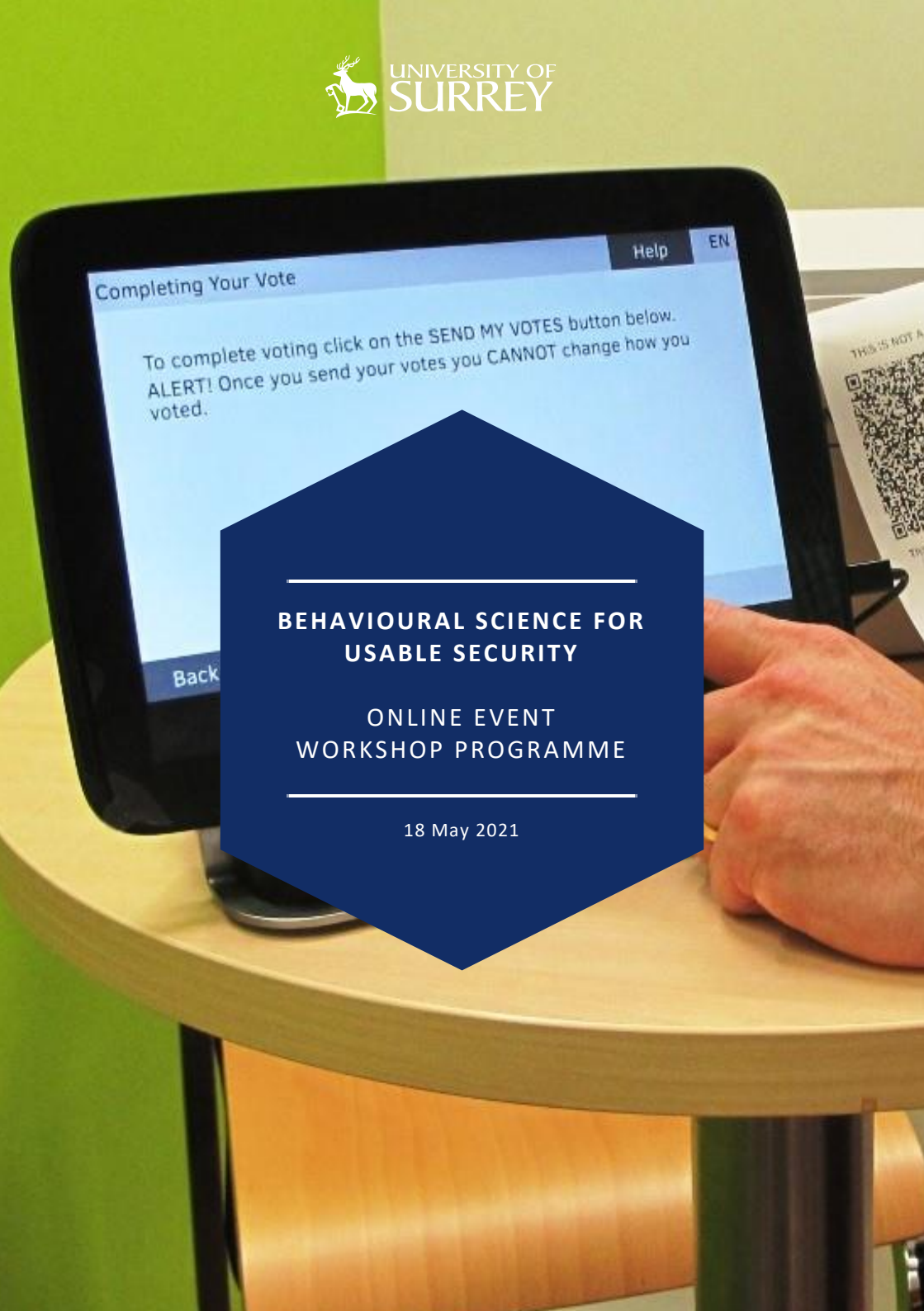
UNIVERSITY OF SURREY



BEHAVIOURAL SCIENCE FOR USABLE SECURITY

ONLINE EVENT
WORKSHOP PROGRAMME

18 May 2021

OUR SPONSORS

DECaDE is a 5-year UKRI/EPSRC interdisciplinary Digital Economy Centre addressing multiple challenges around the emerging decentralised digital economy, across diverse academic fields including Human-Computer Interaction, Artificial Intelligence, Digital Transformation and Digital Business models, Decentralised Data (including Distributed Ledger Technologies), Computational Legal Theory, and Cyber Security.

