



**POLICE
SCOTLAND**

Keeping people safe

POILEAS ALBA

North East

CRIMEALERT

Keeping Communities in the North East Safe

ARTIFICIAL INTELLIGENCE SPECIAL



Welcome to a special Artificial Intelligence (AI) edition of North East Crime Alert.

In a departure from our normal content we look at how AI is shaping our engagement with the online world and how we stay safe in 2025.

In this special edition of North East Crime Alert:

We've all heard about Artificial Intelligence (AI), well, what exactly is it and how does it work? We explain.

What are the most commonly available AI programmes?

We look at how criminals may use AI in 2025 to create frauds that are even more convincing.

Advice on how we navigate the digital world safely using AI.

Plus, we share the experiences of two recent fraud victims.



Website

www.scotland.police.uk



Twitter

[www.twitter.com/
NorthEPolice](https://www.twitter.com/NorthEPolice)



Facebook

[www.facebook.com/
NorthEastPoliceDivision](https://www.facebook.com/NorthEastPoliceDivision)

This newsletter has been produced with the assistance of Microsoft Co-Pilot by the Police Scotland North East Division Crime Reduction Team.

Criminals are using ever more sophisticated methods. By staying better informed and working in partnership we can ensure our communities continue to be a safe place to live and work.



Understanding Artificial Intelligence

What is it and how does it work?

Artificial Intelligence (AI) is a term that often pops up in conversations about technology and the future. But what exactly is AI and how does it impact our daily lives? Let's break it down in simple terms.

What is Artificial Intelligence?

Artificial Intelligence refers to the ability of machines to perform tasks that typically require human intelligence. These tasks include learning from experience, understanding language, recognising patterns, solving problems and making decisions. Essentially, AI enables computers and other devices to think and act in ways that mimic human capabilities.

Types of AI

AI can be broadly categorised into two types: Narrow AI and General AI.

Narrow AI

This type of AI is designed to perform a specific task. Examples include virtual assistants like Siri and Alexa, which can understand and respond to voice commands and recommendation systems used by Netflix and Amazon to suggest movies or products based on your preferences. Narrow AI is highly effective within its limited scope but cannot perform tasks outside its designated function.

General AI

Also known as Artificial General Intelligence (AGI), this type of AI would have the ability to understand, learn and apply knowledge across a wide range of tasks, much like a human. While AGI remains a theoretical concept and has not yet been achieved, it represents the ultimate goal for many AI researchers.

How Does AI Work?

AI systems rely on algorithms, which are sets of rules or instructions that a computer follows to solve problems. These algorithms enable machines to process large amounts of data, identify patterns and make decisions based on that information. Here are some key components of AI.

Machine Learning

A subset of AI, machine learning involves training a computer to learn from data. For example, a machine learning algorithm can be trained to recognise images of cats by being shown thousands of pictures labelled as 'cat' or 'not cat.' Over time, the algorithm improves its accuracy in identifying cats in new images.

Deep Learning

A more advanced form of machine learning, deep learning uses neural networks - complex structures modelled after the human brain - to analyse data. This approach is particularly effective for tasks like image and speech recognition.

Natural Language Processing (NLP)

NLP enables computers to understand and respond to human language. This technology powers chatbots, translation services and voice-activated assistants.

Applications of AI

AI is already integrated into many aspects of our daily lives.

Healthcare

AI helps doctors diagnose diseases, predict patient outcomes, and personalise treatment plans. For instance, AI algorithms can analyse medical images to detect early signs of conditions like cancer.

Finance

Banks and financial institutions use AI to detect fraudulent transactions, assess credit risk and automate trading.

Transportation

Self-driving cars use AI to navigate roads, avoid obstacles and make real-time decisions to ensure passenger safety.

Customer Service

AI-powered chatbots provide instant support to customers, answering questions and resolving issues without human intervention.

The Future of AI

As AI technology continues to advance, its potential applications are virtually limitless. However, with these advancements come important ethical considerations. Issues such as data privacy, job displacement and the potential for biased decision-making must be addressed to ensure that AI benefits society as a whole.

Artificial intelligence is a powerful tool that is transforming various industries and aspects of our lives. By understanding the basics of AI, we can better appreciate its capabilities and how we can stay safe online.



The Future of AI Driven Crime

How criminals may use AI in 2025

As we enter 2025, the landscape of crime is evolving rapidly, with artificial intelligence (AI) playing a pivotal role in how scammers operate. From the perspective of crime reduction and prevention in the UK, understanding and anticipating these changes is crucial for staying ahead of cybercriminals who are increasingly using AI to commit sophisticated crimes.

