HOW CYBER FRAUDSTERS EXPLOIT TECHNOLOGY TO TARGET, DEFRAUD AND EXTORT

By William Taaffe- COO- Lockdown Cyber Security

When was the first recorded instance of fraud?

A. 350 BC

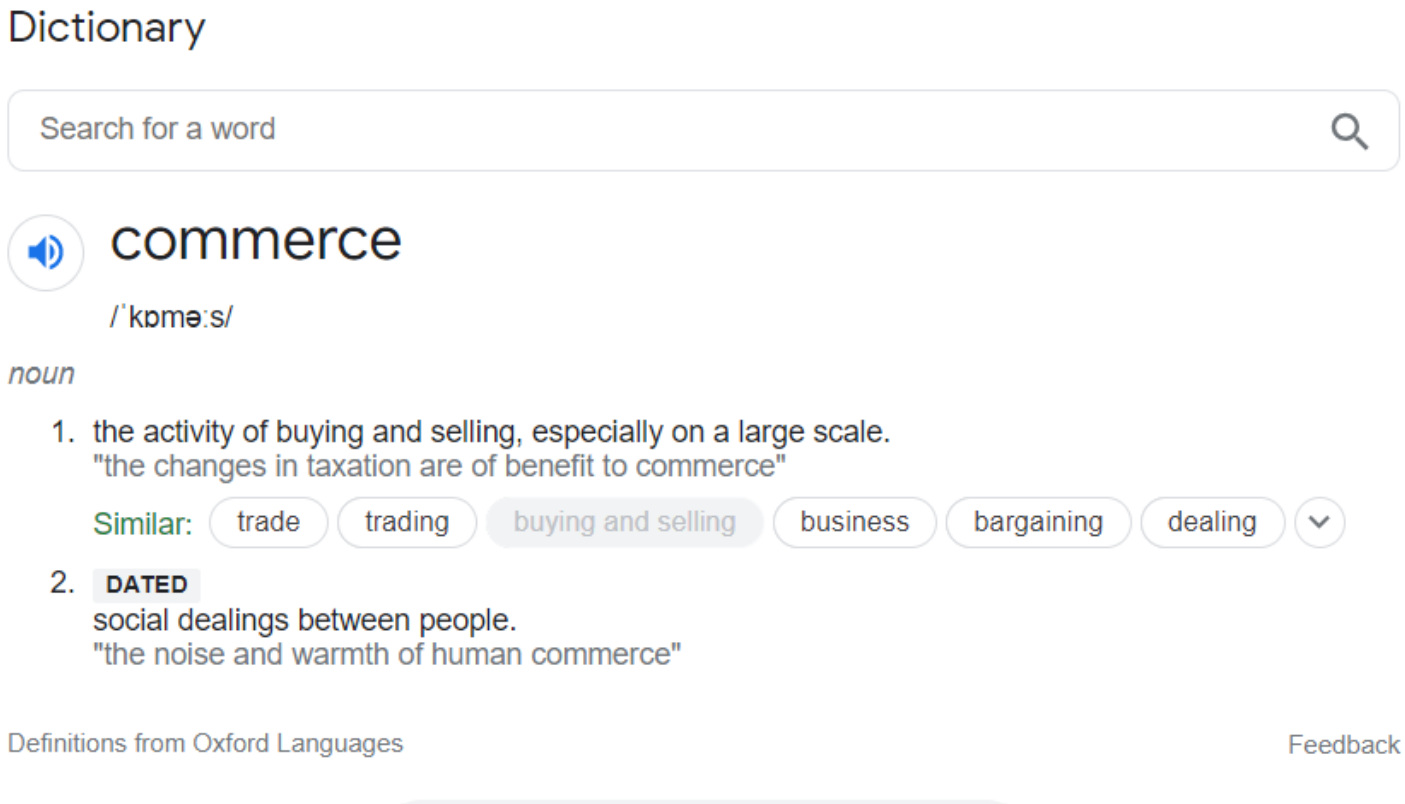
B. 8200 AD

C. 1732

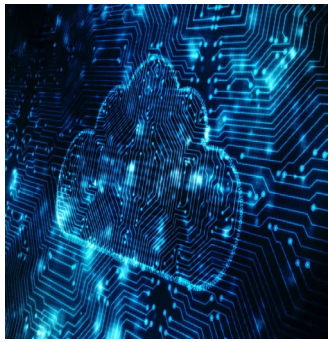
D. 1895

Lockdown
CYBER SECURITY

Since the start of Commerce, there was fraud



The Technological Age



The Technological Age

Technology has ushered in a golden age for humanity, truly connecting the world's global economy and allowing for progression across almost every field and sector

