

Hear first about SASIG events and industry news

Follow us on:



Fraud and the enterprise

Costing businesses as much as individuals

In association with

Which?

Some call cyber-related crime the greatest transfer of wealth in history. If it were an economy, it would have the third largest GDP and enjoy an annual growth rate of 15% – the envy of the United States and China. The estimated cost of cybercrime to the global economy in 2024 was \$8 trillion. While much attention is given to ransomware, which is undeniably disruptive, the proceeds from cyber-enabled fraud far exceed those from online extortion, and the barrier to entry is significantly lower. Fraud is the entry-level crime.

Scams against individuals are well known, but fraud also targets enterprises, often with even greater rewards. When consumers are scammed, businesses, particularly those in the financial sector, also pay the price. The tactics, techniques, and procedures (TTPs) used by online fraudsters are often strikingly similar to those deployed by other cybercriminals. Social engineering, for instance, remains a key weapon in their arsenal.

We are delighted to host this important event in association with Which? to explore the challenges scammers present to both individuals and organisations; how reporting cybercrime can support law enforcement in disrupting criminal networks; and what strategies we can use to reduce our susceptibility to the siren calls of online fraudsters.

All SASIG events operate under Chatham House Rule, and there is no charge to attend. Lunch and refreshments for the day are kindly provided by our hosts.

Thursday 12 June 2025
9.30am to 3.30pm
Camden, London

Chair

Martin Smith MBE Chairman and Founder, The SASIG

9.30am **Registration, coffee, and networking**

10am **Welcome and introductions**
Martin Smith MBE Chairman and Founder, The SASIG

10.15am **Keynote presentation: Beyond the money - What is fraud really costing us?**
Rocio Concha Director of Policy and Advocacy and Chief Economist, Which?

Fraud is no longer just a financial crime, it is a pervasive and evolving threat with serious, long-term consequences. In this session, Rocio will share insights from over nine years of work tackling consumer scams. Drawing on real-world experience and research, she will reveal the key lessons learned. Beyond immediate financial losses, fraud leaves behind a trail of hidden costs: the psychological toll on victims, the erosion of consumer trust, and the wider impact on the UK economy.

10.45am **Panel session: How do we build trust to encourage people to share data?**
Facilitated by **Martin Smith MBE** Chairman and Founder, The SASIG
Dr Mahlet (Milly) Zimeta Head of Digital and Data Policy, Which?
Mark Hendry Digital Risk Partner, S&W
Simon Newman Chief Executive Officer, Online Dating and Discovery Association

Data sharing is a powerful tool in the fight against fraud, enabling stronger prevention, quicker detection, and faster response. But collaboration relies on trust. Whether it's individuals reporting scams or organisations sharing threat intelligence, vital data is often held back due to fears over privacy, liability, or reputational risk. This panel will explore what it takes to build the trust needed for meaningful data sharing. From transparency and consent to regulation and secure frameworks, we will examine the policies, principles and partnerships that can unlock the collective defence we urgently need.

11.30am **Tea, coffee, and networking break**

12 noon **The ripple effect of supply chain attacks in UK CNI**
Gavin Stubbs Principal Consultant, Bridewell

We all know the disruptive impact fraud and cyber attacks can have on a victim organisation, but what about the ripple effects across their supply chain? A successful attack can trigger operational disruption, financial losses, and data exposure. For UK critical national infrastructure (CNI), which relies heavily on complex supply chains and third-party vendors, the consequences can be especially severe.

This session will explore:

- How cyber attacks can cascade through a wider supply chain
- Lessons learned from recent UK-based incidents
- Practical strategies for reducing supply chain risk and improving overall resilience

12.30pm **The ethical fork in the road facing Gen Z: How can we inspire Gen Z to become ethical hackers in modern workplaces?**

Fergus Hay CEO & Co-founder, The Hacking Games

With \$23.8 trillion projected to be lost to cybercrime by 2027, and 80% of NYC teenagers reportedly having been hacked by the age of 16, we're facing a generational crisis. The Hacking Games aims to inspire, educate, and empower young people to become defenders rather than attackers.

This session explores the societal, technological, and law enforcement challenges surrounding youth cybercrime and what we can do to confront and prevent it.

1pm **Networking lunch**

1.45pm **What are the fraud threats to businesses and why should you report to law enforcement?**

Jen V Online Crime Centre Programme Lead, City of London Police

Fraud is no longer a peripheral threat – it is a central economic issue. In the UK alone, the financial impact of fraud runs into the billions, affecting public finances, undermining trust in financial institutions, and placing a growing burden on businesses of all sizes. This session will unpack the true cost of fraud across the economy, from direct financial losses to the indirect consequences such as operational disruption, reputational damage, and increased regulatory pressure. We will explore where the vulnerabilities lie, which sectors are most exposed, and what coordinated action is needed across industry, government, and law enforcement to tackle fraud at scale.

2.15pm **Fuelling fraud: How infostealers drive the dark economy**

Borja Rosales VP EMEA, KELA

Dave Gill EMEA Partner Manager, KELA

Infostealer malware has become a key enabler of cyber-enabled fraud, driving account takeovers, identity theft, and business email compromise (BEC). These lightweight, scalable tools quietly harvest vast amounts of sensitive data from infected devices, often without detection. In this session, KELA will share insights from over 300 real-world cases, revealing how stolen credentials are monetised, and how cyber threat intelligence (CTI) can help organisations detect, prevent, and disrupt fraud at scale. By understanding the tactics, techniques, and procedures (TTPs) of cybercriminals, security teams can stay ahead of evolving threats and reduce the impact of infostealer-driven attacks.

2.45pm

Panel session: Resilience, awareness and education

Facilitated by **Martin Smith MBE** Chairman and Founder, The SASIG

Helen Fairfax-Wall Chief Policy and Communications Officer, Stop Scams UK

Byron Mann Policy Advisor, Which?

Andrew Rose Chief Security Officer, SoSafe

Nick Palmer Technical Director, Censys

Gill Thomas Director of Engagement, Capacity and Resilience, Global Cyber Alliance

Fraudsters exploit human nature as much as technology, making education and awareness our first, and often strongest, line of defence. This panel will explore the practical steps organisations can take to build resilience at every level – from employee training and customer education to better use of data and smarter user experiences. We will also discuss the broader role of financial institutions, tech platforms, and regulators in protecting the public, and why building a culture of awareness is just as critical as investing in cyber tools.

3.30pm

End of meeting

About



The Security Awareness Special Interest Group (SASIG)

SASIG is a subscription-free networking forum, membership now represents thousands of organisations of all sizes from across the world and from all sectors, public and private. Its 10,800+ membership is drawn from CIOs, CISOs and their staff with responsibility for cybersecurity within their organisations. Professionals from other disciplines (risk, HR, legal, supply, etc.) and representatives from government, law enforcement and academia are also being increasingly welcomed at events. The Chatham House Rule is strictly enforced and universally respected at all meetings, and vendors and the Press are routinely excluded. Thus, the level of debate is extraordinarily revealing and rewarding.

SASIG has a members' website at www.thesasig.com. Please register here for membership.

With thanks to our Supporters and Contributors...



01234 707 035

info@thesasig.com

www.thesasig.com