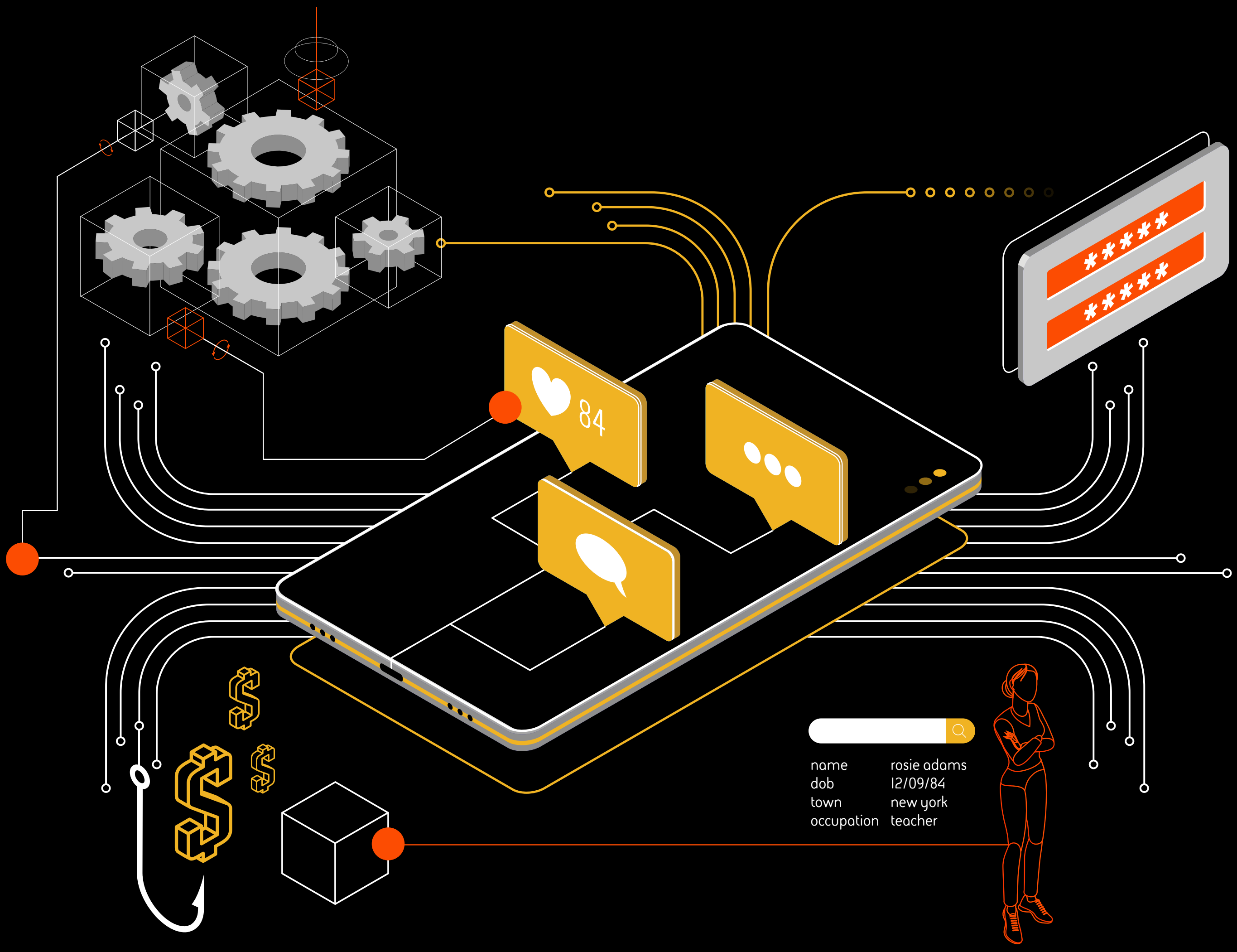
baesystems.com/theintelligencenetwork

Social Engineering

Work Stream Report Five



BAE SYSTEMS

BAE SYSTEMS

Following the launch of our Vision for Tackling Cyber Fraud twelve months ago, a working group from BAE Systems has taken the lead in exploring ways to tackle social engineering – one of the four key themes in the vision.