AI-Enhanced Phishing and Social Engineering

One of the most significant threats posed by AI in 2025 is its ability to enhance phishing and social engineering attacks. AI can generate highly convincing emails and messages that mimic the writing style and tone of legitimate sources, making it difficult for individuals to distinguish between genuine and fraudulent communications. These AI-generated phishing attempts can be tailored to target specific individuals or organisations, increasing their effectiveness and the likelihood of success.

Deepfake Technology

Deepfake technology, which uses AI to create realistic but fake audio and video content, is another area of concern. Scammers can use deepfakes to impersonate trusted figures, such as company executives or family members, to deceive victims into transferring money or divulging sensitive information.

This technology can also be used to create fake news or manipulate public opinion, posing a broader threat to societal trust and security.

AI in Financial Fraud

AI's ability to analyse vast amounts of data quickly and accurately makes it a powerful tool for financial fraud. Scammers can use AI to identify vulnerabilities in financial systems, automate fraudulent transactions, and evade detection by traditional security measures. AI can also be used to create fake identities and documents, further complicating efforts to track and apprehend criminals.

AI-Driven Ransomware

Ransomware attacks are expected to become more sophisticated with the integration of AI. AI can help cybercriminals identify the most valuable targets, optimise the timing of attacks and even negotiate ransom payments. The use of AI in ransomware can enable more rapid and widespread attacks, increasing the potential damage to businesses and individuals.

Impersonation and Identity Theft

AI can be used to create realistic fake identities, complete with social media profiles, photos and even voice recordings. These fake identities can be used to commit various types of fraud, from opening bank accounts to applying for loans. The ability of AI to generate convincing fake identities may make it harder for law enforcement to identify and apprehend criminals.


Law Enforcement Response

To combat these emerging threats, law enforcement agencies in the UK are adopting a proactive and technologically advanced approach. This includes investing in AI-driven tools for detecting and preventing cybercrime, as well as training officers to recognise and respond to AI-enhanced scams. Collaboration with technology companies and cybersecurity experts will also be essential in developing effective strategies to counter AI-driven crime.

Public awareness (such as this newsletter) plays a crucial role in educating individuals and businesses about the risks associated with AI-driven scams and how to protect themselves. Encouraging the use of multi-factor authentication, regular software updates and cybersecurity best practices can help mitigate the risk of falling victim to these sophisticated attacks.

Conclusion

As AI continues to evolve, so too will the methods used by scammers to exploit it. By staying informed about these developments and investing in advanced technologies and training, law enforcement in the UK can better protect the public from the growing threat of AI-driven crime. The fight against cybercrime in 2025 requires a combination of technological innovation, public awareness and international cooperation to stay one step ahead of the criminals.



A Guide to the Most Common AI Software

Readily available applications we can all use

Artificial Intelligence (AI) has become an integral part of our daily lives, often in ways we might not even realise. From virtual assistants to image generators, AI software is designed to make our lives easier and more efficient. Here's a look at some of the most common AI software that the general public uses today.



ChatGPT

Developed by OpenAI, ChatGPT is one of the most popular AI chatbots available. It can generate human-like text based on the prompts it receives, making it useful for a wide range of applications, from answering questions to creating content. ChatGPT is widely used in customer service, education and even for personal assistance.

Google Gemini

Google Gemini, formerly known as Bard, is another powerful AI chatbot. It leverages Google's extensive data and machine learning capabilities to provide accurate and helpful responses. Gemini is integrated into various Google services, making it easily accessible for tasks like searching the web, managing schedules and more.

MidJourney

MidJourney is an AI-powered image generator that transforms text descriptions into visual artworks. This tool is popular among artists and designers for creating unique and high-quality images. It is particularly useful for those who need to generate visuals quickly and efficiently.

QuillBot

QuillBot is an AI writing assistant that helps users improve their writing by paraphrasing text, checking grammar and detecting plagiarism. It's a valuable tool for students, writers and professionals who need to produce clear and polished content.

Hugging Face

Hugging Face is a platform that provides a wide range of AI models and tools, particularly for natural language processing (NLP). It's used by developers and researchers to build and deploy machine learning models. The platform is known for its community-driven approach and extensive library of pre-trained models.

CapCut

CapCut is an all-in-one video editing platform that uses AI to help users create and edit videos. It offers features like automatic captioning, background removal and video enhancement, making it a favourite among content creators and social media enthusiasts.

Character AI

Character AI allows users to create and interact with AI-generated characters. These characters can be based on real people, fictional characters or entirely new creations. The platform is popular for entertainment and educational purposes, providing a unique way to engage with AI.