Technology allows us to better communicate, collaborate, innovate and streamline operations

Data is the new gold

Lockdown
CYBER SECURITY

Digital Security

"The fundamental problem is that security is always difficult, and people always say, 'Oh, we can tackle it later,' or, 'We can add it on later.' But you can't add it on later," said Peter G. Neumann, a computer science pioneer who has chronicled security threats on the online "RISKS Digest" since 1985. **"You can't add security to something that wasn't designed to be secure."**

Lockdown
CYBER SECURITY

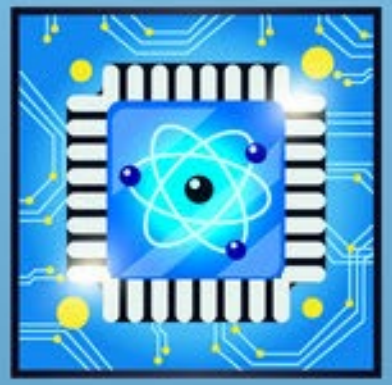
5G INTERNET

EYE AUGMENTATION

5D DATA STORAGE

AUGMENTED REALITY

ELECTRIC CARS



QUANTUM COMPUTING

ARTIFICIAL INTELLIGENCE

SUPER BRAIN

Social Engineering

Social Engineering

Social Engineering is the act of convincing someone to divulge personal or confidential information. Information which is then used to commit a criminal act

This may form part of a direct approach, through social media, dating sites, Linkedin or email. The attackers real identity is usually masked. This can be anything from harvesting personal data through to gaining someone's trust to later extort them

We have to examine our behaviours, both in work and outside of it, to combat the risk of social engineering. In the office, we define processes for a reason; to remain compliant for governance and to protect the information of our customers.