Social engineering remains a key technique for cyber fraudsters, and is therefore critical to the vulnerability of modern society in two separate ways:

- As a technique used by cyber attackers to steal data
- As a technique used by criminals to perpetrate the fraud itself

In this latest work stream report, Simon Viney, Cyber Security Financial Services Sector Lead at BAE Systems Applied Intelligence assesses our progress to date.

A quick recap: why is The Intelligence Network tackling social engineering?

As we laid out in our Vision, the ability of criminals to deceive people is at the heart of both cyber attacks and fraud. Most current effort goes into training people to make near impossible judgements, rather than making their tasks easier.

And sometimes we (as an industry) make it harder for people than it needs to be. For example, we train staff not to click on links or attachments when these are an integral part of business communication. And many consumer organisations communicate with customers in ways that are very hard to differentiate from those of fraudsters. At the same time, social media is making communication between consumers and corporations more public, increasing the potential for cyber-enabled fraud.

What's the scale of the problem?

Taking just the UK as an example, the scale of fraud continues to grow. UK Finance, which publishes an annual study, has reported the following alarming statistics regarding fraud in 2019:

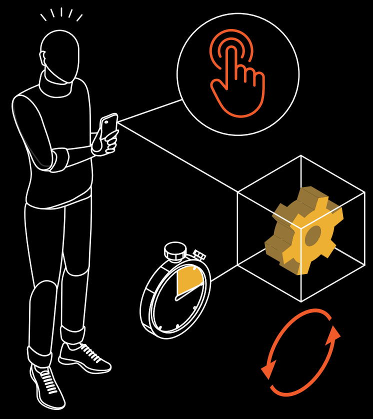
£150m

lost to remote banking fraud[1]

This covers internet banking, telephone banking and mobile app based banking, in which criminals gain unauthorised access to a customer's bank account and make an unauthorised transfer of money. Many of these instances will be due to social engineering in order to gain access to the customer's account, e.g. by tricking them to giving access to their computer.

£456m

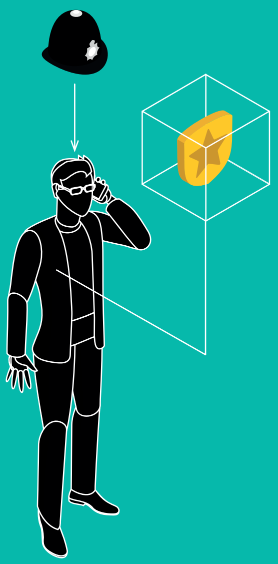
lost due to Authorised Push Payment fraud – with 95% of these frauds involving faster payments[2]



With APP fraud, individuals are tricked into sending money to a fraudster, often via social engineering. In 2019 95% of these frauds involved Faster Payment being used as the transfer mechanism.

£84m

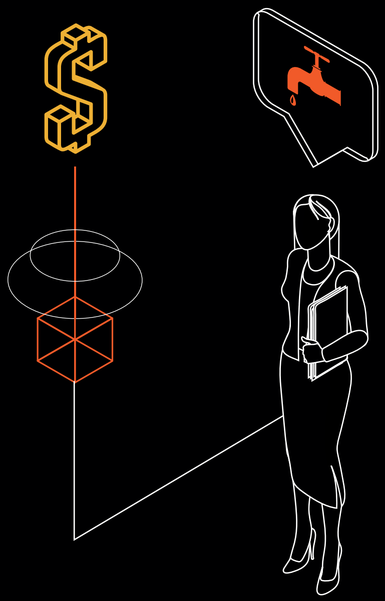
lost due to impersonation of police or bank staff[3]



In which fraudsters pose as police or bank staff and trick the customer into transferring funds to an account the criminal controls.

