKI). Here's what you need to know about them:

Blockchain

While Blockchain started as a means for facilitating cryptocurrencies, it's since become a legitimate platform for business applications, where the immutability of blockchains present significant security benefits when integrated into business software and processes.

Blockchain authentication solutions create tamper-proof documents by matching them with cryptographic hashes - meaning that a document can always be checked against its hash. Fundamentally, blockchain's decentralized nature makes it nearly impossible for bad actors to change internal records stored on the platform, providing a reassurance that once a document is placed on the blockchain, you will always be able to verify it against the authentic version.

Since document hashing takes place in your own environment and hashes cannot be reverse engineered to rebuild the document, this method allows you to avoid sending any sensitive data to third parties.

There are some legitimate concerns about the blockchain's environmental costs given the vast amounts of computing and energy needed to maintain it, although different blockchains offer different advantages in this regard.

AI-detection

AI anomaly detection identifies metadata, formatting, and other criteria for mismatches. This is certainly the most straightforward option – as AI's have become surprisingly adept at spotting the output of other AI. That said, while it can be a cost-effective solution, there is no way of guaranteeing its accuracy given AIs notorious hallucinations. Given this, it can be an effective 'first layer' against forgery but should not be relied upon exclusively.

IDVT

IDVT uses AI to scan metadata and security protocols to detect fakes. This scanning procedure can cross-reference the protocols with trusted databases to prevent using forged credentials in business transactions. The process essentially provides a checkpoint for all your data – documents are flagged immediately if it doesn't match the protocols stored on an organizations database.

IDVT is sometimes hampered by overreliance on database accuracy. Organizations typically require a lot of resources in terms of infrastructure, personnel, and access to reliable data sources to set it up – making it prohibitively expensive for small and medium companies. It's also prone to human error- if an employee sets up protocols incorrectly, the solution becomes near useless.

PKI

PKI relies on shareable digital certificates that authenticate a document's origin and integrity. Using the issuer's public key to check the certificate, both first parties and third parties can check its authenticity. It has the advantage of being intuitive to set up, but has gained an unfortunate reputation of being somewhat insecure – if bad actors are able to obtain the keys and/or modify them, they can certify modified documents as authentic.

Regulation needs to be the answer to systemic document forgery

The truth is, AI forgery is not a business-by-business level problem, but a systemic one that will need higher level regulation to address. Eventually, it will become critical for governments to impose baseline metadata standards and mandatory verification technology that can make vital public documentation verifiable by everyone.

We cannot afford to regard AI forgeries as a distant problem – the threat of serious harm being caused by an AI-doctored document grows daily. Operating a business or running a government where we cannot trust the documents we depend on is an impossible task. Embracing these technologies not only allows us to head off this potential crisis of trust, but can open new opportunities to make the organizations we rely on more transparent.

We've featured the best authenticator app.

This article was produced as part of TechRadarPro's Expert Insights channel where we feature the best and brightest minds in the technology industry today. The views expressed here are those of the author and are not necessarily those of TechRadarPro or Future plc. If you are interested in contributing find out more here: https://www.techradar.com/news/submit-your-story-to-techradar-pro

Adam Maurer

Adam Maurer is COO at Connecting Software.