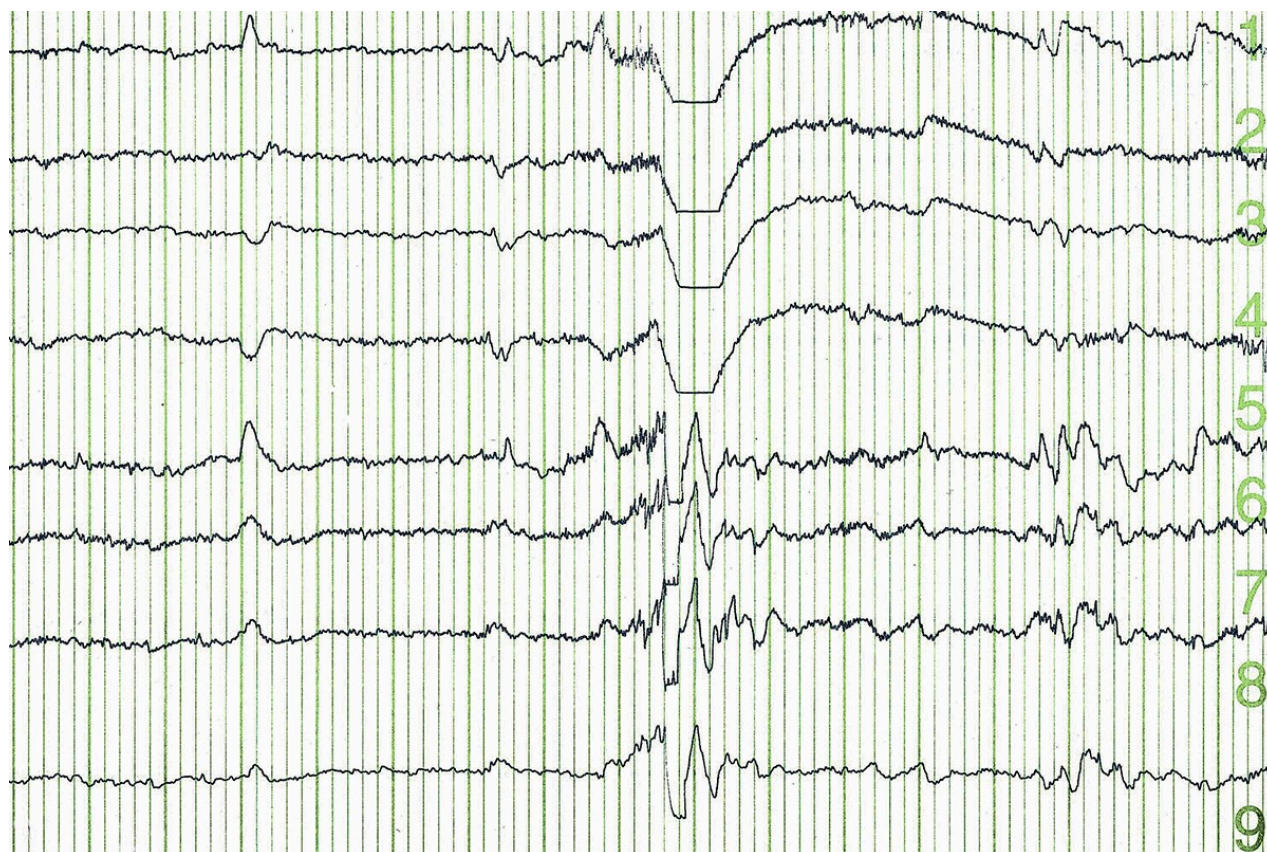DAILY NEWS 19 January 2017

Brainwaves could act as your password – but not if you're drunk

Brainwave: please log me in
Panther Media GmbH/Alamy Stock Photo

By **Nicole Kobie**

Getting drunk could make it harder to enter your password – even if your brainwaves are your login.

Brainwave authentication is one of many biometric measures touted as an alternative to passwords. The idea is for a person to authenticate their identity with electroencephalogram (EEG) readings. For example, instead of demanding a passcode, a computer could display a series of words on a screen and measure the user's response via an EEG headset. EEG signatures are unique and are more complex than a standard password, making them difficult to hack.

But while research suggests that EEG readings can authenticate someone's identity with accuracy rates around 94 per cent, there could be confounding factors – including whether you've had a few too many drinks.

Tommy Chin, a security researcher at cybersecurity consultancy firm Grimm, and Peter Muller, a graduate student at the Rochester Institute of Technology, decided to test this theory experimentally, by analysing

people's brainwaves before and after drinking shots of Fireball, a cinnamon-flavoured whisky.

"Brainwaves can be easily manipulated by external influences such as drugs [like] opioids, caffeine, and alcohol," Chin says. "This manipulation makes it a significant challenge to verify the authenticity of the user because they drank an immense amount of alcohol or caffeinated drink."

Too drunk to log on

Chin and Muller presented their findings at security conference ShmooCon in Washington DC, last weekend, with initial results from a small number of tests indicating that brainwave authentication accuracy could fall to 33 per cent in inebriated users. They recruited more participants at SchmooCon to gather more data.

The problem is not confined to drink and drugs. John Chuang at the University of California, Berkeley, last year published research into the impact of exercise on EEG authentication and found that accuracy degrades immediately after a workout (though it quickly recovered). He suggests that other factors such as hunger, stress or fatigue could also reduce reliability.

"Depending on the application, it may be a wonderful feature that a drunk person cannot authenticate into a system after they have had too many drinks," Chuang says.

If accuracy under different conditions were required, it could be possible to collect multiple brainwave "templates" for a user by separately mapping their EEG signature when drunk, tired and so on. Chin and Muller also found it is possible to tweak the EEG data analysis using machine learning to improve the results for participants who were inebriated.

But for brainwave authentication to be used in the real world, Chuang says that systematic research should be done on how all kinds of different factors could affect its accuracy, "such as physical exercise, mental fatigue, stress, distraction, changes in affect or mood, or the effects of caffeine, sugar, or medication".