Microsoft Copilot

Microsoft Copilot is an AI-powered productivity tool integrated into various Microsoft 365 apps like Word, Excel, PowerPoint, Outlook and Teams. It helps users complete tasks more efficiently by providing real-time intelligence and suggestions. For example, in Word, Copilot can help draft documents, summarise text and generate content based on user prompts. In Excel, it can assist with data analysis, formula suggestions and creating charts.

Conclusion

AI software is becoming increasingly accessible and useful for the general public. Whether you're looking to improve your writing, create stunning visuals, or interact with virtual characters, there's likely to be an AI tool that can help. As these technologies continue to evolve, they will undoubtedly become even more integrated into our daily lives, making tasks easier and more efficient.



How to Use AI Safely

Read our guide to staying safe online in 2025

Artificial Intelligence (AI) is now an integral part of our daily lives, from virtual assistants like Siri and Alexa to recommendation systems on Netflix and Amazon. While AI offers numerous benefits, it's essential to use it safely and responsibly. Here's a guide to help you navigate the world of AI with confidence.

Understand the Basics of AI

AI refers to the simulation of human intelligence in machines that are programmed to think and learn. These systems can perform tasks such as recognising speech, making decisions and translating languages. *Understanding the basics of AI can help you make informed decisions about how to use it safely.*

Protect Your Personal Information

One of the primary concerns with AI is data privacy. AI systems often require access to personal data to function effectively. Here are some tips to protect your personal information.

Be Cautious with Personal Data

Avoid sharing sensitive information like your full name, address, phone number, or financial details unless absolutely necessary. Ensure the platform you are using is trustworthy and has robust privacy policies.

Review Privacy Settings

Regularly check and adjust the privacy settings on AI platforms to control what information is shared and how it is used. This can help you manage your data more effectively.

Use Strong Passwords

Protect your accounts with strong, unique passwords and enable multi-factor authentication (MFA). This adds an extra layer of security to your data.

Be Aware of AI Bias

AI systems learn from data and if the data is biased, the AI can also become biased. This can lead to unfair or discriminatory outcomes.

Educate yourself about AI bias and its potential impacts. Understanding how bias can occur helps you recognise and question AI decisions that seem unfair.

Many AI systems allow users to provide feedback. If you encounter biased or inaccurate results, report them. This helps improve the system and reduce bias over time.

Verify AI-Generated Content

AI can generate content that looks and sounds very realistic, which can sometimes be misleading.

Check Sources

Always verify the sources of AI-generated content. Cross-check information with reputable sources to ensure its accuracy.

Be Sceptical of Deepfakes

Deepfake technology can create highly convincing fake videos and audio. Be cautious of content that seems too sensational or out of character for the individuals involved.

Use AI Tools Responsibly

AI tools can enhance productivity and creativity, but they should be used responsibly.

Follow Ethical Guidelines

Ensure that your use of AI tools aligns with ethical guidelines. Avoid using AI for malicious purposes, such as spreading misinformation or invading privacy.

Stay Updated

AI technology is constantly evolving. Keep yourself updated on the latest developments and best practices for using AI safely.

Educate Others

Sharing your knowledge about AI safety can help create a more informed and secure community.

Discuss AI Safety

Talk to friends, family, and colleagues about the importance of AI safety. Sharing tips and best practices can help others use AI responsibly.

Promote Digital Literacy

Encourage others to learn about AI and digital literacy. Understanding the technology behind AI can empower people to use it more safely and effectively.

Conclusion

AI has the potential to transform our lives in many positive ways, but it's crucial to use it safely and responsibly. By protecting your personal information, being aware of AI bias, verifying AI-generated content, using AI tools responsibly and educating others, you can enjoy the benefits of AI while minimising the risks. Stay informed, stay cautious and make the most of what AI has to offer.



Aberdeenshire Farmer Targeted by Criminals

How scammers defrauded a local businessman of nearly £20,000

A busy Aberdeenshire farmer has fallen victim to a phone sales scam, losing nearly £20,000. The scam involved criminals posing as sellers of a tractor, offering a deal that seemed too good to be true.



They contacted the farmer by telephone, presenting numerous photographs of the vehicle and even the V5 registration document to make the offer appear legitimate.

The scammers claimed to be based on one of the Scottish Islands, making it difficult for the farmer to inspect the tractor in person before committing to the purchase. This geographical barrier was a crucial part of their scam. After some negotiation, a sale price was agreed upon, and the farmer transferred the money. The criminals assured the farmer that transportation had been arranged and that the tractor was on a ferry bound for Aberdeen. However, the tractor never arrived, leaving the farmer out of pocket and without the promised vehicle.