Lockdown
CYBER SECURITY

NOT SO SMART

CYBER SECURITY


Ransomware

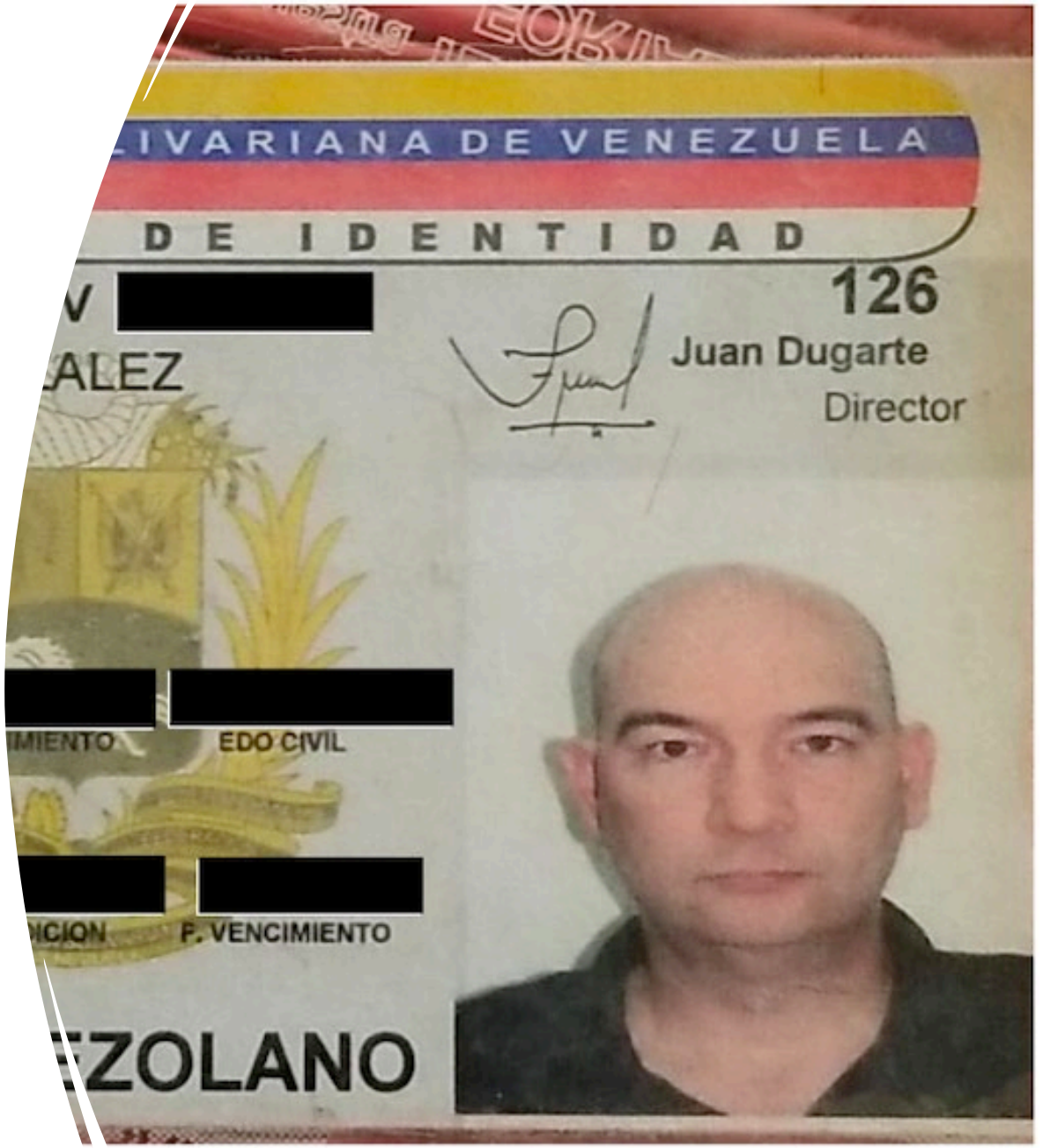
Ransomware

Ransomware: An insidious piece of malicious software which through encryption, renders systems and data inoperable.

Though examples of Ransomware can be found from the 1980's, this form of attack is often viewed as modern

The pandemic environment has seen ransoms grow 2-3 fold. Estimated global ransom payments in 2021 were predicted to be between $40bn-$170bn

United States Of America: **Most Wanted**



A Criminal in the Spotlight

Moises Luis Zagala Gonzalez was recently named and shamed by the US, as being the author of the JigSaw Ransomware strain and Thanos, Ransomware as a Service software. **But what is his day job?**

A. High School Math Teacher

B. Heart Surgeon

C. Counter Fraud Professional

D. Bus Driver

Lockdown
CYBER SECURITY

RaaS- Ransomware as a service

Ransomware attacks are growing in sophistication. Criminals have moved away from a trawler net approach to creating targeted and well researched attacks

This nefarious industry, fuelled by Cryptocurrency and supported by organised crime, allows criminals with low technical acumen to purchase sophisticated malware for global distribution. A commission is paid to the software creator for every successful attack

ShadowBrokers, Reevil and Conti are all well known ransomware gangs

Lockdown
CYBER SECURITY


DEEPFAKE

Advanced Business Email Compromise

Advanced BEC

Business Email Compromise is the act of commandeering somebodies legitimate email account, to pretend to pose as the individual as a method of committing fraud. In America, this attack method claimed upwards of $43bn between 2016-2021

This attack works effectively because the email comes from a trusted and legitimate source

Best practice is to orally confirm the intention of payment with the email sender. This usually uncovers the potential crime, showing the attempt to be illegitimate

Lockdown
CYBER SECURITY

Advanced BEC Utilises AI

Deepfake audio AI can be generated through capturing as little as ten minutes of voice audio

With this technology, an attacker can steal voice recordings from the VoIP telephone system, feed that into an AI machine and automatically generate the voice of the target, using similar syntax and sentence structuring

This technology can then be used to add an additional layer of authenticity to the attack method

Lockdown
CYBER SECURITY

Technology fights back

Though technology can be a great enabler of Cyber Fraud, it can also help detect and prevent it from happening. We see this through advanced authentication methods, due diligence tools, fraud detection software and algorithms

Cyber Fraud cannot be tackled solely through technology. In order to prevent it, we must view the problem holistically. Only through taking a joined up strategic view can we begin to really impact Cyber Fraud within our organisations. As always, tone from the top is of paramount importance

Create a common language of risk across the organisation. Using risk quantification allows you to understand the monetary impact of key digital risks, allowing for more strategic and collaborative decision making

Lockdown
CYBER SECURITY

Contact Details

Lockdown

CYBER SECURITY

William Taaffe
William@lockdowncybersecurity.co.uk
Linkedin: William Taaffe
Mobile: 07850 983 666