£50m

lost due to other impersonations[4]



Fraudsters impersonating other organisations such as utility companies, telecommunications providers or a government department such as HMRC.

For North America, according to Verizon's 2019 Data Breach Investigation Report[5], social engineering was used in 33 percent of all breaches in 2018. To give further example of the scale of such attacks the FBI's 2018 Internet Crime Report[6] highlights alarming statistics:

- 25,000 individuals reported being a victim of one of several types of social engineering attacks, resulting in nearly $50 million in losses.
- More than $100 million was reported in losses resulting from social media platforms used to facilitate the crime.
- Business email compromise / email account compromise (BEC/EAC) takes the lead netting out at more than $1.2 billion in victim losses, with California being hit the hardest and Texas taking a close second.

These figures present a significant level of fraud and highlight the ongoing challenge of tackling cyber fraud and social engineering.

Honing in on two-way trust

Unfortunately we live in a world where we do not have a good mechanism for two-way trust between organisations and individuals (or indeed between different organisations) when conducting financial transactions.

In the digital age, organisations have typically relied on usernames and passwords to authenticate individuals. Unfortunately, this doesn't work well as a two-way trust process. Where the individual did not initiate the communication, there is, for example, no easy way for them to confirm they are dealing with the correct organisation in the first place.

Furthermore, this lack of two way trust applies to both online and offline interactions, e.g. by telephone, SMS text, email and post. However, the key difference with post is that there is a significant cost and overhead for fraudsters to contact multiple targets as they often do with, say, telephone, SME text or email fraud attempts, especially if the fraud is being perpetrated from a different country.

Honing in on the issue of two-way trust, and how to solve it, is a chief concern of this working group.

So what has the industry done so far?

Our research to date has found that many activities have been performed or are currently underway to help address the risk of individuals falling victim to social engineering.

These include:

Customer education campaigns, e.g. by financial institutions - Many of the top-tier banks and some insurers, but also government bodies and government funded organisations such as the UK's Action Fraud and UK Finance (via the Take Five campaign) have been working on campaigns to educate.[7]

APP scams voluntary code - Implementation of the APP scams voluntary code in the UK is providing better redress to banking customers who fall victim to APP fraud

Telecoms providers and regulatory body activities – The telecoms providers and regulatory bodies (e.g. OFCOM in the UK and FCC in the US) have been acting to address issues around scam phone calls and robocalls. In the UK, this includes OFCOM's 'Do not originate' scheme which allows organisations to publish telephone numbers on which customers can contact them, but from which outgoing calls will not be made – thus allowing the telephone providers to block any outgoing calls using those numbers.

Shortened telephone call clearing times – In recent years the changes made – for example by BT Openreach in the UK – to shorten call clearing times to seconds, is preventing the interception of call backs made to concerned customers, stopping those customers from falling victim to a scam where they think they've dialled their bank or utility organisation but actually the fraudster kept the line open

Despite these activities, and as has been obvious to many individuals and companies during the current COVID-19 situation, fraudulent attempts using social engineering continue apace.

What technology can help?

Technology solutions will play a key role in solving the issue of two way trust. For email communications for example, the use of DMARC provides a robust way for organisations to flag which emails legitimately originate from domains they control, allowing recipients to determine if the emails are genuine or not (in practice, the recipient's email software should automatically perform this determination taking the decision away from the individual).