decade.ac.uk

The institute of Advanced Studies (IAS)
The Institute of Advanced Studies (IAS) at the University of Surrey sponsors workshops and Fellowships at the 'cutting edge' of science, engineering, social science and the humanities. Through this scheme the Institute fosters interdisciplinary collaborations and encourages a flow of international scholars to visit, enjoy their stay at Surrey and leave behind excellent ideas and innovations.

ias.surrey.ac.uk

INTRODUCTION

Cyber security is hard. When people interact with the Internet for applications such as online banking, they understand that there are cyber-security risks, and they must follow procedures, at some slight inconvenience, in order to manage them. However, when security mechanisms are optional, they do not achieve the necessary take-up.

Behavioural science approaches have occasionally been applied to such security mechanisms to obtain a better understanding of users' security decisions and behaviour, but more is needed for the insights from behavioural science to affect the design of usable secure systems. The aim of this proposed workshop is to shed light on how security needs to be designed to work with real users.

We propose to use online electronic voting as a context to provide a focus for the workshop.

The cyber security problem is particularly acute in electronic voting, where the technical literature contains some of the most complex and subtle technical security designs of any enterprise system.

They must ensure ballot secrecy, end-to-end verifiability, election integrity, and voter authentication and anonymity within one system. Designs typically make use of cryptography to obtain the technical assurances, but also rely on sufficient voters following particular security (optional) procedures, in particular to verify their own vote.

System design questions raise both computer science and behavioural issues. The following table poses questions tagged with concepts/phenomena from psychology, management science/economics that may be examined using verifiable electronic voting as a novel and impactful context for the study of human behaviour.

How can we get voters to follow these procedures?	Influence/persuasion, motivation, ethical judgment and decision-making
Why should users care about verifiability and other features of the system? Is verifiability incentive-compatible for voters?	Motivation, incentive-compatibility, citizenship behaviour, attitude change
How will voters learn about the features of the system? What kinds of unintended behaviours/risks are possible?	Problem-solving, learning, ability/motivation and skill acquisition forms and processes, ethical judgment and decision-making
How can we understand their view of the system, and how can it help us design better more effective systems?	Survey design, intentions and behaviour, psychological needs, satisfaction, identity, inclusivity, judgment and decision-making (including ethics, defaults, order effects, etc.)

Continued ▶

The “big picture” is that there is a real problem with design issues that can become a context for the study of human behaviour and therefore, appeal to behavioural researchers as well. This is because for the system to be effective, end users need to master specific knowledge and skills, engage with various features the system offers, including key features that ensure system security, and contribute feedback to ensure the design caters to the needs of end users. Electronic voting is a particular application that raises these challenges, some particular to voting but others more general, and the insights gained will be more widely applicable.

The aim of the workshop is to bring together computer scientists and behavioural scientists to address these challenges.

Welcome to the workshop on Behavioural Science for Usable Security. We think that this workshop is a great opportunity to bring together behavioural science and usable security and seek novel solutions to cyber security problems. We are delighted to welcome our four keynote speakers who will introduce their areas of expertise and set us up for breakout room discussions later on, when we will tackle some security challenges with a mix of behavioural and security experts. We are looking forward to sharing these discussions with you and hope that you find the workshop inspiring and productive.