This incident highlights the importance of being cautious when dealing with unsolicited offers, especially those that seem unusually good.

It serves as a reminder to verify the authenticity of sellers and to be wary of transactions that require significant upfront payments without the opportunity for personal inspection.

5 Tips to Avoid This Scam

Verify the Seller's Identity

Always check the seller's credentials and contact details. Look for reviews or feedback from other buyers to ensure they are legitimate.

Request a Video Call

Ask for a live video call to see the item in real-time. This can help confirm the existence and condition of the item.

Use Secure Payment Methods

Avoid direct bank transfers. Use secure payment methods that offer buyer protection, such as credit cards or reputable online payment services.

Check Documentation Carefully

Verify the authenticity of any documents provided, such as registration papers, by cross-referencing with official records or contacting the issuing authority.

Be Wary of Too-Good-to-Be-True Deals

If an offer seems unusually good, it probably is.

Trust your instincts and be cautious of deals that require quick decisions or upfront payments without thorough verification.



Sextortion Nightmare

One North East Man's Nightmare of Sexual Exploitation

In the digital age, dating apps have revolutionised how people connect. But for one young North East man in his 20's, what began as an exciting match on a popular dating app, spiralled into a harrowing ordeal of sexual extortion, ultimately costing him £10,000.



The Scam

The victim, who has chosen to remain anonymous, matched with a seemingly suitable individual on a dating app. After weeks of engaging and flirtatious conversations, the scammer suggested moving their interaction to a private messaging platform. What followed was an intimate exchange of personal and compromising photos - a moment of trust that the scammer would exploit.

Soon after receiving the photos, the scammer revealed their true intentions. They threatened to release the explicit material to the victim's family, friends and employer unless he paid a substantial amount of money. Fear and embarrassment drove the victim to comply, sending money in increments over several weeks.

The Aftermath

By the time the scam ended, the victim had transferred £10,000 to scammers. Realising the futility of paying, he finally sought help from authorities.

Scams such as these are meticulously planned, and victims often feel too ashamed to report them. It's crucial to break this stigma and raise awareness.

What Could Have Been Done?

Cybersecurity experts emphasise that awareness and caution are key to avoiding such scams. Here's what the victim, and others in similar situations, could have done to protect themselves.

Vet Profiles Thoroughly

Cross-check the social media profiles of potential matches for inconsistencies. Scammers often use fake or stolen photos.

Delay Sharing Personal Details

Avoid moving conversations to private platforms too quickly and refrain from sharing personal or compromising information, no matter how trustworthy the person seems.

Beware of Emotional Manipulation

Scammers are adept at building trust and creating a false sense of intimacy. Take time to assess the legitimacy of their intentions.

Use Reverse Image Search

This simple tool can help identify if the photos used in a profile are fake or stolen from elsewhere on the internet.

Report Suspicious Behaviour

If anything feels off, report the profile to the dating app. Early intervention can prevent escalation.

Resources for Victims

For those who fall victim to sextortion, Police Scotland urges immediate reporting.

A Call for Vigilance

This young man's story highlights the urgent need for heightened vigilance in the digital dating world. While technology brings us closer together, it also provides an opportunity for exploitation. By staying informed and cautious, individuals can protect themselves from falling prey to such insidious scams.

For further advice visit www.scotland.police.uk/advice-and-information

Keeping Our Communities in the North East Safe

Police Scotland's North East Division covers rural and urban areas in Moray, Aberdeenshire and Aberdeen City. The division has five territorial command areas which have their own dedicated Area Commander, who is responsible for the daily policing function. Each command area is served by a number of community policing teams whose activities are built around the needs of the local community. These teams respond to local calls and look for long term solutions to key issues. They are assisted by the division's Crime Reduction Unit who deliver against

Force and local priorities in a number of areas, including physical and social crime prevention, supporting and enhancing community engagement and creating and sustaining strong and effective partnership working.

Website

www.scotland.police.uk

Twitter

www.twitter.com/NorthEPolice

Facebook

www.facebook.com/NorthEastPoliceDivision



North East Division Crime Reduction Team

Moray

PC Richard Russell
richard.russell@scotland.police.uk

Aberdeen City

PC Mark Irvine
mark.irvine@scotland.police.uk

Aberdeenshire

PC Mike Urquhart
michael.urquhart@scotland.police.uk



**POLICE
SCOTLAND**
Keeping people safe
POILEAS ALBA