Identity thieves beware! AI software accurately spots if someone is lying online by studying their mouse movements

- **The AI, which analyses speed of mouse movements, is 95% accurate**
- **A group of 40 participants took part in a quiz of their personal information**
- **Half the group was asked to lie and produced distinctive mouse movements**
- **The findings could be used to develop better online security methods**

By TIM COLLINS FOR MAILONLINE
PUBLISHED: 06:18 EST, 12 June 2017 | **UPDATED:** 06:38 EST, 12 June 2017

A surprising new method for catching out online fraudsters has been uncovered by researchers studying computer mouse movements.

Cognitive scientists created AI software that can spot when a person is lying thanks to changes in the way they move their onscreen pointer, with 95 per cent accuracy.

The findings could be used as an additional security step to detect criminal activity when we provide sensitive information over the internet.

Scroll down for video

Scientists measured the mouse movements of participants in a computerised quiz and found that the average movements of people who were told to lie were much less direct than those who told the truth

Researchers from the University of Padova in Italy asked 40 participants to provide personal details during a computerised quiz.

Half of the group were told to respond truthfully, while the other half were given fake identities to memorise.

They were then asked a series of 12 questions and the computer kept track of the movements of each participant's mouse as they filled out the information.

The quiz consisted of six expected questions, which focused on the type of information contained in online security verification, like 'is Giulia your real name' and 'were you born in Padova'.

But they were also asked six unexpected questions, like 'is Capricorn your Zodiac sign' and 'is Venezia the capital of the region where you live', designed to trip up the liars.

The researchers found that fake answers produced a different style of movement to people who were answering truthfully, particularly in these unexpected questions.

MOUSE MOVEMENTS

Cognitive scientists who measured the mouse movements of a group of 40 participants of a computerised quiz have found that their AI software can spot a liar with 95 per cent accuracy.

The researchers found that fake answers produced a different style of movement to people who were answering truthfully, particularly in unexpected questions which required additional thinking or research to answer.

Truth tellers generated a smooth line movement while liars produced a more chaotic pattern.

And this pattern was visible even when the liars were telling the truth, their dishonesty seemed to affect their movements overall.

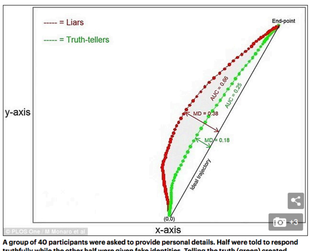
The findings could be used as an additional security step when we give out sensitive information.

Writing in their paper, published in the journal **PLOS One**, the researchers said: 'While truth-tellers respond automatically to unexpected questions, liars have to "build" and verify their responses.

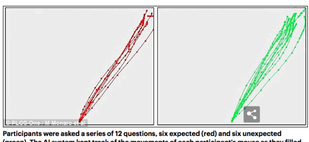
'While truth-tellers easily verify questions involving the zodiac, liars do not have the zodiac immediately available, and they have to compute it for a correct verification.

'This lack of automaticity is reflected in the mouse movements used to record the responses as well as in the number of errors.'

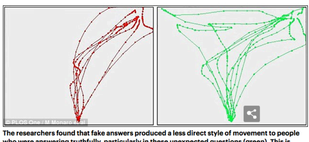
Participants were also asked eight control questions requiring a yes or no answer, which the liars also told to answer truthfully.



A group of 40 participants were asked to provide personal details. Half were told to respond truthfully while the other half were given fake identities. Telling the truth (green) created mouse movements much closer to the ideal than those who were lying (red)



Participants were asked a series of 12 questions, six expected (red) and six unexpected (green). The AI system kept track of the movements of each participant's mouse as they filled out the information. Truth tellers generated a smooth line movement (pictured)



The researchers found that fake answers produced a less direct style of movement to people who were answering truthfully, particularly in these unexpected questions (green). This is because they had to 'build' the answers to the questions, rather than answer automatically

The researchers found that the liars had a distinctive mouse movement pattern that was less direct than truth tellers.

This pattern was visible even when the liars were telling the truth, their dishonesty seemed to affect their movements overall.

'From a cognitive point of view, what is interesting here is that, in the experimental design, the mind-set of the liars also extended its effects to questions when they were responding truthfully,' the researchers added.

'To our knowledge, this pattern of results has never been reported before and could be an indication of the level of sensitivity of the technique of mouse-movement analysis.'

THIEVES CAN STEAL YOUR PIN USING THERMAL IMAGING

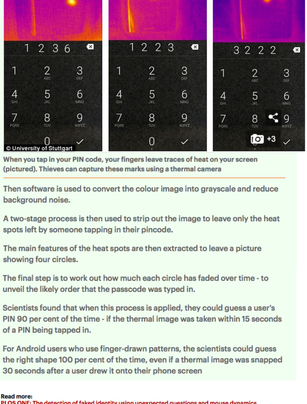
Thieves have uncovered a new way to find out your smartphone pin code, it was revealed in March.

After you tap in the digits, scammers can use thermal camera to take picture of the heat marks from where your fingers have just tapped the screen.

They can even work out the order that you typed in your code because each heat spot gets fainter over time.

And Android users who use a finger-drawn pattern to unlock their phone are the highest risk of falling victim to this new scam, scientists have revealed.

First, a thermal camera set to detect temperatures between 19 degrees Celsius (66F) and 32 degrees Celsius (90F) takes a snap of an phone screen immediately after a code is entered.



When you tap in your PIN code, your fingers leave traces of heat on your screen (pictured). Thieves can capture these marks using a thermal camera

Then software is used to convert the colour image into grayscale and reduce background noise.

A two-stage process is then used to strip out the image to leave only the heat spots left by someone tapping in their pincode.

The main features of the heat spots are then extracted to leave a picture showing four circles.

The final step is to work out how much each circle has faded over time - to unveil the likely order that the passcode was typed in.

Scientists found that when this process is applied, they could guess a user's PIN 90 per cent of the time - if the thermal image was taken within 15 seconds of a PIN being tapped in.

For Android users who use finger-drawn patterns, the scientists could guess the right shape 100 per cent of the time, even if a thermal image was snapped 30 seconds after a user drew it onto their phone screen

Read more:
PLOS ONE: The detection of faked identity using unexpected questions and mouse dynamics