Workshop chair:
Prof Steve Schneider, University of Surrey

Organising committee:
Dr Adrian Banks, University of Surrey
Dr Irina Cojuharenco, University of Surrey
Prof Steve Schneider, University of Surrey
Prof Helen Treharne, University of Surrey

Administrative support:
Vicki Blamey, Institute of Advanced Studies
Ele Pucci, Surrey Centre for Cyber Security

PROGRAMME

(UK time)

13.00 – 13.10	Welcome and Introduction— Prof Steve Schneider

RESEARCH PRESENTATIONS

13.10 – 13.25	Dr Karen Renaud, University of Strathclyde
13.25 – 13.40	Prof Daniel Read, Warwick Business School
13.45 – 13.55	Edward Flavahan, The Behavioural Insights Team
13.55 – 14.10	Prof Peter Ryan, University of Luxembourg
14.10 – 14.30	Q & A
14:30 – 14.45	Break
14.45 – 14.55	Introduction to breakout sessions - Dr Irina Cojuharenco
14:55-15:45	Break-out rooms
15:45-16:00	Break
16:00 - 16:50	Feedback from breakout groups
16:50 - 17:00	Final Remarks

SPEAKERS

DR KAREN RENAUD

Strathclyde Chancellor's Fellow, Human Centred Security and Privacy at the University of Strathclyde

Karen Renaud's research focuses on human-centred security, a branch of Human Computer Interaction (HCI). She is interested in the interplay between users and security in the context of societal and industrial use. She is working towards creating a natural, easy yet secure interaction between humans and devices.

Her work has a strong development, experimental and deployment focus, testing solutions in practical situations. She has come up with a number of novel solutions to improve usability in a wide range of situations. She has also done fundamental work in understanding people's mental models of security in a variety of applications and contexts.

PROF DANIEL READ

Professor of Behavioural Economics at Warwick Business School

Daniel Read is professor of behavioural economics at Warwick Business School He has held faculty positions at Leeds University Business School, London School of Economics (Reader) and Durham Business School (Professor), and visiting positions at INSEAD, Yale School of Management, and Rotterdam Business School. Professor Read has consulted for the UK government and the Financial Services Authority on many aspects of behavioural economics, especially as it relates to consumer welfare and environmental marketing. He has published widely in leading journals including Psychological Review, Management Science, Organizational Behaviour and Human Decision Processes, Risk Analysis, and Journal of Experimental Psychology: Applied. He is a former associate editor of Management Science, and former editor of Journal of Economic Psychology.

Daniel's research interests include judgment and decision making including intertemporal choice, choice under uncertainty and risk, heuristics and biases, together with philosophical psychology.

Continued ▶

EDWARD FLAHAVAN

Policy Advisor at The Behavioural Insights Team

Edward Flahavan is an Advisor working across multiple policy areas. He works closely with BIT's CEO, David Halpern, on pressing policy issues. Prior to this, Edward was seconded to the Cabinet Office's Economic and Domestic Affairs Secretariat (EDS). Within BIT, his previous role was working as a researcher in the health team working across a range of public health projects.

Before joining BIT, Edward worked as a macroeconomic analyst at a financial research firm and in the consumer goods industry.

Edward holds an MSc in Behavioural and Economic Science from the University of Warwick and a BA in Philosophy, Politics, Economics and Sociology from Trinity College Dublin.

PROF PETER RYAN

Professor of Applied Security at the University of Luxembourg

Peter Ryan has published extensively on cryptography, cryptographic protocols, mathematical models of computer security and, most recently, high assurance voting systems. He is the creator of Prêt à Voter (with David Chaum and Steve Schneider), Pretty Good Democracy (with Vanessa Teague) and OpenVote (with Feng Hao) and Selene (with P Roenne and V Iovino) verifiable voting schemes. With Feng Hao he proposed the Password Authenticated Key Establishment Protocol J-PAKE.

Prior to joining the University of Luxembourg he was a Professor of Computing Science at Newcastle University. He has worked at GCHQ, the Defence Research Agency, the Stanford Research Institute, Cambridge and the Software Engineering Institute, CMU Pittsburgh.

Peter's research interests include information assurance, cryptography, cryptographic protocols, design and analysis of secure systems and properties, analysis of information flow, fully verifiable voting schemes, quantum cryptography and the socio-technical aspects of security.

SURREY CENTRE FOR CYBER SECURITY

University of Surrey
Guildford, GU2 7XH, UK

surrey.ac.uk