

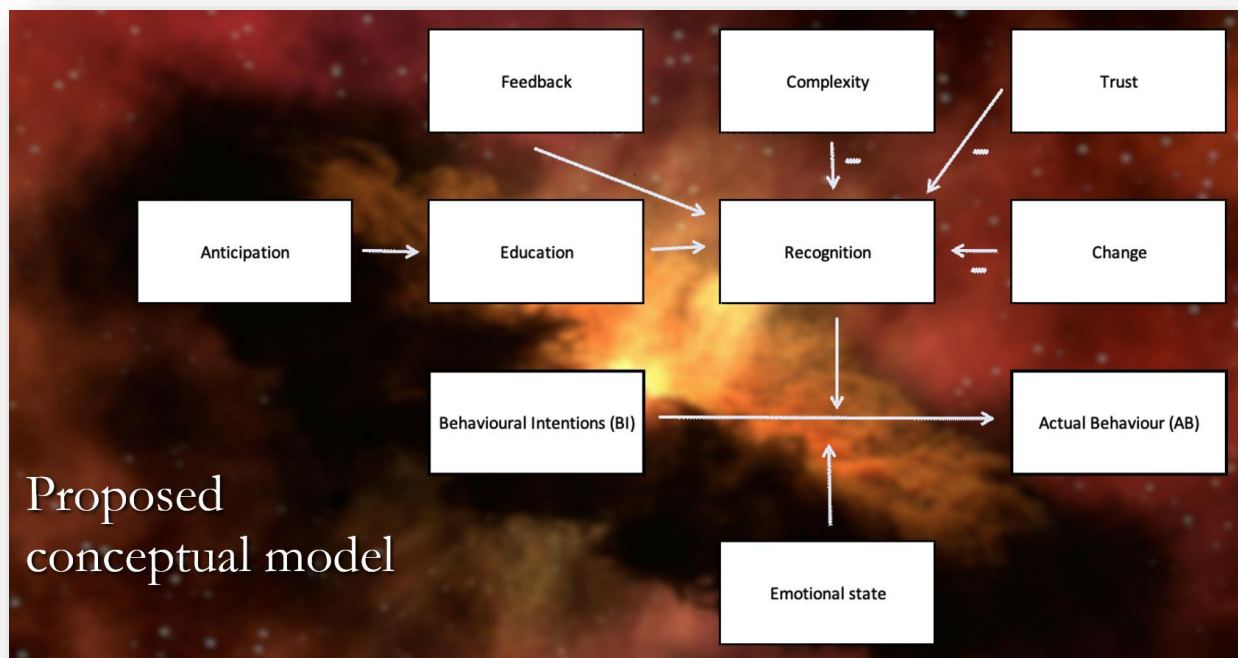
**FinCrime F\*\*\*-Ups Virtual Event Series – 14 January 2021**

Fred Jekel – Bytes vs. Behaviour

Thank you for joining the first edition of the webinar series ‘Navigating through the lessons learned from financial crime failures within a confidential environment,’ powered by the ACFCS Dutch Chapter. During our first webinar, we explored the relation between human behaviour and technical security measures. The key question was, could we make the technical measures work effective by influencing human behaviour? In order to answer this question, it is critical to understand why people become victims of cybercrime. Often, the technical measures we have in place are effective and people should not fall for social engineering schemes. However, we see that actual behaviour differs from these intentions. The same goes for technical prescriptions in an IT environment: why do people refrain from taking the measures as they should be? Consider a safety belt in a car: if you don’t use it, it is worthless.

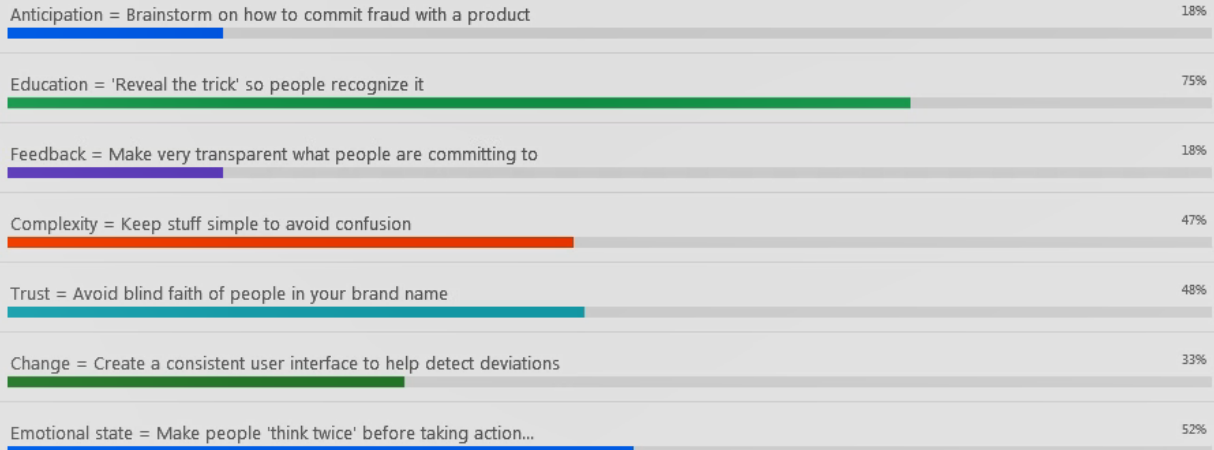
If we understand this relation, we can take steps to make the technical measures more effective.

During the webinar, a conceptual model was presented which explains the relation between behavioural intentions and actual behaviour in the field of cyber security. This model is the result of an MBA thesis at Nyenrode Business University.



The model is composed of 8 propositions – concepts that influence another concept or the relation between behavioural intentions and actual behaviour. During the webinar we conducted a poll to get an indication of the strength of each concept. The results are shown below.

Fred presented 10 constructs. Which three are constructs that would have the most impact on keeping you from clicking on a possibly malicious invite? Pick three:



Are you interested in participating in the further enhancements of the model? Please reach out to [member@acfcs.nl](mailto:member@acfcs.nl) to learn how you can contribute.