In addition, in the US the Federal Communications Commission (FCC) is pushing telecommunications carriers to implement STIR/SHAKEN. STIR/SHAKEN is a set of methods created by the Internet Engineering Task Force (IETF). The FCC describes use of STIR/SHAKEN as follows:

"STIR/SHAKEN is a framework of interconnected standards. STIR/SHAKEN are acronyms for the Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) standards. This means that calls traveling through interconnected phone networks would have their caller ID "signed" as legitimate by originating carriers and validated by other carriers before reaching consumers. STIR/SHAKEN digitally validates the handoff of phone calls passing through the complex web of networks, allowing the phone company of the consumer receiving the call to verify that a call is in fact from the number displayed on Caller ID."[8]

In the UK, OFCOM has consulted on the use of STIR/SHAKEN[9] and more recently the University of Warwick has announced it has received a research grant to identify new ways to tackle the problem of trust in caller ID which does not require use of a system such as STIR/SHAKEN.[10]

What more can be done?

Ultimately, the goal of this Tackling Cyber Fraud project is to provide an assessment of where we believe industry and government needs to go, in order to 'move the needle' in the fight against cyber fraud. This should entail changes that can be made at a macro level and protect individuals en-mass rather than, for example, relying on awareness and communication to individuals.

Identifying mechanisms in which communications channels such as email, SMS and telephone can become 'trusted', i.e. so that a recipient can trust the identity of a caller if they recognise the identifying details (email domain, phone number, etc.) will become key. Technologies like DMARC provide this for email, but are still not widely adopted. Meanwhile, the implementation of technologies like STIR/SHAKEN in the telecoms space, or an equivalent system, would help to prevent telephone number spoofing.

However, whilst technology solutions like these will help, we also need to reduce the opportunity for people to contact individuals from non-trusted numbers and then, with some readily obtainable personal information, socially engineer the individual in such a way as to allow a fraud to occur.

To tackle the issue of social engineering, the steps in our work stream look something like the below:

Step one

Understand the social engineering problem space

Step two

Question what the technical potential is for enabling two-way trust

Step three

Understand what has been done thus far

We are here!

Step four

Provide an assessment of where we believe industry and government needs to go in order to enable two-way trust

Step five

Reduce the opportunity for social engineering

Get involved

(GET IN TOUCH) In the telecoms industry? Have a view on the ease of implementation of authentication measures?

(GET IN TOUCH) Are you a bank, insurer or asset manager? Have you investigated how your customers fall victim to social engineering?

Find out more

(READ) The Intelligence Network's Vision for Tackling Cyber Fraud

(CHECK) the Social Engineering work stream reports:

- Four tactics sustaining cyber fraud
- Thoughts on two-way authentication
- Findings from our focus group

(WATCH) perspectives from across the cyber fraud lifecycle

Join the conversation

Email Simon Viney

Join our LinkedIn Community

BAE SYSTEMS

At BAE Systems, we provide some of the world's most advanced technology, defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
Level 1
14 Childers St
Canberra, ACT 2601
Australia
T: +61 1300 027 001

BAE Systems
Suite 905 Arjaan Office Tower,
Dubai Media City
Dubai
T: +971 (0) 4556 4700

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

References

[1] Fraud – the Facts 2020, the definitive overview of payment industry fraud, UK Finance (March 2020)

[2] Fraud – the Facts 2020, the definitive overview of payment industry fraud, UK Finance (March 2020)

[3] Fraud – the Facts 2020, the definitive overview of payment industry fraud, UK Finance (March 2020)

[4] Fraud – the Facts 2020, the definitive overview of payment industry fraud, UK Finance (March 2020)

[5] 2019 Data Breach Investigations Report, Verizon (May 2019)

[6] 2018 Internet Crime Report, FBI (April, 2019)

[7] Take Five, UK Finance (September, 2020)

[8] Combatting spoofed robocalls with caller ID authentication, Federal Communications Commission (August 2020)

[9] Promoting trust in telephone numbers, first consultation, Ofcom (April 2019)

[10] New ways to stop caller ID spoofing to be investigated, Warwick University (March 2020)

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/theintelligencenetwork

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai

Copyright © BAE Systems plc 2020. All rights reserved.

BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc. BAE Systems Applied Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ. No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.